Avaimenvaihto – Blomin järjestelmä

LuK-tutkielma
Saana Riekki
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2022

Sisällys

Johdanto

Avaimenvaihdossa luotettava auktoriteetti on vastuussa käyttäjien identiteettien varmistamisesta, sertifikaattien myöntämisestä sekä avainten valitsemisesta ja lähettämisestä käyttäjille. Avaintenvaihto voidaan toteuttaa ennakkojakona, yksittäisen istunnon avainjakona tai sopimuksilla avaimista. Avaimenjakoja on erilaisia, kuten esimerkiksi Blomin järjestelmä, joka esitellään tässä tutkielmassa.

Tässä tutkielmassa esitellään avaimenvaihto yleisesti sekä perehdytään Blomin järjestelmään. Blomin järjestelmästä tarkastellaan erikseen erityistä Blomin järjestelmän mallia, jossa turvallisuusparametri saa arvon yksi sekä Blomin järjestelmän yleistä tapausta. Tutkielmassa perehdytään myös ulkopuolisiin hyökkäyksiin sekä Blomin järjestelmän turvallisuuteen.

Tutkielmassa on käytetty pääasiallisena lähteenä teosta Stinson, Douglas ja Paterson, Maura: Cryptography – Theory and Practice, CRC Press 2019. [1].

1 Esitietoja

Tässä kappaleessa esitetään käsitteitä ja lauseita, jotka ovat oleellisia avaimenvaihtoon liittyen. Eri käsitteet ja lauseet voivat liittyä joko yleisesti avaimenvaihtoon tai vaihtoehtoisesti Blomin järjestelmään sekä siihen liittyvien lauseiden todistamiseen.

Määritelmä 1.1. (Alkuluku). *Alkuluku* on kokonaisluku p, jolle pätee $p \geq 2$ ja joka on jaollinen vain itsellään ja luvulla 1.

Määritelmä 1.2. (Kongruenssi). *Kongruenssissa* kokonaisluku a on kongruentti luvun b kanssa modulo n, kun lukujen a ja b erotus on jaollinen luvulla n. Tämä merkitään

$$a \equiv b \pmod{n}.$$

Tällöin kongruenttius voidaan esittää myös muodossa

$$\frac{a-b}{n} = k,$$

jossa $k \in \mathbb{Z}$.

Määritelmä 1.3. (Lineaarinen polynomi). *Lineaarisen polynomin* koordinaatistoon piirretty kuvaaja on suora. Näin ollen lineaarista polynomia kuvaava lineaarinen funktio on joko ensimmäisen asteen polynomi tai pelkkä vakio.

Määritelmä 1.4. (Lineaarinen interpolointi). *Lineaarisen interpoloinnin* mukaan voidaan olettaa, että funktio on kahden erillisen pisteen välissä aina lineaarinen.

Määritelmä 1.5. (Summa). *Summaa* merkitään käyttäen merkintää $\sum$. Summakaavoja käyttäessä summa esitetään muodossa

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n,$$

jossa i on summausindeksi. Tällainen summa voidaan lausua muodossa "summa x_i:stä, kun i on luvut 1:stä n:nään".

Määritelmä 1.6. (Tulo). *Tulo* merkitään käyttäen merkintää $\prod$.Tulokaavoja käyttäessä tulo esitetään muodossa

$$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot \cdots \cdot x_n,$$

jossa i on tuloindeksi. Tällainen tulo voidaan lausua muodossa "tulo x_i:stä, kun i on luvut 1:stä n:nään".

Määritelmä 1.7. (Symmetrinen polynomi). *Symmetrinen polynomi* on polynomi, joka pysyy muuttumattomana, vaikka polynomin muuttujien paikkaa vaihdettaisiin. Kahden muuttujan symmetriselle polynomille pätee siis $f(x,y) = f(y,x)$.

2 Avaimenvaihto

Tässä kappaleessa esitellään avaimenvaihto yleisesti pohjautuen lähteeseen [1]. Kappaleessa esitellään avaimenvaihdon perusasiat, kuten avainten jakaminen salausjärjestelmään kuuluville henkilöille sekä luotettavan auktoriteetin eli TA:n osuus avaimenvaihdossa.

Avaimenvaihdossa tärkein henkilö TA valitaan salausjärjestelmään kuuluvien kesken niin, että TA on luotettava auktoriteetti. Luotettavan auktoriteetin tehtävänä on eri avaimenvaihtosalauksissa jakaa salausavaimet eri osapuolille kullekin salaustyypille ominaisella tavalla sekä tarkistaa salausjärjestelmiin osallistuvien henkilöiden identiteetit.

Avainten ennakkojakelussa luotettava auktoriteetti TA jakaa informaation avaimista etukäteen valitulla salaisella alustalla niin, että tietoja voi luovuttaa turvallisesti eri osapuolille. Avainten sisältämän tiedon avulla salausjärjestelmään kuuluvat henkilöt voivat myöhemmin salata tietoja sekä avata saamiaan viestejä. Salaisten avainten tietoja voidaan käyttää myös salattujen viestien allekirjoitukseen. Salausjärjestelmään kuuluvat henkilöt voivat määrittää keskenään uusia avaimia, jotka ovat vain heidän tiedossaan. Näillä salaisilla avaimilla henkilöt voivat kommunikoida keskenään salaisesti ilman, että muut salausjärjestelmään kuuluvat pystyvät avaamaan viestejä.

Istuntoavainten jakelussa kaikilla osapuolilla on etukäteen jaetut salaiset avaimet, jotka ovat luotettavan auktoriteetin tiedossa. Luotettava auktoriteetti jakaa käyttäjille väliaikaisen istuntoavaimen, käyttäjän pyytäessä sellaista. Istuntoavaimen TA salaa käyttäjän oman salaisen avaimen avulla. Istuntoavaimia käytetään yksittäisissä lyhyissä jaksoissa viestien salaamiseen, ja kun henkilö tarvitsee uuden avaimen, hän voi pyytää sellaisen taas TA:lta.

On olemassa myös avaimenvaihtojärjestelmiä, joissa luotettavaa auktoriteettia ei tarvita. Tällainen on erimerkiksi avaintensopimisjärjestelmä. Avaintensopimisessa salausjärjestelmään kuuluva käyttäjäpari käyttää interaktiivista protokollaa muodostaakseen oman istuntoavaimensa.

2.1 Ulkopuoliset hyökkääjät

Avaimenvaihdossa tulee aina huomioida mahdolliset ulkopuoliset hyökkääjät ja niiden aiheuttamat haitat. Ulkopuolisten hyökkääjien lisäksi on aina myös huomioitava mahdollisuus siitä, että joku salausjärjestelmässä mukanaolevista henkilöistä onkin hyökkääjä. Hyökkääjien huomioimisen tärkeä keino on tiedostaa mahdollisen hyökkääjän tavoitteet sekä keinot, joilla tavoitteeseen pääseminen olisi mahdollista. Avaimenvaihdossa käytetään usein internettiä ja sen erilaisia alustoja. Nämä alustat eivät ole täysin turvallisia hyökkääjien varalta.

Ulkopuolista hyökkääjää voidaan kutsua joko aktiiviseksi tai passiiviseksi hyökkääjäksi, riippuen sen toimintatavoista ja -malleista. Passiiviseksi hyökkääjäksi kutsutaan sellaista henkilöä, joka keskittyy hiljaisesti eli passiivisesti tiedon keräämiseen muiden lähettämien viestien perusteella. Aktiivinen hyökkääjä taas pyrkii aktiivisesti keräämään tarvitsemaansa tietoa esimerkiksi tallentamalla muiden lähettämiä viestejä itselleen tai esiintymällä useampana verkon käyttäjänä samanaikaisesti.

Aktiivisen hyökkääjän tavoitteena voi olla esimerkiksi määrittää uusia avaimia tai käyttää jo poistuneita avaimia ja saada muut järjestelmään kuuluvat henkilöt uskomaan, että ne ovat todellisia avaimia, tai saada käyttäjät uskomaan, että he ovat vaihtaneet avaimia keskenään, vaikkeivat todellisuudessa ole. Passiivinen hyökkääjä taas voi pyrkiä selvittämään vaihtuvien avainten avulla käyttäjien salaisia elementtejä ja näin koittaa ratkaista uudet avaimet ja lopulta viestien sisältö.

Hyökkääjän toimia voi estää esimerkiksi vaihtamalla käyttäjien välisiä avaimia tarpeeksi usein, jolloin hyökkääjän on aloitettava avaimen tietojen selvittäminen alusta. Hyökkääjän tietäessä yksittäisiä istuntoavaimia, voidaan lähetettävät viestit pitää salaisina vielä pitkäaikaisten avaimien avulla. Jos käyttäjien pitkäaikaiset avaimet tulevat hyökkääjän tietoon, on salausten murtaminen helpompaa. Tällaista tilannetta kutsutaankin katastrofaaliseksi hyökkäykseksi.

3 Blomin järjestelmä

Tässä kappaleessa käsitellään Blomin järjestelmää, joka on eräs avaimenvaihdon salausjärjestelmistä. Blomin järjestelmään liittyen kerrotaan avainten valinnasta sekä käyttäjien välisestä kommunikoinnista. Kappaleessa käsitellään myös Blomin järjestelmän turvallisuutta ja salausten murtamista. Kappaleissa 3.1 ja 3.2 on käytetty pääasiallisena lähteenä teosta [1].

3.1 Avaimen valinta ja tekstin salaaminen

Blomin järjestelmässä avaimenvaihtotyylinä käytetään avainten ennakkojakelua. Valittu luotettava auktoriteetti valitsee kaikille salausjärjestelmään kuuluville käyttäjäpareille $\{U,V\}$ satunnaisen avaimen, jolle pätee $K_{U,V} = K_{V,U}$. TA jakaa valitsemansa avaimen käyttäjille salaista kanavaa pitkin. Avainten jaossa voi olla ongelmana se, että TA:n tulee jakaa salaisesti yhteensä $\binom{n}{2}$ avainta, kun salausjärjestelmään kuuluvat henkilöt tallentavat $(n-1)$ avainta. Tätä kutsutaan n^2-ongelmaksi. Ongelma syntyy siitä, että usein salauksissa on turvallista käyttää suurta lukua n, jotta salausten murtaminen on mahdollisimman vaikeaa. Kuitenkin tällöin, kun salausjärjestelmään kuuluvat henkilöt joutuvat tallentamaan $(n-1)$ avainta, tallennustilaa tarvitaan todella paljon. Salaisten avainten kokonaismäärä salausjärjestelmässä on $\binom{n}{2}$ ja se kasvaa koko ajan n:n neliönä.

Blomin järjestelmää käytetään saavuttamaan tilanne, jossa n^2-ongelmasta ei tarvitsisi välittää. Blomin järjestelmässä salausjärjestelmään kuuluvat henkilöt $\{U,V\}$ voivat sopia salaisista avaimista keskenään, jolloin liialliselta avainten tallentamiselta säästytään.

TA valitsee ensin luvun k. Nyt TA valitsee alkuluvun p, jonka hän määrittää julkiseksi kaikille salausjärjestelmään kuuluville. TA lähettää käyttäjille $k+1$ alkiota, joille pätee $k+1 \in \mathbb{Z}_p$. Yksi Blomin järjestelmän yleisimmistä muodoista on niin kutsuttu erityinen Blomin järjestelmän malli, jossa valitaan $k = 1$.

3.1.1 Erityinen Blomin järjestelmän malli

Erityisen Blomin järjestelmän mallin mukaan TA valitsee $k = 1$ ja määrittää sitten luvun p normaalisti. Jokaiselle käyttäjälle U luotettava auktoriteetti valitsee alkion $r_U \in \mathbb{Z}_p$ ja julkaisee tämän. Jokaisen käyttäjän alkio r on oltava keskenään eriävä. TA valitsee vielä kolme satunnaista alkiota $a, b, c \in \mathbb{Z}_p$. Näiden alkioiden ei ole pakko olla eriäviä. Alkioiden avulla TA muodostaa symmetrisen polynomin

$$f(x,y) = a + b(x + y) + cxy \pmod p,$$

jota ei julkaista yleiseen tietoon. Jokaiselle käyttäjälle U luotettava auktoriteetti muodostaa oman polynomin

$$g_U(x) = f(x,r_U) \pmod p,$$

joka voidaan sen lineaarisuuden johdosta esittää myös muodossa

$$g_U(x) = a_U + b_U x,$$

missä $a_U = a + br_U \pmod p$ ja $b_U = b + cr_U \pmod p$.

Kun kaksi käyttäjää U ja V haluavat kommunikoida keskenään, he muodostavat yhteisen salaisen avaimen

$$K_{U,V} = K_{V,U} = f(r_U,r_V) = a + b(r_U + r_V) + cr_U r_V \pmod p.$$

Käyttäjä U saa salaisen avaimen laskemalla

$$K_{U,V} = g_U(r_V)$$

ja käyttäjä V laskemalla

$$K_{V,U} = g_V(r_U).$$

Näin ollen TA:n muodostamaa alkuperäistä funktiota ei tarvitse tietää vaan riittää, kun jokainen käyttäjä tietää oman salaisen polynominsa g sekä muiden käyttäjien julkisen elementin r, sillä käyttäjien salaiset polynomit on muodostettu alkuperäisen polynomin avulla.

Esimerkki 3.1. (Avainten muodostaminen). Nyt $k = 1$. TA valitsee alkuluvun $p = 37$. Hän julkaisee käyttäjien alkiot $r_U = 7$ ja $r_V = 19$, kun r_U,$r_V \in \mathbb{Z}_{37}$. Nyt TA valitsee alkiot $a = 3$, $b = 7$ ja $c = 3$ ja muodostaa näiden avulla polynomin

$$f(x,y) = 3 + 7(x + y) + 3xy \quad (mod\ 37).$$

TA muodostaa käyttäjille U ja V salaiset polynomit

$$\begin{aligned} g_U(x) = f(x,r_U) &= 3 + 7(x + 7) + 3 \cdot x \cdot 7 = 3 + 7x + 49 + 21x \\ &= 52 + 28x = 15 + 28x \quad (mod\ 37) \end{aligned}$$

ja

$$\begin{aligned} g_V(x) = f(x,r_V) &= 3 + 7(x + 19) + 3 \cdot x \cdot 19 = 3 + 7x + 133 + 57x \\ &= 136 + 64x = 25 + 27x \quad (mod\ 37). \end{aligned}$$

Nyt käyttäjät U ja V voivat kommunikoida muodostamalla yhteisen avaimen

$$\begin{aligned} K_{U,V} = K_{V,U} = f(r_U,r_V) &= 3 + 7(r_U + r_V) + 3r_U r_V = 3 + 7(7 + 19) + 3 \cdot 7 \cdot 19 \\ &= 3 + 182 + 399 = 584 = 29 \quad (mod\ 37). \end{aligned}$$

3.1.2 Yleinen tapaus

Erityisestä Blomin järjestelmän mallista poiketen Blomin järjestelmän yleisessä tapauksessa TA valitsee jonkin luvun $k \geq 1$ ja määrittää sitten luvun p normaalisti. Jokaiselle käyttäjälle U luotettava auktoriteetti valitsee alkion $r_U \in \mathbb{Z}_p$ ja julkaisee tämän. Jokaisen käyttäjän alkio r on oltava keskenään eriävä. TA valitsee vielä satunnaisen alkion $a_{i,j} \in \mathbb{Z}_p$, kun $0 \leq i,j \leq k$. Nyt pätee myös $a_{i,j} = a_{j,i}$. Alkion avulla TA muodostaa kaikilta käyttäjiltä salaisen symmetrisen polynomin

$$f(x,y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j} x^i y^j \quad (mod\ p).$$

Jokaiselle käyttäjälle U luotettava auktoriteetti muodostaa salaisen polynomin $f(x,y)$ avulla oman polynomin

$$g_U(x) = f(x,r_U) \quad (mod\ p) = \sum_{i=0}^{k} a_{U,i} x^i.$$

TA lähettää käyttäjälle U vektorin $(a_{U,0}, \ldots, a_{U,k})$. Kun kaksi käyttäjää U ja V haluavat kommunikoida keskenään, he muodostavat yhteisen salaisen avaimen oman polynomin g sekä toisen käyttäjän julkisen alkion r avulla. Nyt

$$K_{U,V} = K_{V,U} = f(r_U, r_V).$$

Käyttäjä U laskee avaimen

$$K_{U,V} = g_U(r_V)$$

ja käyttäjä V laskee

$$K_{V,U} = g_V(r_U).$$

Esimerkki 3.2. (Avainten muodostaminen).
Nyt valitaan $k = 3$. TA valitsee alkuluvun $p = 37$. Hän julkaisee käyttäjien alkiot $r_U = 7$ ja $r_V = 19$, kun r_U,$r_V \in \mathbb{Z}_{37}$. Nyt TA valitsee alkion $a_{i,j} \in \mathbb{Z}_{37}$, joka saa arvon

$$\begin{vmatrix} i/j & 0 & 1 & 2 & 3 \\ 0 & 4 & 2 & 18 & 22 \\ 1 & 2 & 32 & 7 & 13 \\ 2 & 18 & 7 & 36 & 10 \\ 3 & 22 & 13 & 10 & 3 \end{vmatrix}$$

ja muodostaa näiden avulla polynomin

$$\begin{aligned} f(x,y) = {} & 4 + 2x + 2y + 32xy + 18x^2 + 18y^2 + 7x^2y + 7xy^2 + 36x^2y^2 + 22x^3 + 22y^3 \\ & + 13x^3y + 13xy^3 + 10x^3y^2 + 10x^2y^3 + 3x^3y^3 \quad (mod\ 37). \end{aligned}$$

TA muodostaa käyttäjille U ja V salaiset polynomit

$$\begin{aligned} g_U(x) = f(x,r_U) &= 4 + 2x + 2 \cdot 7 + 32x \cdot 7 + 18x^2 + 18 \cdot 7^2 + 7x^2 \cdot 7 + 7x \cdot 7^2 + 36x^2 \cdot 7^2 \\ &\quad + 22x^3 + 22 \cdot 7^3 + 13x^3 \cdot 7 + 13x \cdot 7^3 + 10x^3 \cdot 7^2 + 10x^2 \cdot 7^3 + 3x^3 \cdot 7^3 \\ &= 8446 + 5028x + 5261x^2 + 1632x^3 \\ &= 10 + 33x + 7x^2 + 4x^3 \quad (mod\ 37) \end{aligned}$$

ja

$$\begin{aligned} g_V(x) = f(x,r_V) &= 4 + 2x + 2 \cdot 19 + 32x \cdot 19 + 18x^2 + 18 \cdot 19^2 + 7x^2 \cdot 19 + 7x \cdot 19^2 + 36x^2 \cdot 19^2 \\ &\quad + 22x^3 + 22 \cdot 19^3 + 13x^3 \cdot 19 + 13x \cdot 19^3 + 10x^3 \cdot 19^2 + 10x^2 \cdot 19^3 + 3x^3 \cdot 19^3 \\ &= 157438 + 92304x + 81737x^2 + 24456x^3 \\ &= 3 + 26x + 4x^2 + 36x^3 \quad (mod\ 37). \end{aligned}$$

Nyt käyttäjät U ja V voivat kommunikoida muodostamalla yhteisen avaimen. Käyttäjä U saa avaimen laskemalla

$$\begin{aligned} K_{U,V} &= f(r_U,r_V) = g_U(r_V) = 10 + 33 \cdot 19 + 7 \cdot 19^2 + 4 \cdot 19^3 \pmod{37} \\ &= 10 + 35 + 11 + 19 \pmod{37} \\ &= 1 \pmod{37} \end{aligned}$$

ja käyttäjä V

$$\begin{aligned} K_{V,U} &= f(r_V,r_U) = g_V(r_U) = 3 + 26 \cdot 7 + 4 \cdot 7^2 + 36 \cdot 7^3 \pmod{37} \\ &= 3 + 34 + 11 + 27 \pmod{37} \\ &= 1 \pmod{37}. \end{aligned}$$

3.2 Salauksen murtaminen

Blomin järjestelmässä valitaan aina jokin turvallisuusparametri k. Tämä parametri kertoo järjestelmän turvallisuusasteen. Blomin järjestelmän salaukset ja avaimet ovat turvassa k käyttäjää vastaan, mutta jos $k+1$ käyttäjää jakaisi keskenään kaikki tietonsa, koko järjestelmä voitaisiin murtaa. Näin ollen myös, jos ulkopuolinen hyökkääjä onnistuu selvittämään $k+1$ käyttäjän salaiset tiedot, voi hän ratkaista myös muiden tiedot ja näin murtaa kaikki mahdolliset järjestelmän viestit.

Blomin järjestelmän turvalisuus k käyttäjää vastaan ja toisaalta taas turvattomuus $k+1$ käyttäjää vastaan voidaan osoittaa Lagrangen interpolointikaavaa sekä Lagrangen kaksimuuttujaista interpolointikaavaa käyttäen.

Lause 3.3. *(Lagrangen interpolointikaava).*
Oletetaan, että p on alkuluku ja $x_1, x_2, \ldots, x_{m+1} \in \mathbb{Z}_p$ eroavat toisistaan. Oletetaan myös, että $a_1, a_2, \ldots, a_{m+1} \in \mathbb{Z}_p$. Näin ollen voidaan olettaa, että on olemassa yksikäsitteinen polynomi $A(x) \in \mathbb{Z}_p[x]$, jonka asteluku on enintään m. Nyt polynomi $A(x)$ voidaan esittää muodossa

$$A(x) = \sum_{j=1}^{m+1} a_j \prod_{1 \le h \le m+1, h \neq j} \frac{x - x_h}{x_j - x_h}. \tag{1}$$

Todistus sivuutetaan.

Esimerkki 3.4. Valitaan $x = x_1$, $m = 2$ ja $h = 3$. Nyt

$$\begin{aligned} A(x) &= a_1 \left(\frac{x - x_2}{x_1 - x_2}\right)\left(\frac{x - x_3}{x_1 - x_3}\right) + a_2 \left(\frac{x - x_1}{x_2 - x_1}\right)\left(\frac{x - x_3}{x_2 - x_3}\right) + a_3 \left(\frac{x - x_1}{x_3 - x_1}\right)\left(\frac{x - x_2}{x_3 - x_1}\right) \\ &= a_1 \left(\frac{\cancel{x_1 - x_2}}{\cancel{x_1 - x_2}}\right)\left(\frac{\cancel{x_1 - x_3}}{\cancel{x_1 - x_3}}\right) + a_2 \left(\frac{\cancel{x_1 - x_1}}{x_2 - x_1}\right)^{0}\left(\frac{x_1 - x_3}{x_2 - x_3}\right) + a_3 \left(\frac{\cancel{x_1 - x_1}}{x_3 - x_1}\right)^{0}\left(\frac{x_1 - x_2}{x_3 - x_1}\right) \\ &= a_1. \end{aligned}$$

Nyt huomataan, että kaavan 3.3 summan kaikki termit saavat arvon nolla, paitsi termi $j = i$, joka saa arvon 1 ja näin ollen $A(x_i) = a_i$.

Lause 3.5. *(Lagrangen kaksimuuttujainen interpolointikaava).*

Oletetaan, että p on alkuluku ja $y_1, y_2, \ldots, y_{m+1} \in \mathbb{Z}_p$ eroavat toisistaan ja, että $a_1(x), a_2(x), \ldots, a_{m+1}(x) \in \mathbb{Z}_p[x]$ ovat polynomeja, joiden asteluku on enintään m. Näin ollen voidaan olettaa, että on olemassa yksikäsitteinen polynomi $A(x, y) \in \mathbb{Z}_p[x,y]$, jonka asteluku on myös enintään m. Nyt polynomi $A(x, y)$ voidaan esittää muodossa

$$A(x,y) = \sum_{j=1}^{m+1} a_j(x) \prod_{1 \le h \le m+1, h \ne j} \frac{y - y_h}{y_j - y_h}. \tag{2}$$

Todistus sivuutetaan.

Esimerkki 3.6. Oletetaan, että $p = 7$, $m = 3$, $y_1 = 1$, $y_2 = 2$, $y_3 = 3$ ja $y_4 = 4$. Nyt

$$\begin{aligned} a_1(x) &= 5 + x^2 \\ a_2(x) &= 1 + x + x^2 + x^3 \\ a_3(x) &= 4x + 6x^3 \\ a_4(x) &= 5 + x + 2x^3. \end{aligned}$$

Näin saadaan

$$\frac{(y-2)(y-3)(y-4)}{(1-2)(1-3)(1-4)} = \frac{1}{6}(-y^3+9y^2-26y+24) = y^3+5y^2+5y+4$$

$$\frac{(y-1)(y-3)(y-4)}{(2-1)(2-3)(2-4)} = \frac{1}{2}(y^3-8y^2+19y-12) = 4y^3+3y^2+6y+1$$

$$\frac{(y-1)(y-2)(y-4)}{(3-1)(3-2)(3-4)} = -\frac{1}{2}y^3+\frac{7}{2}y^2-7y+4 = 3y^3+7y^2+4$$

$$\frac{(y-1)(y-2)(y-3)}{(4-1)(4-2)(4-3)} = \frac{1}{6}(y^3-6y^2+11y-6) = 6y^3+6y^2+3y+6.$$

Nyt polynomi $A(x,y)$ saadaan muotoon

$$\begin{aligned}
A(x,y) &= (5+x^2)(y^3+5y^2+5y+4)+(1+x+x^2+x^3)(4y^3+3y^2+6y+1)\\
&\quad +(4x+6x^3)(3y^3+7y^2+4)+(5+x+2x^3)(6y^3+6y^2+3y+6) \pmod 7\\
&= 34x^3y^3+57x^3y^2+12x^3y+37x^3+5x^2y^3+8x^2y^2+11x^2y+5x^2\\
&\quad +22xy^3+37xy^2+9xy+23x+39y^3+58y^2+46y+51 \pmod 7\\
&= 2+2x+4y+2xy+5x^2+2y^2+4x^2y+2xy^2\\
&\quad +x^2y^2+2x^3+4y^3+5x^3y+xy^3+x^3y^2+5x^2y^3+6x^3y^3 \pmod 7.
\end{aligned}$$

Nyt voidaan yksinkertaisesti todistaa, että $A(x,i) = a_i(x), i = 1,2,3,4$. Kun $i = 1$, saadaan

$$\begin{aligned}
A(x,1) &= 2+2x+4\cdot 1+2x\cdot 1+5x^2+2\cdot 1^2+4x^2\cdot 1+2x\cdot 1^2\\
&\quad +x^2\cdot 1^2+2x^3+4\cdot 1^3+5x^3\cdot 1+x\cdot 1^3+x^3\cdot 1^2+5x^2\cdot 1^3+6x^3\cdot 1^3 \pmod 7\\
&= 2+2x+4+2x+5x^2+2+4x^2+2x+x^2+2x^3+4+5x^3\\
&\quad +x+x^3+5x^2+6x^3 \pmod 7\\
&= 12+7x+15x^2+14x^3 \pmod 7 = 5+x^2 \pmod 7.
\end{aligned}$$

3.2.1 Erityinen Blomin järjestelmän malli

Lause 3.7. *Erityinen Blomin järjestelmän malli on turvallinen vain ja ainoastaan yksittäisiä hyökkääjiä vastaan.*

Todistus. Oletetaan, että käyttäjä W haluaa muodostaa avaimen

$$K_{U,V} = a + b(r_U + r_V) + cr_U r_V \pmod p,$$

kun $W \neq U,V$. Käyttäjä W tietää alkiot r_U, r_V, sillä nämä ovat julkisia, mutta alkiot a, b ja c ovat tuntemattomia. Käyttäjä W tietää TA:n hänelle lähettämästä polynomista alkiot

$$a_W = a + br_W \pmod p$$
$$b_W = b + cr_W \pmod p.$$

Nyt W ei pysty poissulkemaan mitään arvoja avaimesta $K_{U,V}$. Nimittäin tarkastellaan seuraavaa yhtälöä:

$$\begin{pmatrix} 1 & r_U + r_V & r_U r_V \\ 1 & r_W & 0 \\ 0 & 1 & r_W \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} K^* \\ a_W \\ b_W \end{pmatrix},$$

missä $K^* \in \mathbb{Z}_p$.
Yhtälössä luodaan hypoteesia $K_{U,V} = K^*$ ja käytetään hyväksi käyttäjän W tietämiään tietoja alkioista a, b ja c polynomin $g_W(x)$ avulla. Kerroinmatriisin determinantiksi saadaan

$$r_W^2 + r_U r_V - (r_U + r_V) r_W = (r_W - r_U)(r_W - r_V).$$

Nyt, koska Blomin järjestelmän määritelmän mukaan $r_W \neq r_U, r_W \neq r_V$ ja p on alkuluku, kerroinmatriisilla on nollasta poikkeava determinantti modulo p ja matriisiyhtälöllä on yksikäsitteiset ratkaisut alkioille a, b ja c. Näin ollen käyttäjän W tiedoilla ei voida tehdä mitään päätelmiä avaimesta $K_{U,V}$ eikä sitä siis voida ratkaista. □

Lause 3.8. *Kaksi erillistä käyttäjää W ja X voivat ratkaista minkä tavansa avaimen $K_{U,V}$.*

Todistus. Käyttäjät W ja X voivat ratkaista avaimen $K_{U,V}$, missä
$W,X \cap U,V = \emptyset$. Käyttäjät W ja X voivat yhdistää tietonsa, jolloin he tietävät, että

$$a_W = a + br_W,$$
$$b_W = b + cr_W,$$
$$a_X = a + br_X,$$
$$b_X = b + cr_X.$$

Nyt huomataan, että käyttäjät W ja X pystyvät muodostamaan neljä erillistä yhtälöä, kun tuntemattomia alkioita on kolme, joten he pystyvät helposti ratkaisemaan alkiot. Käyttäjien tietäessä alkiot a, b ja c, he pystyvät ratkaisemaan minkä tahansa haluamansa avaimen TA:n salaisesta polynomista $f(x,y)$.

□

3.2.2 Yleinen tapaus

Lause 3.9. *Blomin järjestelmän yleinen tapaus on turvaton aina $k+1$ hyökkääjää vastaan.*

Todistus. Nyt $k+1$ käyttäjän liittouma, esimerkiksi $W_1, \ldots, W_{k+1}$, tietää yhteensä $k+1$ k-asteista polynomia

$$g_{W_i}(x) = f(x,r_{W_i})) \pmod p,$$

jossa $1 \leq i \leq k+1$. Lagrangen kaksimuuttujaista interpolointikaavaa käyttämällä käyttäjät voivat muodostaa polynomin $f(x,y)$. Kun polynomi $f(x,y)$ on tiedossa, voivat käyttäjät muodostaa minkä tahansa haluamansa avaimen.

□

Lause 3.10. *Blomin järjestelmä on turvallinen aina k käyttäjän liittoumia vastaan.*

Todistus. Liittouma, esimerkiksi $W_1, \ldots, W_k$ tietää yhteensä k kappaletta k-asteen polynomia

$$g_{W_i}(x) = f(x,r_{W_i}) \pmod p,$$

jossa $1 \leq i \leq k$. Olkoon nyt K avain, jonka arvoa liittouma ei tiedä ja valitaan K^* mielivaltaisesti. Nyt voidaan osoittaa, että on olemassa symmetrinen polynomi $f^*(x,y)$, joka on liittouman tiedossa olevien tietojen mukainen ja salainen avain K^* on muodostettu polynomin $f^*(x,y)$ avulla. Näin ollen k käyttäjän liittouma ei pysty poissulkemaan avaimen arvoja. Polynomi $f^*(x,y)$ voidaan määritellä

$$f^*(x,y) = f(x,y) + (K^* - K) \prod_{1 \leq i \leq k} \frac{(x - r_{W_i})(y - r_{W_i})}{(r_U - r_{W_i})(r_V - r_{W_i})}.$$

Tästä nähdään, että $f^*(x,y)$ on symmetrinen polynomi ja $f^*(x,r_{W_i}) = f(x,r_{W_i}) = g_{W_i}(x)$. Lisäksi havaitaan, että $f^*(r_U,r_V) = f(r_U,r_V) + K^* - K = K^*$. Täten kaikille avaimen arvoille K^* on olemassa symmetrinen polynomi $f^*(x,y)$ niin, että $f^*(U,V) = K^*$. Näin ollen k käyttäjän liittoumat eivät pysty murtamaan Blomin järjestelmää.

□

Lähdeluettelo

[1] Stinson ja Paterson: Cryptography – Theory and Practice. 4. painos. CRC Press, Florida, 2019.