hyväksymispäivä arvosana

arvostelija

Elliptisten käyrien soveltuvuus salausjärjestelmiin

Antti Nyberg

Helsinki 27.4.2007

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Antti Nyberg

Työn nimi — Arbetets titel — Title

Elliptisten käyrien soveltuvuus salausjärjestelmiin

Oppiaine — Läroämne — Subject

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
	27.4.2007	18 sivua + 0 liitesivua

Tiivistelmä — Referat — Abstract

Tämä artikkeli käsittelee elliptisten käyrien käyttöä ja niihin perustuvan salausjärjestelmän turvallisuutta. Aloitetaan esittelemällä elliptiset käyrät, niiden ryhmäoperaatiot ja äärelliset kunnat; tavoitteena on luoda selkeä yhteys lähtökohtana käytetyn ryhmäoperaatioiden geometrisen kuvauksen ja äärellisten kuntien laskutoimitusten välillä. Seuraavaksi tutustutaan elliptisten käyrien turvallisuuden perustana olevaan diskreetin logaritmin ongelmaan ja arvioidaan sen vaativuutta. Esimerkkinä elliptisen käyrän salauksesta annetaan kuvaus viestin allekirjoituksesta ja salaisen avaimen vaihdosta; lisäksi tutustutaan lyhyesti älykortteihin eräänä elliptisen käyrän salauksen mahdollisena sovellusalustana. Artikkelin päättää kappale erilaisista elliptisiä käyriä vastaan esitetyistä hyökkäyksistä.

ACM Computing Classification System (CCS):
E.3 [Data Encryption]

Avainsanat — Nyckelord — Keywords
elliptinen käyrä, äärellinen kunta, salaus, hyökkäys, älykortit

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisältö

1 Johdanto

Ajatus elliptisten käyrien hyödyntämisestä salausjärjestelmissä esitettiin jo vuonna 1985; matematiikassa käyrät on tunnettu paljon pidempään. Niiden etuna pidetään lyhyempää avaimen pituutta verrattuna kilpaileviin salausmenetelmiin. Elliptisen käyrän salausta vastaan ei ole löydetty tehokkaita algoritmeja, mutta toisaalta sellaisten olemassaoloa tai -olemattomuutta ei kumpaakaan ole kyetty teoreettisesti todistamaan.

Ensisijaisesti tämä artikkeli pyrkii selventämään miten, missä ja miksi elliptisiä käyriä käytetään. Ymmärrettävästi aihepiiri on laaja, mikä tekee vähääkään yksityiskohtaisemman kuvauksen vaikeaksi; toisaalta käsiteltävän aihealueen tarkempaa rajaamista on vaikeuttanut tarve *sekä* välttää liiallista päällekäisyyttä toisaalla esitettyjen tulosten [1] kanssa *että* tuoda itse esiin riittävän mielenkiintoisia tuloksia.

Aluksi esitellään lyhyesti elliptiset käyrät ja niiden laskennan geometriset perusteet [Han04]; seuraavassa kappaleessa esitetään, miten äärellisten kuntien avulla voidaan toteuttaa elliptisten käyrien kannalta oleelliset laskutoimitukset [Cer00]. Varsinaista salausjärjestelmää käsittelevän kappaleen alle on koottu niin kuvaus diskreetin logaritmin ongelmasta [Tra04], viestien allekirjoitus ja avaimenvaihto [Ayd99, Tra04] kuin älykortit yhtenä elliptisen käyrän sovellusalueena. Seuraavaksi esitellään elliptisten käyrien turvallisuutta koskevia tuloksia, niitä vastaan suunnattuja hyökkäyksiä [Han04, Sab05] ja näiden vastatoimia [Tra04, Cor99, Möl01]. Lopuksi esitetään vielä yhteenveto.

Niin tiettyjen asioiden esitystarkkuuden kuin matemaattisten lausekkeidenkin suhteen on tehty joitakin yksinkertaistuksia; esimerkiksi symbolia ∞ käytetään suoraan tarkoittamaan äärettömyyteen määriteltyä pistettä.

2 Elliptiset käyrät

Elliptiset käyrät ovat algebrallisia, neliöllisiä tasokäyriä, joiden määritelmä on jokin *Weierstraßin normaalimuodon* eli yhtälön

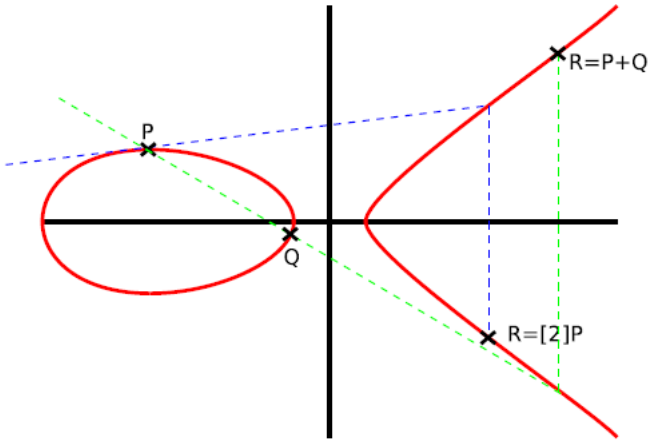
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

yksinkertaistus; valitsemalla kertoimet a_i sopivasti saadaan käyrän kaava helpommin käsiteltävään muotoon. Koska käyrien on lisäksi oltava *epäsingulaarisia*, eli vailla

[1] kts. Mikko Alakunnaan artikkeli samassa seminaarissa

teräviä kohtia tai itsensä leikkauksia, edellytetään myös, että yhtälön diskriminantti $\Delta \neq 0$. [Han04]

Elliptisten käyrien hyödyntämisen kannalta ratkaisevin ominaisuus on mahdollisuus määritellä yhteenlaskusääntö kahdelle käyrän pisteelle siten, että summa on kolmas käyrän piste. Tästä seuraa luonnollisesti se, että kukin piste on voitava laskea yhteen myös *itsensä kanssa*; mahdollisuus kertoa piste kahdella yleistyy helposti muillekin skalaareille k. Käytännössä juuri yhteenlaskuominaisuus mahdollistaa monien perinteisten salausmenetelmien ja -algoritmien toteuttamisen elliptisillä käyrillä, sillä näissä käytetty kertolasku ja eksponentin ottaminen voidaan korvata elliptisen käyrän pisteiden yhteenlaskulla ja skalaarilla kertomisella. [Tra04]



Kuva 1: Geometriset kuvaukset elliptisen käyrän pisteiden P ja Q yhteenlaskulle sekä pisteen P kahdella kertomiselle.

Käyrän kahden eri pisteen P ja Q kautta kulkeva suora leikkaa käyrän kolmannessa pisteessä; peilaamalla tämä piste x-akselin suhteen saadaan $R = P + Q$. Käyrän pisteen P tangentti leikkaa sekin käyrän omassa pisteessään; vastaavasti peilaamalla tämä piste x-akselin suhteen saadaan $R = 2P$. Kuva 1 havainnollistaa molempia laskutoimituksia. [Tra04]

Elliptiset käyrät ovat helpoimmin ymmärrettävissä, kun ne on määritelty yli reaalilukualueen. Ne on kuitenkin mahdollista määritellä myös kompleksiluvuille ja jopa mille tahansa yleiselle *kunnalle* [Han04].

3 Määritteleminen yli äärellisten kuntien

Äärelliset kunnat koostuvat äärellisestä joukosta kuntaelementtejä, joiden kesken on määritelty tietyt ehdot täyttävät yhteen- ja kertolaskuoperaatiot. Koska elliptisten käyrien vaatimat laskutoimitukset olisivat reaali- tai kompleksiluvuilla liian hitaita, ja pyöristysvirheiden vuoksi myös liian epätarkkoja, elliptinen käyrä määritellään salausjärjestelmissä yleensä jonkin äärellisen kunnan yli. Mahdollisia vaihtoehtoja ovat alkuluku- ja binäärikunnat; tarkemmin kunta valitaan siten, että sen ja valitun elliptisen käyrän muodostama ryhmä sisältää riittävän suuren, äärellisen määrän pisteitä takaamaan salausjärjestelmälle halutun turvallisuustason. Näiden pisteiden lukumäärän laskeminen ja halutun suuruusluokan takaaminen ovat oma osa-alueensa elliptisten käyrien tutkimusta. [Han04]

Koska kummankaan seuraavana esitellyn kunnan tapauksessa elliptisen käyrän kuvaaja ei ole sileä, reaaliluvuille määritellyt pisteiden yhteenlaskun ja kahdella kertomisen geometriset kuvaukset eivät toimi sellaisenaan; niistä muokatut laskusäännöt esitellään lyhyesti omissa aliluvuissaan. Molemmissa tapauksissa laskusääntöjä selventää vertaaminen edellisen luvun kuvaan 1. Yhteenlaskun yhteydessä käsitellään myös vähennyslasku, jota tarvitaan tietyissa pisteiden kertolaskun toteutuksissa. Lisäksi esitellään kummankin äärellisen kunnan vaikutus elliptisen käyrän parametreihin. [Cer00]

3.1 Alkulukukunnat

Alkulukukuntien laskuoperaatiot hyödyntävät moduloaritmetiikkaa. Aihe voitaneen kuitenkin olettaa niin hyvin tunnetuksi, ettei sen tarkempaa määrittelyä tarvita.

Elliptisen käyrän yhtälöksi yli alkulukukunnan F_p on valittu $y^2 \bmod p = x^3 + ax + b \bmod p$, missä $4a^3 + 27b^2 \bmod p \neq 0$. Tämän äärellisen kunnan elementit ovat, ja siinä määritellyt laskuoperaatiot käsittelevät, kokonaislukuja väliltä 0 ja $p - 1$; alkuluku p puolestaan on valittu siten, että elliptisellä käyrällä on riittävän suuri määrä pisteitä takaamaan salausjärjestelmän turvallisuus.

Elliptisen käyrän parametrit yli alkulukukunnan F_p ovat p, a, b, G, n ja h; p on kunnalle määritetty alkuluku, a ja b määräävät käyrän yhtälön, $G = (x_a, y_a)$ on käyrältä valittu generoiva piste, ja n on käyrän asteluku. Lisäksi $\#E(F_p)$ on käyrällä sijaitsevien pisteiden määrä, ja h on pisteiden määrän suhde käyrän astelukuun.

3.1.1 Pisteiden yhteen- ja vähennyslasku

Olkoot kaksi pistettä P ja Q sellaiset, että $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ ja $P \neq Q$. Määritellään lisäksi vasta-alkio $-Q = (x_Q, -y_Q \bmod p)$. Haluttu summapiste $R = (x_R, y_R) = P + Q = Q + P$ saadaan kaavoista

$$x_R = s^2 - x_P - x_Q \bmod p \tag{2}$$

$$y_R = -y_P + s(x_P - x_R) \bmod p \tag{3}$$

$$s = \frac{y_P - y_Q}{x_P - x_Q} \bmod p \tag{4}$$

joissa s on pisteiden P ja Q kautta kulkevan suoran kulmakerroin. Mikäli $P = -Q$, on $P + Q = \infty$, ja mikäli $P = Q$ eli $P + Q = 2P$, käytetään pisteen kahdella kertomisen kaavoja.

Vähennyslaskun tapauksessa otetaan käyttöön edellä määritelty vasta-alkio, jonka avulla saadaan haluttu $P - Q = P + (-Q)$.

3.1.2 Pisteen kertominen kahdella

Olkoon piste P sellainen, että $P = (x_P, y_P)$ ja $y_P \neq 0$. Haluttu tulopiste $R = (x_R, y_R) = 2P$ saadaan kaavoista

$$x_R = s^2 - 2x_P \bmod p \tag{5}$$

$$y_R = -y_P + s(x_P - x_R) \bmod p \tag{6}$$

$$s = \frac{3x_P^2 + a}{2y_P} \bmod p \tag{7}$$

joissa s on elliptisen käyrän tangentti pisteessä P ja a on yksi tälle käyrälle valituista parametreista. Mikäli $y_P = 0$, on $2P = \infty$.

3.2 Binäärikunnat

Elliptisen käyrän yhtälöksi yli binäärikunnan F_2^m on valittu $y^2 + xy = x^3 + ax^2 + b$, missä $b \neq 0$. Tämän äärellisen kunnan elementit ovat korkeintaan m bittiä pitkiä kokonaislukuja. Niitä voidaan pitää asteen $m-1$ binäärisinä polynomeina; kunnassa määritellyt laskuoperaatiot käsittelevät korkeintaan astetta $m-1$ olevia polynomeja. Myös luku m on valittu siten, että elliptisellä käyrällä on riittävän suuri määrä pisteitä takaamaan salausjärjestelmän turvallisuus.

Elliptisen käyrän parametrit yli binäärikunnan F_2^m ovat m, $f(x)$, a, b, G, n ja h; m on kunnan määräävä kokonaisluku, $f(x)$ on polynomiaritmetiikassa käytettävä jaoton polynomi, a ja b määräävät käyrän yhtälön, $G = (x_a, y_a)$ on käyrältä valittu generoiva piste, ja n on käyrän asteluku. Lisäksi $\#E(F_2^m)$ on käyrällä sijaitsevien pisteiden määrä, ja h on pisteiden määrän suhde käyrän astelukuun.

Ennen binäärikunnille muokattujen laskusääntöjen esittelyä tutustutaan lyhyesti polynomiaritmetiikkaan, sillä se on jonkin verran moduloaritmetiikkaa vieraampaa ja monimutkaisempaa.

3.2.1 Polynomiaritmetiikka

Käsitellään siis korkeintaan astetta $m-1$ olevia binäärisiä polynomeja. Niiden kertoimet ovat joko ykkösiä tai nollia, eli esimerkiksi 4-bittinen binäärijono 1011_2 on polynomin $x^3 + x + 1$ binääriesitysmuoto. Moduloaritmetiikan modulo p:tä vastaa astetta m oleva jaoton polynomi - niinkutsuttu *vähennyspolynomi* - jota ei voi esittää kahden alempaa astetta olevan polynomin tulona; mikäli jokin laskutoimitus tuottaa yli astetta $m-1$ olevan polynomin, vähennyspolynomia käytetään vähentämään sen aste alle m:n - siis aivan kuten moduloa käytetään alkulukukuntien yhteydessä.

Polynomien yhteen- ja vähennyslasku ovat binäärikunnissa sama laskutoimitus, joka saadaan aikaan yksinkertaisesti lukujen XOR-bittioperaatiolla. Polynomilla A on vähennyspolynomin $f(x)$ suhteen käänteinen polynomi A^{-1} siten, että $A * A^{-1} \pmod{f(x)} = 1$. Polynomien kertolasku suoritetaan normaalisti, mutta sen lisäksi saatu tulos vähennetään alle asteen m:

$$1101_2 * 0110_2 = 101110_2 \tag{8}$$

$$f(x) = 10011_2 \tag{9}$$

$$101110_2 \bmod 10011_2 = 1000_2 \tag{10}$$

Tarkempi kuvaus vähennyspolynomin $f(x)$ käytöstä modulona sivuutetaan; kyseessä on periaatteessa polynomin jakaminen $f(x)$:llä siten, että tuloksesta poistuvat kaikki yli astetta $m-1$ tai kerrointa 1 olevat termit. Jäljelle jää haluttua muotoa oleva binäärinen polynomi.

Polynomien jakolasku voidaan edellä määritellyn käänteispolynomin avulla palauttaa kertolaskun määritelmään.

3.2.2 Pisteiden yhteen- ja vähennyslasku

Olkoot kaksi pistettä P ja Q sellaiset, että $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ ja $P \neq Q$. Määritellään lisäksi vasta-alkio $-Q = (x_Q, x_Q + y_Q)$. Haluttu summapiste $R = (x_R, y_R) = P + Q = Q + P$ saadaan kaavoista

$$x_R = s^2 + s + x_P + x_Q + a \tag{11}$$

$$y_R = s(x_P + x_R) + x_R + y_P \tag{12}$$

$$s = \frac{y_P + y_Q}{x_P + x_Q} \tag{13}$$

joissa s on pisteiden P ja Q kautta kulkevan suoran kulmakerroin ja a on yksi käyrälle valituista parametreista. Mikäli $P = -Q$, on $P + Q = \infty$, ja mikäli $P = Q$ eli $P + Q = 2P$, käytetään pisteen kahdella kertomisen kaavoja.

Vähennyslaskun tapauksessa otetaan käyttöön edellä määritelty vasta-alkio, jonka avulla saadaan haluttu $P - Q = P + (-Q)$.

3.2.3 Pisteen kertominen kahdella

Olkoon piste P sellainen, että $P = (x_P, y_P)$ ja $x_P \neq 0$. Haluttu tulopiste $R = (x_R, y_R) = 2P$ saadaan kaavoista

$$x_R = s^2 + s + a \tag{14}$$

$$y_R = x_P^2 + (s + 1) * x_R \tag{15}$$

$$s = \frac{x_P + y_P}{x_P} \tag{16}$$

joissa s on elliptisen käyrän tangentti pisteessä P ja a on yksi käyrälle valituista parametreista. Mikäli $x_P = 0$, on $2P = \infty$.

4 Elliptisen käyrän salausjärjestelmä

Luottamus elliptisen käyrän salausmenetelmiin perustuu paljolti uskoon diskreetin logaritmin ongelman vaativuudesta elliptisten käyrien tapauksessa; teoreettista todistusta asiasta ei ole kyetty yli 30 vuodessa muodostamaan. Toisaalta se, ettei ongelmaan myöskään ole löydetty tehokasta ratkaisualgoritmia, lujittaa uskoa elliptisen käyrän salausjärjestelmiin. [Han04]

Tässä luvussa esitellään aluksi diskreetin logaritmin ongelma suhteessa elliptisiin käyriin, seuraavaksi tutustutaan elliptisen käyrän salaukseen viestin alkuperän varmistamisen ja avainten vaihdon kannalta, ja lopulta esitellään eräs elliptisen käyrän salauksen mahdollisista sovellusalueista - älykortit.

4.1 Diskreetin logaritmin ongelma

Klassisessa diskreetin logaritmin ongelmassa halutaan löytää yhtälön $x = g^k \pmod p$ toteuttava kokonaisluku k, kun yhtälön muut tekijät tunnetaan. Kappaleessa 2 kuvatut laskuoperaation mahdollistavat ongelman määrittämisen myös elliptisille käyrille, sillä eksponentin ottaminen voidaan korvata skalaarilla kertomisella.

Määritelmä: Olkoot P ja Q elliptisen käyrän E pisteitä. Halutaan löytää yhtälön $Q = kP(= P+P+...+P)$ toteuttava, aidosti E:n astelukua pienempi kokonaisluku k, kun tunnetaan P ja Q. Haettu k tunnetaan myös Q:n diskreettinä logaritmina kannassa P; sen ollessa riittävän suuri, ongelmaa pidetään laskennallisesti liian vaativana. [Tra04]

Elliptisten käyrien kohdalla ongelman uskotaan olevan olennaisesti vaikeampi kuin alkuperäisessä määrittelyssään - johtuen juuri äärellisten kuntien yhteydessä esitetystä tavasta kertoa piste P skalaarilla k. Kuitenkaan sen vaativuutta ei ole kyetty teoreettisesti todistamaan. Ongelman ei tiedetä olevan NP-kova, ja koska sen päätösversio tunnetusti kuuluu vaativuudeltaan sekä luokkaan NP että *co-*NP, ei todistusta NP-kovuudesta edes pidetä odotettavana; sellaisen löytyminen merkitsisi, että NP = *co-*NP. Koska ongelma ei välttämättä edes ole NP-kova, ei polynomiaikaisen ratkaisualgoritmin löytyminen käsittääkseni kuitenkaan antaisi mitään vastausta vaativuusanalyysin kannalta tärkeään kysymykseen, päteekö $P = NP$. [Han04]

Kuitenkin sekä tehokkaiden ratkaisualgoritmien puuttuminen ongelman pitkäaikaisesta tutkimuksesta huolimatta, että viitteet ongelman *mahdollisesta* NP-kovuudesta ainakin tietyillä rajoitetuilla ryhmillä, antavat molemmat tietyn kuvan ongelman ilmeisestä vaativuudesta.

4.2 Elliptisen käyrän salaus

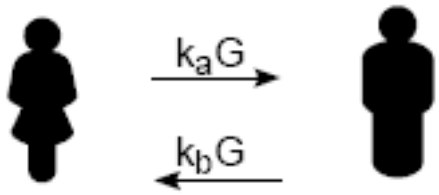
Kaikki elliptiset käyrät eivät takaa salauksen turvallisuutta; esimerkiksi *ylisingulaaristen* elliptisten käyrien kohdalla diskreetin logaritmin ongelmaan on olemassa tehokas

ratkaisualgoritmi. Sopivan käyrän löytäminen on laskennallisesti vaativaa, mutta sitä pidetään saavutetun lyhyemmän avaimenpituuden arvoisena. [Han04]

Tässä artikkelissa elliptisen käyrän salaukseen tutustutaan esittämällä, miten aikaisemminkin tunnettuja salausmenetelmiä on voitu tehostaa määrittelemällä ne elliptisille käyrille. Varsinaista viestin salausta ja salauksen purkamista ei esitetä, vaan rajoitetaan tarkastelu viestin allekirjoittamiseen ja avaimen vaihtoon.

4.2.1 Viestin alkuperän varmistaminen

Allekirjoitusalgoritmeja käytetään, kun halutaan varmuus viestin todellisesta lähettäjästä. Usein käytetyssä esimerkissä Alice allekirjoittaa viestinsä omalla salaisella avaimellaan, ja lähettää sen sitten Bobille viestin mukaan luodun allekirjoituksensa saattelemana. Koska Alicen julkinen avain on yleisessä tiedossa, ja vain sen avulla voi varmistaa vastaavalla salaisella avaimella luodun allekirjoituksen, Bob saa selvyyden sekä viestin aitoudesta että sen todellisesta lähettäjästä.



Kuva 2: Kummankin osapuolen julkiset avaimet ovat yleisessä tiedossa, mutta ne on silti kyettävä välittämään jotakin turvallista, *autentikoitua* kanavaa pitkin.

Digitaalisen allekirjoituksen algoritmista DSA (Digital Signature Algorithm) on kehitetty elliptisiä käyriä hyödyntävä versio ECDSA (Elliptic Curve Digital Signature Algorithm); sen *uskotaan* takaavan saman turvallisuustason kuin DSA, vastaavassa suoritusajassa ja lyhyemmillä avaimen kooilla. Osapuolien on ensin sovittava keskenään elliptisten käyrien tarvitsemat parametrit. Alicen avainpari koostuu sekä salaisesta avaimesta k_A, joka on satunnainen, aidosti elliptisen käyrän E astelukua n pienempi kokonaisluku, sekä julkisesta avaimesta k_AG, missä G on elliptisen käyrän E parametrina määritelty generoiva piste. Jos otetaan huomioon tarvittava parametrien sopiminen, julkiset avaimet ovatkin oikeastaan nelikkoja (E, G, n, kG). [Ayd99]

Alice luo allekirjoituksen lähetettävälle viestille m seuraavasti:

1. Laske $e = H(m)$, missä H on sopiva hajautusfunktio (esim. SHA-1)
2. Valitse satunnaisluku $l \in [1, n-1]$
3. Laske $r = x1 \pmod n$, kun $(x1, y1) = lG$; jos $r = 0$, palaa kohtaan 2
4. Laske $s = l^{-1}(e + k_A r) \pmod n$; jos $r = 0$, palaa kohtaan 2
5. Allekirjoitus on pari (r, s)

Taulukko 1: Allekirjoituksen luonti

Koska Bob tietää Alicen julkisen avaimen $k_A G$, hän voi puolestaan varmistaa saapuneen viestin alkuperän seuraavasti:

1. Varmista, että $r, s \in [1, n-1]$. Jos ei, hylkää allekirjoitus
2. Laske $e = H(m)$ samalla hajautusfunktiolla H
3. Laske $w = s^{-1} \pmod n$
4. Laske $u_1 = ew \pmod n$ ja $u_2 = rw \pmod n$.
5. Laske $(x1, y1) = u_1 G + u_2 * k_A G$
6. Jos $x1 = r \pmod n$, hyväksy allekirjoitus; muuten hylkää se

Taulukko 2: Allekirjoituksen varmistus

4.2.2 Avaimenvaihtoprotokolla

DH (Diffie-Hellman) on usein käytetty protokolla, joka mahdollistaa kahdenkeskisen jaetun salaisen avaimen käyttämisen sellaista edellyttävissä algoritmeissa; osapuolet vaihtavat keskenään julkista tietoa, ja yhdistämällä sen henkilökohtaiseen salaiseen tietoonsa kummatkin pystyvät laskemaan yhteisen salaisen viestin.

Elliptisiä käyriä hyödyntävä versio ECDH (Elliptic Curve Diffie-Hellman) edellyttää luonnollisesti, että osapuolet Alice ja Bob sopivat ensin keskenään elliptisten käyrien tarvitsemat parametrit. Tällä kertaa molemmilla on avainparit, jotka koostuvat salaisesta avaimesta k ja julkisesta avaimesta kG; salaiset avaimet ovat sa-

tunnaisia, aidosti käyrän astelukua n pienempiä kokonaislukuja, ja G on elliptisen käyrän yhteisesti sovittuna parametrina oleva generoiva piste.

1. Alice laskee $K = (x_K, y_K) = k_A * k_B G$
2. Bob laskee $L = (x_L, y_L) = k_B * k_A G$
3. Koska $k_A k_B G = k_B k_A G$, niin $K = L$
4. Yhteinen salaisuus on täten K

Taulukko 3: Avaimen vaihto

Koska pidetään käytännössä mahdottomana johtaa tunnetuista julkisista avaimista niin salaisia avaimia d_A ja d_B kuin yhteistä salaisuuttakaan, ei mikään kolmas osapuoli pääse salakuuntelemaan Alicen ja Bobin jakamia salaisuuksia. [Tra04]

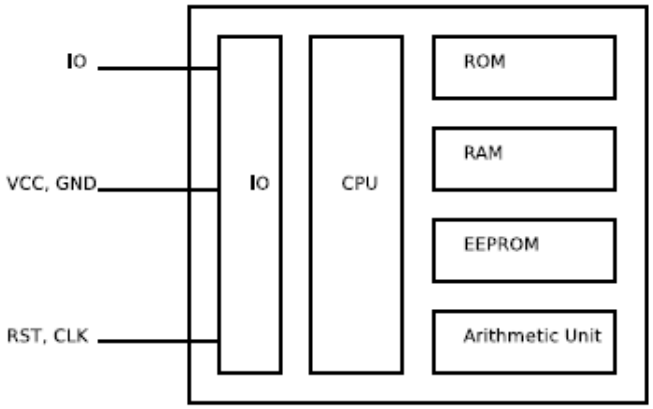
Edellä esitetyssä yhteinen salaisuus määräytyi julkisten ja salaisten avainten mukaan; jos Alice haluaa lähettää salaisesti jonkin tietyn K:n, on protokollaa muokattava seuraavasti:

1. Alice valitsee K:n, laskee $k_A G = k_A K$ ja lähettää sen Bobille
2. Bob laskee $M = k_B * k_A G$ ja lähettää sen Alicelle
3. Alice laskee $N = k_A^{-1} \pmod n M = k_B G$ ja lähettää sen Bobille
4. Bob laskee $K = k_B^{-1} \pmod n N$; nyt molemmat tietävät salaisuuden

Taulukko 4: Avaimen vaihto ennalta valitulla K:n arvolla [Ayd99]

4.3 Sovellusalue: älykortit

Eräs elliptisten käyrien usein mainittuja sovellusalueita on älykortti (smart card). Älykortteja käytetään pääasiallisesti elektronisina maksuvälineinä, mutta myös digitaalisina henkilökortteina ja maksullisten TV-lähetysten purkukortteina. Kaikissa luetelluissa käyttötarkoituksissa luetettavan salauksen - ja erityisesti väärentämättömyyden - tarve on ilmeinen, niin taloudellisista kuin turvallisuuteenkin liittyvistä syistä.



Kuva 3: Älykortin rakenne.

Minkä tahansa salausjärjestelmän sisällyttämistä älykortteihin rajoittavat kuitenkin alhaisena pidettävät valmistuskustannukset, äärimmäiset kokorajoitukset, vähäinen muisti, hidas prosessori sekä käytössä olevat yksinkertaiset ohjelmointikielet. On myös huomattava, että erilliseen virtalähteeseen tukeutuvat älykortit ovat alttiita tietyille hyökkäystyypeille, joita ei perinteisemmässä työasema- ja palvelinympäristön salauksessa ole koskaan tarvinnut huomioida.

5 Hyökkäykset ja niihin varautuminen

Koska elliptisen käyrän salauksen turvallisuudesta ei ole olemassa riittävää teoreettista todistusta, on syytä esitellä joitakin vahvimpia sitä vastaan kohdistettuja hyökkäyksiä; karkeana arviona voidaan sanoa, että minkä tahansa salausjärjestelmän luotettavuus on kääntäen verrannollinen sitä vastaan kehitettyjen hyökkäysten tehokkuuteen.

Paremman tiedon puutteessa on yleensä varminta lähteä oletuksesta, että hyökkääjä tietää salausjärjestelmästä ja sen toteutuksesta kaiken - lukuunottamatta tavoittelemaansa salaista avainta. Lisäksi oletetaan usein, että hyökkääjän käytössä ovat lähes rajattomat resurssit. Tämä onkin välttämätöntä, mikäli salauksen murtaminen edellyttää satojen huipputietokoneiden rinnakkaista laskentaa. Monien sivukanavahyökkäysten toteuttaminen ei kuitenkaan vaadi hyökkääjältä kohtuuttomia investointeja; joidenkin toteuttamiseen riittää pelkkä ajastin, mutta myös oskilloskooppeja ja elektromagneettisia sensoreita on helposti ja taloudellisesti saatavissa.

On selvää, ettei mikään yksittäinen varotoimenpide suojaa kaikilta hyökkäyksiltä. Päinvastoin vaikuttaa pikemminkin siltä, että lähes jokainen hyökkäystyyppi vaatisi erillistä varautumista.

5.1 Suorat hyökkäykset

Elliptisen käyrän diskreetin logaritmin ongelmaan ei ole löydetty tehokasta yleistä ratkaisua; alla esitetyt ratkaisut toimivat hyvin vain tietyillä joukoilla elliptisiä käyriä. Niiden isäksi on mainittava Pollardin ρ -algoritmi, vaikkei sitä käsitelläkään tässä tarkemmin. Toisin kuin esiteltävät deterministiset algoritmit, Pollardin ρ on satunnaisalgoritmi. Sen arvioitu suoritusaika on $O(\sqrt{\pi n}/2)$, missä n on generoivan pisteen P asteluku, ja silti tilantarve on minimaalinen. Vaikka se ei välttämättä palautakaan oikeaa vastausta äärellisessä ajassa, on se silti tehokkain tunnettu algoritmi elliptisiä käyriä vastaan. Tähän vaikuttanee osaltaan se, että algoritmista on kehitetty rinnakkaislaskentaa hyödyntävä versio. Ikävä kyllä tietämykseni ei nykytasollaan täysin riittänyt tämän algoritmin toiminnan tarkempaan ymmärtämiseen. [Han04]

5.1.1 Pohlig-Hellman -hyökkäys

Tämän algoritmin tavoitteena on palauttaa yhtälön $k = \log_P Q$ laskenta diskreettien logaritmien laskemiseen P:n alkulukukertaluvun osajoukoissa. Olkoon P elliptisen käyrän E piste. Oletetaan, että n on pienin yhtälön $nP = \infty$ toteuttava kokonaisluku, ja sen alkulukutekijöihinjako on $n = p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$. Tavoitteena on laskea $k_i = k \pmod{p_i^{e_i}}$ kaikilla $1 \leq i \leq r$, ja sitten ratkaista syntyvät kongruenssit käyttämällä *kiinalaista jäännösteoreemaa* (Chinese Remainder Theorem); se takaa syntyneelle kongruenssien järjestelmälle yksilöllisen ratkaisun k. [Han04]

Esimerkki: Olkoot käyrä $E(F_{7919}) : y^2 = x^3 + 1001x + 75$, $P = (4023, 6036)$ piste käyrällä E ja $Q = (4135, 3169)$ P:n generoima piste; P:n asteluku $n = 7889 = 7^3 23$. Halutaan ratkaista diskreetti logaritmi $k = \log_P Q$. [Han04]

1. Aluksi määritellään $k_1 = k \bmod 7^3 = z_0 + z_1 7 + z_2 7^2$ laskemalla $P_0 = 7^2 23P = (7801, 2071)$ ja $Q_0 = 7^2 23Q = (7801, 2071)$; koska $P_0 = Q_0$, tiedetään että $z_0 = 1$. Edelleen lasketaan $Q_1 = 7 \cdot 23(Q - P) = (7285, 14) = 3P_0$, josta saadaan $z1 = 3$, ja $Q_2 = 23(Q - P - 3 \cdot 7P) = (7285, 7905) = 4P_0$, josta saadaan $z_2 = 4$; on saatu $k_1 = 1 + 3 \cdot 7 + 4 \cdot 7^2 = 218$.

2. Seuraavaksi määritellään $k_2 = k \bmod 23$ laskemalla $P_0 = 7^3P = (7190, 7003)$ ja $Q_0 = 7^3Q = (2599, 759)$; koska $P_0 = 10Q_0$, on saatu $k_2 = 10$.

3. Lopulta ratkaistaan kongruenssit $k = 218 \pmod{7^3}$ ja $k = 10 \pmod{23}$, mistä saadaan $k = 4334$.

Kuten esimerkistä näkee, Pohlig-Hellman -hyökkäys edellyttää onnistuakseen, että n:llä on vain pieniä alkulukutekijöitä; täten hyökkäyksen torjumiseksi riittää valita E ja P siten, että n - eli siis P:n asteluku - on jaollinen mahdollisimman suurella alkuluvulla. [Tra04]

5.1.2 Baby Step, Giant Step -hyökkäys

BSGS-hyökkäyksen ideana on jakaa skalaarikerroin k kahteen osaan, ja suorittaa molemmilla osilla kattava etsintä; algoritmin nimikin viittaa kahteen erilaiseen askeleeseen. On huomattu, että yhtälöstä $k = \log_P Q$ voidaan käytetyn jakoalgoritmin nojalla olettaa $k = jm + i$, missä $0 \leq i < m$. Lasketaan ennalta lista pareja (i, iP) siten, että $0 \leq i < m$, ja järjestetään se jälkimmäisen komponentin mukaan. Edelleen jokaista $0 \leq j < m$ kohti lasketaan $Q - jmP$ ja tarkistetaan, vastaako tulos mitään listan järjestysalkiota; mikäli $Q - jmP = iP$ jollakin i, tästä seuraa, että $Q = (i + jm)P$ ja täten saadaan haluttu $k = jm + i$. [Sab05]

Binäärikenttien tapauksessa kerroin k jaetaan alku- ja loppupään bitteihin siten, että $k = k_{alku} + 2^{\frac{n}{2}}k_{loppu}$, ja törmäystä etsitään joukkojen $Q - k_{alku}P$ ja $2^{\frac{n}{2}}k_{loppu}P$ väliltä, mutta olennaisilta osiltaan menetelmä on sama.

Tämän algoritmin tilantarve on $O(m)$ alkiota sisältävä taulukko, ja sen aikavaativuus on $O(m \log m)$ operaatiota jokaista testattavaa j:n arvoa kohden. Binäärikenttien tapauksessa tilantarpeeksi ilmoitetaan $O(\sqrt{2^n})$, mutta ero tulosten välillä johtunee käytettyjen äärellisten kuntien eroista. Joka tapauksessa on arvioitu, että nykyinen teknologia mahdollistaa tämän algoritmin käytön vain alle astelukua 10^{40} olevien käyräjoukkojen kohdalla. [Sab05, Tra04]

5.2 Sivukanavahyökkäykset

Tyypillisiä ylimääräisen tiedon lähteitä ovat laskentaan kuluva aika, laitteiston virrankulutus ja syntyvä elektromagneettinen säteily. Teoriassa lähteeksi soveltuu mikä tahansa havaittavissa oleva vaihtelu salauslaitteiston toiminnassa, mikäli sen voidaan

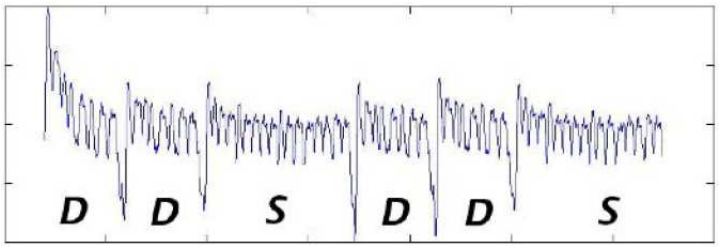
olettaa liittyvän kulloinkin käytettyyn avaimeen tai salattuun viestiin; lisäksi on kyettävä tuottamaan analyysin kannalta riittävästi testiaineistoa. [Han04, Cor99].

Tietyissä toteutusympäristöissä esiintyy luontaisesti paljon salausalgoritmin toimintaan vaikuttavia virheitä; toisaalta virheet saattavat myös olla hyökkääjän keinotekoisesti aikaansaamia. Molemmissa tapauksissa salausalgoritmi saattaa paljastaa hyödynnettävää tietoa itsestään joko oman toimintansa, lähettämiensä virheilmoitusten tai virheen ajallisen sijainnin kautta. Näitä hyökkäyksiä ei esitellä tässä yhteydessä tarkemmin, sillä niistä ei ole osoitettu olevan merkittävää uhkaa. [Han04]

Kokonsa vuoksi älykortit tarvitsevat ulkoista, epäluotettavaa virtalähdettä; tämä heikkous mahdollistaa niiden virrankulutuksen tarkan analysoinnin esimerkiksi korvaamalla älykortin lukulaite omalla, toiminnaltaan vastaavalla mutta haluttuja tietoja keräävällä versiolla. Vastaavina "Troijan hevosina"on aiemmin käytetty esimerkiksi väärennettyjä pankkiautomaatteja. Tosin näissä tapauksessa salainen avain saatiin suoraan kortin omistajan syöttämänä; älykorteissa avain on sisäinen.

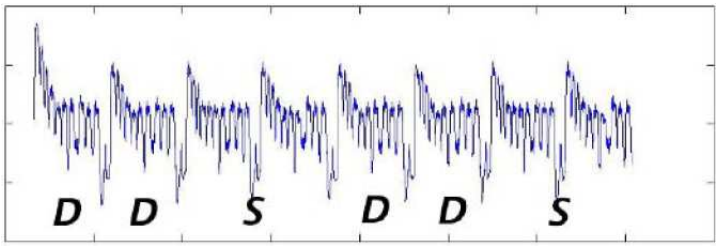
5.2.1 Virrankulutuksen analysointi

SPA (Simple Power Analysis) perustuu oletukseen, että tiettyjen salauksen aikana suoritettavien operaatioiden suoritusjärjestys riippuu jollakin tavalla salaisesta avaimesta, ja että näiden operaatioiden erilainen virrankulutus on havaittavissa virrankulutusta seuraavasta käyrästä. Operaatioiden suorittaminen ehdollisesti voi riippua monestakin salaisen avaimen täyttämästä ehdosta; yleensä salainen avain kuitenkin tulkitaan bittijonona, jossa nolla ja ykkönen vastaavat esimerkiksi elliptisen käyrän yhteenlasku- ja kahdella kertomisoperaatioita. Jos käytössä on yksinkertainen binäärinen pisteiden kertomismetodi, analyysi paljastaa koko salaisen avaimen, ja jos käytössä on esimerkiksi binäärinen NAF-metodi, paljastuu silloinkin merkittävä määrä tietoa salaisen avaimen biteistä. Mainitut laskuoperaatiot tekevät elliptisen käyrän salauksesta erityisen alttiin tämäntyyppiselle hyökkäykselle, sillä niiden virrankulutuksen erot ovat yleensä selvästi havaittavissa. [Han04]



Kuva 4: Virrankulutus suoritettaessa jonoa elliptisen käyrän laskuoperaatioita. S vastaa yhteenlaskua ja D kahdella kertomista.

Kuvan 4 virrankulutuksesta voi selvästi erottaa sen aikaansaaneen operaatiojonon. Mahdollisena vastatoimena voidaan joko muuttaa algoritmia satunnaisemmaksi tai lisätä siihen turhia operaatioita tasoittamaan virrankulutuksessa näkyviä eroja [Möl01]. Kuva 5 sisältää saman operaatiojonon virrankulutuksen suojatulla algoritmilla.

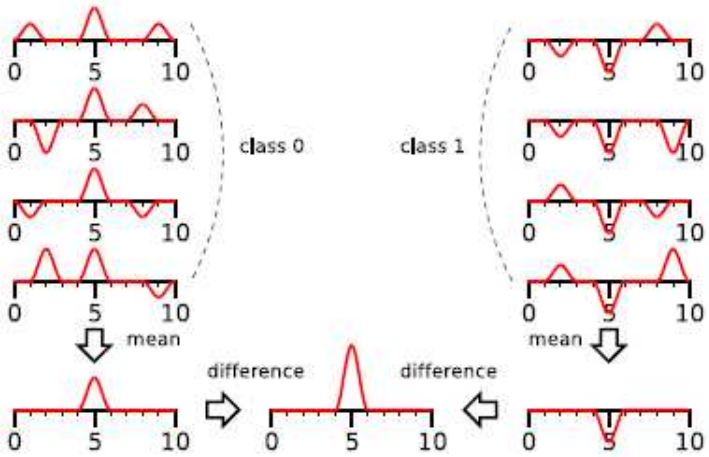


Kuva 5: Virrankulutus suoritettaessa jonoa elliptisen käyrän laskuoperaatioita. S vastaa yhteenlaskua ja D kahdella kertomista, mutta nyt niiden välistä eroa on huomattavasti vaikeampi havaita.

Salausoperaatioiden analyysin sijaan DPA (Differential Power Analysis) seuraa käsiteltyjen muuttuja-arvojen kanssa korreloivia vaihteluita virrankulutuksessa. Nämä erot ovat yleensä huomattavasti pienempiä kuin SPA:han liittyvät, ja ne saattavat jopa peittyä taustakohinan ja mittausvirheiden alle; tästä johtuen kerätään selvästi suurempi määrä virrankulutustietoa - muutama tuhat ajoa, riippuen kuitenkin salausavaimen koosta - ja kerätyn tiedon analyysiin sovelletaan tilastollisia menetelmiä.

Valitaan seurattavaksi jokin salausoperaatioihin liittyvä sisäinen muuttuja V - esimerkiksi yksittäinen bitti - jonka arvoon vaikuttaa tieto viestistä m ja tuntemattoman salaisen avaimen k osasta k'. Yhdessä nämä muodostavat valintafunktion $V = f(k', m)$; tämän perusteella tehdään arvauksia arvon k' suhteen, ositetaan kerätyt virrankulutustiedot kahteen luokkaan arvon V mukaan, otetaan molemmista luokista keskiarvot, ja lopuksi vertaillaan keskiarvojen eroja. Tämä menetelmä elimi-

noi tarkkailusta virrankulutustiedoille yhteisen vakio-osan, joten jäljelle jäävät erot selittyvät arvon k' suhteen tehdyllä arvauksella. Menetelmää toistamalla saadaan selville yhä suurempi osa salaisesta avaimesta k. [Cor99]



Kuva 6: Usean mitatun virrankulutuskäyrän yhdistäminen valitun luokittelutekijän mukaan. Keskiarvojen käyttäminen eliminoi taustakohinan ja muut vakiotekijät, joten ideaalitilanteessa jäljelle jäävät vain aidot erot luokkien välillä.

Jo esitetyn kaltaiset muutokset algoritmiin tehoavat myös DPA-hyökkäystä vastaan. Kummassakaan tapauksessa vastatoimien tehokkuudesta ei ole takuita, eivätkä ne myöskään suojaa muilta sivukanavahyökkäyksiltä. On todistettu, etteivät esitetyt muutokset vaikuta merkittävästi algoritmien suoritusaikoihin. Kuitenkin niiden suoritusaikainen tilantarve ja käytettyyn ohjelmointikieleen kohdistuvat vaatimukset epäilemättä kasvavat; tällä on merkitystä erityisesti älykorttien ja muiden rajallisten resurssien suoritusalustojen kannalta.

6 Yhteenveto

Elliptiset käyrät eivät varsinaisesti ole uudistaneet käyttämiämme salausmenetelmiä, mutta ne ovat tarjonneet mahdollisuuden toteuttaa tunnetut menetelmät turvallisemmin; toisin sanoen menetelmät voidaan toteuttaa yhtä turvallisesti kuin ennenkin, mutta *käyttäen lyhyempiä avaimia*. Näin ainakin uskotaan, sillä teoreettista todistusta perustana olevan elliptisen käyrän diskreetin logaritmin ongelman vaativuudesta ei ole löydetty. Toisaalta elliptisen käyrän salausoperaatio vie enemmän

aikaa, kun ottaa huomioon laskennallisesti vaativan etsinnän salaukseen soveltuvan elliptisen käyrän löytämiseksi.

On mielenkiintoista, että elliptiset käyrät yhdistetään alan kirjallisuudessa usein juuri älykortteihin; molemmat ovat omalla tavallaan alttiita virrankulutusanalyysin kaltaisille hyökkäyksille, joten niiden yhdistäminen tuntuisi jo tämän vuoksi huonolta ajatukselta. Älykorttien asettamat laitteistorajoitukset hankaloittavat esitettyjen vastatoimien toteuttamista tällä nimenomaisella alustalla, eikä vastatoimien tehokkuudestakaan ole esittää takuita.

Lähteet

Ayd99 Aydos, M., Savaş, E. ja Koç, c. K., Implementing network security protocols based on elliptic curve cryptography. *Proc. of the 4th Symposium on Computer Networks*, Oktuğ, S., Orencik, B. ja Harmancı, E., toimittajat, Istanbul, Turkki, toukokuu 1999, sivut 130–139.

Cer00 Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic curve cryptography, version 1.0, 2000. `http://www.secg.org/download/aid-385/sec1_final.pdf`

Cor99 Coron, J.-S., Resistance against differential power analysis for elliptic curve cryptosystems. *International Workshop on Cryptographic Hardware and Embedded Systems - CHES '99*, 1717, sivut 292–302.

Möl01 Möller, B., Securing elliptic curve point multiplication against side-channel attacks. *Information Security - ISC '01*, 2200, sivut 324–334.

Han04 Menezes, A., Vanstone, S. ja Hankerson, D., *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York, 2004.

Sab05 Sabaté, M. M., Elliptic curve cryptography: A software perspective, 2005. `http://www.math.uiuc.edu/~mmasdeu2/entrega/pfc.pdf`

Tra04 Trappe, W. ja Washington, L. C., *Introduction to Cryptography with Coding Theory (2nd edition)*. Prentice Hall, 2005.