Elliptisten käyrien kryptosysteemejä

18. helmikuuta 2014

Aloitetaan määrittelemällä *elliptisten käyrien diskreetin logaritmin ongelma*: Annettu pisteet P ja $Q = kP$ elliptisellä käyrällä E kunnassa $\mathbb{Z}_p$. Määritettävä k.

Tämä ongelma on tunnetusti erittäin haastava.

Hasse on todistanut, että elliptisellä käyrällä kunnassa $\mathbb{Z}_p$ on suurinpiirtein $p+1$ pistettä. Tarkka muotoilu on seuraavanlainen:

Lause 1. *Olkoon N_p elliptisen käyrän E pisteiden määrä (mukaanlukien äärettömyyspiste) kunnassa $\mathbb{Z}_p$. Nyt*

$$p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p}.$$

Elliptisen käyrän pisteen P *kertaluku* on n, mikäli

$$nP = O = \infty,$$

mutta $mP \neq O$ kaikilla positiivisilla $m < n$.

1 ElGamal elliptisillä käyrillä

Jokainen käyttäjä, joka haluaa ottaa vastaan kryptattua dataa, generoi ensin avaimen toimimalla seuraavasti: Valitaan alkuluku p, elliptinen käyrä $E \pmod p$, ja siltä pisteet P ja $kP = Q$, missä $k \in [2, p-2]$ on salainen avain. Julkistetaan (p, P, Q). Tämä kolmikko muodostaa julkisen avaimen. (Huomaa, että tällä datalla on jo selvitettävissä käyrä E!)

Näin tätä käytetään kryptaamiseen:

Alice haluaa lähettää Bobille viestin. Bobin julkinen avain on (p, P, Q), ja Bobilla on salainen avain k, ja lisäksi Alicella on tiedossaan miten eri pisteen Bobin elliptisellä käyrällä vastaavat eri viestejä (eli jokin tulkinta pisteiden merkityksestä on oltava).

Alicen viestiä vastaava piste Bobin käyrällä on R. Nyt Alice valitsee satunnaisen luvun $a \in [2, p-2]$, ja laskee pisteet aP ja $R + aQ$, ja hän lähettää nämä Bobille.

Bobin on suoraviivaista purkaa kryptaus, sillä hänen pitää vain laskea:

$$R + aQ - baP = R + abP - baP = R.$$

2 Diffie-Hellman elliptisillä käyrillä

Alice ja Bob tarvitsevat yhteisen salasanan, ja heillä on käytössä kommunikointiin vain julkinen kanava (Hesarin etusivu, ilmoitustaulu, jne). Diffie-Hellman on melkein samanlainen elliptisillä käyrillä kuin muutenkin, eli:

1. Sovitaan yhteisesti iso alkuluku p, elliptinen käyrä $E \pmod p$ ja käyrältä piste P.
2. Alice valitsee luvun a ja Bob valitsee luvun b. Alice laskee luvun $Q_a = aP \pmod p$ ja Bob laskee luvun $Q_b = bP \pmod p$.
3. Alice julkistaa luvun Q_a ja Bob julkistaa luvun Q_b.
4. Alise laskee luvun aQ_b ja Bob laskee luvun bQ_a. Koska $aQ_b = abP$ ja $bQ_a = baP$, niin yhteiseksi salasanaksi voidaan valita $Q = aQ_b = bQ_a$.

3 Digitaalinen allekirjoitus elliptisillä käyrillä

Lähtökohta: Alice haluaa lähettää allekirjoitetun viestin m Bobille.

3.1 Kuinka allekirjoitetaan?

Allekirjoitussysteemin pystyyn pistäminen: Alice ja Bob valitsevat elliptisen käyrän E modulo alkuluku p. Valitaan käyrältä generaattori G (eli ikäänkuin primitiviinen juuri, eli sellainen piste, jonka monikertana kaikki pisteet saadaan) ja olkoon n pisteen G kertaluku. Oletetaan vielä lisäksi, että luku n on alkuluku. Nämä kaikki parametrit ovat siis Alicen että Bobin tiedossa.

Alice valitsee positiivinen luvun $d \leq n - 1$, joka on salainen, ja laskee $Q = dG$, ja julkistaa pisteen Q.

Nyt päästään varsinaiseen allekirjoitukseen.

Alice käyttää kryptografista hash-funktiota. (Kryptografinen hash-funktio on funktio, joka antaa jokaiselle viestille jonkin arvon, ja joka toteuttaa ehdot: Viestin arvo on helppo laskea. Annetulle arvolle ei voi järkevästi laskea viestiä. Jos viestiä muutetaan, niin arvo muuttuu. Kahdella viestillä ei ole samaa arvoa.) Olkoon f kyseinen funktio. Alice laskee

$$e = f(m),$$

missä e on jokin luku. Huom! Myös Bob on tietoinen tästä funktiosta!

Olkoon L_n luvun n pituus binäärijärjestelmässä. Olkoon z se luku, joka saadaan, kun luvusta e otetaan L_n bittiä vasemmalta lähtien (nämä otetut bitit siis muodostavat luvun z). Nämäkin kaikki arvot Bob pystyy helposti laskemaan.

Tästä eteenpäin pidetään laskut salassa, kunnes lopulta allekirjoitus lähetetään Bobille. Valitaan satunnainen positiivinen kokonaisluku $k \leq n-1$, ja lasketaan elliptiseltä käyrältä piste $kG = (x, y)$. Redusoidaan x modulo n, eli määritetään sellainen x', että $x \equiv x'$

(mod n) ja $0 < x' \leq n-1$. Mikäli $x' = 0$, niin suoritetaan luvun k valinta uudelleen ja lasketaan piste (x, y) uudelleen niin monta kertaa, että $x' \neq 0$. .

Lasketaan $s \equiv k^{-1}(z + xd)$ ja redusoidaan: $s' \equiv s \pmod{n}$ ja $0 \leq s' \leq n-1$. Mikäli $s' = 0$, niin valitaan k uudelleen niin monta kertaa, että saadaan sellainen k, että $x' \neq 0$ ja $s' \neq 0$.

Allekirjoitus on pari (x', s').

3.2 Kuinka allekirjoitus verifioidaan?

Allekirjoituksessa on kovin vähän järkeä, jos sitä ei voi verifioida. Käydään siis seuraavaksi verfiointi läpi.

1. Onko allekirjoitus päällisin puolin kunnossa, eli päteekö $0 < x', s' \leq n-1$ ja ovathan luvut x' ja s' kokonaislukuja?
2. Bob laskee $e = f(m)$, kuten Alicekin laski.
3. Bob määrittää luvun z samoin kuin Alicekin.
4. Bob laskee $w = s'-1 \pmod{n}$.
5. Bob laskee luvut t ja u: $t \equiv zw \pmod{n}$ ja $u \equiv x'w \mod n$.
6. Bob laskee käyrän pisteen $(x'', y'') = tG + uQ$.
7. Mikäli $x'' \equiv x' \pmod{n}$, niin allekirjoitus on kunnossa.

3.3 Miksi tämä toimii?

Huomaa, että

$$tG + uQ = zwG + dx'wG = w(z + dx')G \equiv s^{-1}(z + dx')G \equiv \left(k^{-1}(z + xd)\right)^{-1}(z + dx')G.$$

Koska $x' \equiv x \pmod{n}$, niin $(z + xd)^{-1}(z + x'd) \equiv 1 \pmod{n}$, joten

$$\left(k^{-1}(z + xd)\right)^{-1}(z + dx')G \equiv kG \pmod{n}.$$

Toisaalta luvusta x' tiedetään, että

$$(x', y) \equiv (x, y) = kG \pmod{n},$$

joten mikäli allekirjoitus on kunnossa, saa Bob verifioiduksi, että allekirjoitus on oikea.