Usean muuttujan julkisen avaimen salausjärjestelmät

Pro Gradu -tutkielma
Jesse Salo
2309369
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2019

Sisältö

Johdanto

Jo muinaiset roomalaiset painivat sen ongelman kanssa, että kaikkea informaatiota ei ole tarkoitettu kenen tahansa luettavaksi, mutta tällaistakin tietoa on välitettävä eteenpäin. Tämä aiheuttaa sen vaaran, että joku kaappaa lähetettävän viestin ja pääsee käsiksi sen sisältöön. Tämä ongelma on pyritty ratkaisemaan kehittämällä erilaisia salausmenetelmiä, mikä estää kaappaajaa saamasta selville viestin todellista sisältöä. Näin tietoon pääsevät käsiksi ainoastaan siihen oikeutetut vastaanottajat, jotka tuntevat järjestelmän salaisen avaimen.

Tässä tutkielmassa perehdytään usean muuttujan julkisen avaimen salausjärjestelmiin, joiden historia alkaa 1980-luvun lopulta. Näiden järjestelmien julkinen avain koostuu usean muuttujan polynomiyhtälöistä jonkin äärellisen kuntalaajennuksen suhteen. Järjestelmien käyttö perustuu siihen, että yhtälöt ovat salattavan tekstin suhteen lineaarisia, jolloin viestin salaaminen ja avaaminen on yksinkertaista, mutta selkotekstin suhteen yhtälöt ovat epälineaarisia. Tämän takia selkotekstin selvittäminen salatusta tekstistä ilman salaista avainta on erittäin haastavaa, koska viestin avaamiseksi on ratkaistava epälineaarinen yhtälöryhmä. Termistä usean muuttujan julkisen avaimen salausjärjestelmä käytetään tässä tutkielmassa nimeä MPKC (Multivariate Public Key Cryptography). Kvanttitietokoneiden kehityksen myötä useat nykyisin käytössä olevat salausjärjestelmät muuttuvat tulevaisuudessa turvattomiksi, minkä takia uusia kvanttitietokonehyökkäykset kestäviä salausjärjestelmiä on kehitettävä. MPKC-järjestelmät ovat yksi tämän alan tutkimushaara. Lukijalta edellytetään esitietoina lineaarialgebran, kuntarakenteiden sekä salausmenetelmien tuntemusta. Tutkielmassa on käytetty lähteenä pääasiassa teosta [8].

Luvussa 1 esitetään tutkielmassa käytettäviä lineaarialgebran ja kuntarakenteiden käsitteiden määritelmiä sekä todistetaan joitakin tarpeellisia niihin liittyviä perustuloksia. Äärellisiä kuntalaajennuksia käsitellään tutkielmassa vektoriavaruuksina kerroinkunnan suhteen. Luku toimii näyteikkunana tutkielman sisältämään matematiikkaan, jonka oletetaan olevan lukijalle tuttua.

Tutkielman Luvussa 2 tutkitaan Imai-Matsumoto -järjestelmää, joka on ensimmäisenä kehitetty MPKC-järjestelmä. Tämä menetelmä aloitti kokonaan uuden salausjärjestelmien haaran ja toimi perustana useille siitä johdetuille jälkeläisille. Ensiksi esitetään järjestelmän rakentamisen matemaattinen perusta, jota seuraa esimerkkejä järjestelmän käytöstä. Seuraavaksi esitetään menetelmä, jolla järjestelmä saadaan murrettua. Luvun lopussa esitetään muunnos Imai-Matsumoto -järjestelmästä.

Kolmannessa luvussa käsitellään Jacques Patarinin 1990-luvulla esittämää paranneltua versiota Imai-Matsumoto -järjestelmästä, nimeltään Pieni

lohikäärme. Järjestelmästä esitetään jälleen sen matemaattinen perusta ja esimerkkejä järjestelmän käytöstä. Tämän jälkeen osoitetaan, miksi Pieni lohikäärme ei murru samalla menetelmällä, jota käytettiin Imai-Matsumoto -järjestelmän murtamiseen. Pieni lohikäärme kuitenkin murtuu helposti, jos siinä käytettävä salainen eksponentti valitaan huonosti. Lopuksi esitetään Coppersmith-Patarin -menetelmä, jolla järjestelmä saadaan murrettua yleisessä tapauksessa.

Luvussa 4 tarkastellaan paranneltuja muunnoksia Pienestä lohikäärmeestä. Näistä ensimmäinen on Patarinin Iso lohikäärme. Tätä seuraa permutaatiopolynomeja koskeva kappale, jossa todistetaan niihin liittyviä tuloksia. Näitä käytetään kahdessa 2010-luvulla esitetyssä MPKC-järjestelmässä. Ensin esitetään Pieni lohikäärme kaksi ja sen rakentamisen perusta sekä käsitellään järjestelmän turvallisuutta. Tätä seuraa vastaavanlainen tarkastelu Poly-Dragon -järjestelmästä. Näissä järjestelmissä on havaittavissa suurta kehitystä verrattuna Imai-Matsumoto -järjestelmään.

Tutkielman viimeisessä luvussa luodaan lyhyt katsaus usean muuttujan julkisen avaimen salausjärjestelmien menestykseen sekä niiden nykytilanteeseen. Luvussa mainitaan muutamia nykyaikaisia usean muuttujan julkisen avaimen salausjärjestelmiä, jotka johdattavat kiinnostuneen lukijan halutessaan tutkimaan aihetta lisää.

1 Tarpeellista algebraa

Ennen tutkielman pääaiheen käsittelyä on tarpeen määritellä joitakin käsitteitä. Tämän luvun tarkoitus on tuoda esille seuraavissa luvuissa tarvittavia määritelmiä ja tuloksia, joiden oletetaan kuitenkin olevan lukijalle jossain määrin tuttuja. Luku toimii kertauksena lineaarialgebran ja kuntarakenteiden valikoiduista perusasioista ja antaa yleiskuvan siitä, millaista matematiikkaa tutkielma sisältää.

Määritelmä 1.1. Olkoon $\mathbb{K}$ joukko, jolla on joukon $\mathbb{K}$ suhteen suljetut binääriset operaatiot $+$ ja $*$. Kolmikko $(\mathbb{K}, +, *)$ on kunta, jos seuraavat ehdot toteutuvat:

1. Pari $(\mathbb{K}, +)$ on Abelin ryhmä, jonka neutraalialkio on $0 \in \mathbb{K}$,
2. pari $(\mathbb{K} \setminus \{0\}, *)$ on Abelin ryhmä ja
3. $(a + b) * c = a * c + b * c$ kaikilla $a, b, c \in \mathbb{K}$.

Merkitään jatkossa $\mathbb{K} \setminus \{0\} = \mathbb{K}^*$ ja sen neutraalialkiota $1 \in \mathbb{K}^*$. Jos äärellisen kunnan kertaluku on q, toisin sanoen se sisältää q alkiota, merkitään kuntaa $\mathbb{F}_q$.

Määritelmä 1.2. Kunnan $\mathbb{K}$ *karakteristika* on ykkösen generoiman syklisen ryhmän $\{n1 | n \in \mathbb{Z}\}$ kertaluku k (yhteenlaskun suhteen), mikäli ryhmä on äärellinen. Tällöin merkitään $\operatorname{char} \mathbb{K} = k$. Jos ykkösen generoima syklinen ryhmä ei ole äärellinen, niin $\operatorname{char} \mathbb{K} = 0$.

Määritelmä 1.3. Olkoon V Abelin ryhmä ja $\mathbb{K}$ kunta. Operaatiota $\mathbb{K} \times V \to V$, $(k, v) \mapsto kv$ sanotaan joukon V *skalaarituloksi* kunnan $\mathbb{K}$ suhteen, mikäli $kv \in V$ kaikilla $k \in \mathbb{K}$ ja $v \in V$.

Määritelmä 1.4. $\mathbb{F}$*-kertoiminen vektoriavaruus* on Abelin ryhmä $(V, \star)$ varustettuna skalaaritulolla kunnan $(\mathbb{F}, +, \cdot)$ suhteen, missä $\star$ on vektorien yhteenlasku, mikäli skalaaritulo toteuttaa seuraavat ehdot kaikilla $a, b \in \mathbb{F}$ ja $\overline{v}, \overline{w} \in V$:

1. $1\overline{v} = \overline{v}$, missä 1 on kunnan $\mathbb{F}$ ykkösalkio,
2. $(a + b)\overline{v} = a\overline{v} \star b\overline{v}$,
3. $a(\overline{v} \star \overline{w}) = a\overline{v} \star a\overline{w}$ ja
4. $(a \cdot b)\overline{v} = a(b\overline{v})$.

$\mathbb{F}$-kertoimisen vektoriavaruuden V osajoukon $S = \{s_1, s_2, \ldots, s_n\}$ *virittämä aliavaruus* on

$$\operatorname{span} S = \{a_1 s_1 + a_2 s_2 + \ldots + a_n s_n | a_1, a_2, \ldots, a_n \in \mathbb{F}\}.$$

Jos vektoriavaruuden V lineaarisesti vapaan osajoukon S virittämä aliavaruus $\operatorname{span} S = V$, niin osajoukkoa S kutsutaan vektoriavaruuden V *kannaksi*. Vektoriavaruuden V *dimensio* on jonkin sen kannan vektorien lukumäärä ja merkitään $\dim V = n$.

Huomautus 1.5. Vektoriavaruuden kanta ei ole yksikäsitteinen, mutta jokainen vektoriavaruuden alkio voidaan esittää kussakin kannassa yksikäsitteisesti kannan vektorien lineaarikombinaationa.

Määritelmä 1.6. Olkoot V ja W vektoriavaruuksia kunnan $\mathbb{K}$ yli. Kuvaus $L : V \mapsto W$ on lineaarinen, jos

1. $L(v + w) = L(v) + L(w)$,
2. $L(\lambda v) = \lambda L(v)$, kaikilla $v, w \in V$ ja $\lambda \in \mathbb{K}$.

Tällöin sanotaan, että L on lineaarikuvaus.

Määritelmä 1.7. Olkoot V ja W vektoriavaruuksia sekä $L : V \to W$ lineaarikuvaus. Kuvauksen L ydin on joukko

$$\operatorname{Ker} L = \{v \in V | L(v) = 0\}.$$

Lause 1.8. *Olkoot V ja W vektoriavaruuksia sekä $L : V \to W$ lineaarikuvaus. Tällöin L on injektio jos ja vain jos* $\operatorname{Ker} L = \{0\}$.

Todistus. Olkoon L injektio. Valitaan $x \in \operatorname{Ker} L$, jolloin $L(x) = 0 = L(0)$. Siten $x = 0$, koska L on injektio ja edelleen $\operatorname{Ker} L = \{0\}$.

Olkoon nyt $\operatorname{Ker} L = \{0\}$. Nyt ehdosta $L(x) = L(y)$ seuraa kuvauksen lineaarisuuden perusteella $L(x - y) = 0$. Näin ollen $x - y \in \operatorname{Ker} L = \{0\}$. Koska $\operatorname{Ker} L = \{0\}$, niin $x - y = 0$ eli $x = y$. Näin ollen kuvaus L on injektio. □

Määritelmä 1.9. Olkoon $\mathbb{K}$ kunta ja $\mathbb{F}$ sen alikunta. Tällöin kunta $\mathbb{K}$ on kunnan $\mathbb{F}$ *kuntalaajennus*, merkitään $\mathbb{K}/\mathbb{F}$. Kuntalaajennuksen $\mathbb{K}/\mathbb{F}$ *aste* on kunnan $\mathbb{K}$ $\mathbb{F}$-kertoimisen vektoriavaruuden dimensio.

Huomautus 1.10. Kunnalla $\mathbb{K}$ ja sen alikunnalla $\mathbb{F}$ on sama karakteristika, $\operatorname{char} \mathbb{K} = \operatorname{char} \mathbb{F}$.

Määritelmä 1.11. Olkoon $\mathbb{F}_q$ äärellinen kunta ja $n \in \mathbb{Z}_+$. Jos alkio $x \in \mathbb{F}$ on yhtälön $x^n = 1$ ratkaisu, niin x on n:s *ykkösjuuri kunnassa* $\mathbb{F}$. Ykkösjuuri on *primitiivinen*, jos $x^n = 1$ ja $x^k \neq 1$ kaikilla $k = 1, 2, \ldots, n-1$. Tällöin alkion x *kertaluku* on n, merkitään $ord\, x = n$.

Lause 1.12. *Kunnassa $\mathbb{F}_q$ jokainen alkio x toteuttaa yhtälön $x^q - x = 0$, ts. $x^q = x$.*

Todistus. Kunnan alkion x kertaluku α jakaa aina kunnan kertolaskuryhmän kertaluvun $q-1$, $\alpha b = (q-1)$, $b \in \mathbb{Z}_+$. Nyt

$$x^q = x \cdot x^{q-1} = x \cdot x^{\alpha b} = x \cdot 1^b = x.$$

Tämän perusteella $x^q - x = x - x = 0$. □

Lause 1.13. *Olkoon kunnan $\mathbb{F}_q$ karakteristika p. Tällöin kaikilla $x, y \in \mathbb{F}, n \in \mathbb{Z}_+$, pätee $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.*

Todistus. Osoitetaan lause induktiolla. Olkoon aluksi $n = 1$. Nyt

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p,$$

koska luku p jakaa binomikertoimen kaikilla $i = 1, 2, \ldots, p-1$.

Oletetaan seuraavaksi, että $(x+y)^{p^n} = x^{p^n} + y^{p^n}$. Tällöin

$$(x+y)^{p^{n+1}} = (x+y)^{p^n p} = (x^{p^n} + y^{p^n})^p.$$

Koska luku p jakaa taas binomikertoimen kaikilla $i = 1, 2, \ldots, p-1$, niin

$$(x^{p^n} + y^{p^n})^p = (x^{p^n})^p + (y^{p^n})^p = x^{p^{n+1}} + y^{p^{n+1}}.$$

□

Määritelmä 1.14. Olkoon $\mathbb{F}_{q^n}$ kunnan $\mathbb{F}_q$ laajennuskunta ja $\alpha \in \mathbb{F}_{q^n}$. Alkion α *konjugaatit* kunnan F_q suhteen ovat alkiot $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{(n-1)}}$.

Määritelmä 1.15. *Redusoitu jäännösluokkasysteemi* modulo m on joukko, joka sisältää $\varphi(m)$ kokonaislukua, jotka eivät ole keskenään kongruentteja modulo m ja ovat keskenään jaottomia luvun m kanssa. Tässä $\varphi(m)$ on Eulerin φ-funktio.

Määritelmä 1.16. Olkoon f ja g sellaisia kuvauksia, että $f(n), g(n)$ ovat määriteltyjä ja positiivisia kaikilla $n \geq n_0$. Jos on olemassa sellainen vakio C, että $f(n) \leq C \cdot g(n)$ kaikilla $n \geq n_0$, niin merkitään $f = \mathcal{O}(g)$. Merkintä $\mathcal{O}$ luetaan "iso oo".

2 Imai-Matsumoto -salausjärjestelmä

Vuonna 1988 julkaisemassaan artikkelissa Tsutomu Matsumoto ja Hideki Imai esittelivät Imai-Matsumoto -salausjärjestelmän (myös Matsumoto-Imai tai C* joissain yhteyksissä), joka perustuu äärellisiin kuntalaajennuksiin ja vektoriavaruuksiin [10]. Tässä tutkielmassa käytetään myös lyhennettä IM tästä järjestelmästä. Kyseinen järjestelmä oli edistyksellinen ja edisti samantyyppisten salausjärjestelmien kehitystä. Myöhemmin tästä järjestelmästä on esitetty useita muunnoksia ja paranneltuja versioita. Seuraavassa kappaleessa esitetään Neal Koblitzin hieman yksinkertaistettu versio kyseisestä järjestelmästä [8].

2.1 Järjestelmän rakenne

Olkoon $\mathbb{K}$ astetta n oleva äärellisen kunnan $\mathbb{F}_q$ kuntalaajennus, missä q on jokin luvun 2 potenssi ja olkoon $\{\beta_1, \beta_2, \ldots, \beta_n\}$ kunnan $\mathbb{K}$ $\mathbb{F}_q$-kertoimisen vektoriavaruuden kanta. Imai-Matsumoto -salausjärjestelmää käytetään nyt kunnassa $\mathbb{K}$ ja jokaista sen alkiota voidaan kuvata vektoriavaruuden $\mathbb{F}_q^n$ vektorina. Valittu vektoriavaruuden kanta pidetään salassa. Merkitään selkokielisiä viestiyksiköitä $\bar{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ ja salattuja viestiyksiköitä $\bar{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. Nämä vektorit ajatellaan pystymatriiseiksi, mutta ne kirjoitetaan johdonmukaisesti tässä tutkielmassa vaakavektoreina.

Järjestelmässä käytetään kahta vektoria $\bar{u}$ ja $\bar{v} \in \mathbb{F}_q^n$. Vastaavia alkioita kunnassa $\mathbb{K}$ kannan β_j suhteen merkitään $\mathbf{u} = u_1\beta_1 + u_2\beta_2 + \ldots + u_n\beta_n \in \mathbb{K}$. Valitaan vielä eksponentti $h = q^\theta + 1$, $0 < h < q^n$, joka toteuttaa ehdon $\text{syt}(h, q^n - 1) = 1$. Valittu eksponentti pidetään salassa.

Huomautus 2.1. Ehto $\text{syt}(h, q^n - 1) = 1$ varmistaa, että eksponentilla h on käänteisalkio h^{-1} modulo $q^n - 1$. Tällöin myös kuvauksella $\mathbf{u} \mapsto \mathbf{u}^h$ on käänteiskuvaus $\mathbf{u} \mapsto \mathbf{u}^{h^{-1}}$. Koska annetut ehdot täyttäviä eksponentteja h on verrattain vähän, järjestelmää murtaessa voi sopivan eksponentin löytää kokeilemalla varsin nopeasti. Tämän takia Imai-Matsumoto -järjestelmän turvallisuus perustuu muihin seikkoihin.

Esimerkki 2.2. Valitaan $q^n - 1 = 2^{20} - 1 = 1048575$. Nyt muotoa $h = q^\theta + 1$, $0 < h < q^n$ olevia eksponentteja, jotka toteuttavat ehdon $\text{syt}(h, q^n - 1) = 1$ on vain viisi: 2, 17, 257, 4097 ja 65537.

Seuraavaksi valitaan kaksi kääntyvää $n \times n$-matriisia,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix},$$

$1 \leq i, j \leq n, a_{ij}, b_{ij} \in \mathbb{F}_q$, sekä kaksi vakiovektoria $\overline{c} = (c_1, c_2, \ldots, c_n)$ ja $\overline{d} = (d_1, d_2, \ldots, d_n)$, $c_i, d_i \in \mathbb{F}_q$. Näiden avulla muodostetaan affiinit muunnokset, joilla saadaan piilotettua kuvaus $\mathbf{u} \mapsto \mathbf{u}^h$, mikä antaa tämäntyyppisille salausjärjestelmille nimen *kätketyn monomin salausjärjestelmät.* Selväkielinen viestivektori $\overline{x}$ piilotetaan asettamalla $\overline{u} = A\overline{x} + \overline{c}$ ja laskemalla vektori $\mathbf{v} = \mathbf{u}^h \in \mathbb{K}$. Vektori $\mathbf{v}$ on muotoa

$$\mathbf{v} = \sum_{l=1}^{n} v_l \beta_l, \quad v_l = \sum_{1 \leq i,j,s \leq n} m_s u_i u_j, \quad m_s \in \mathbb{F}_q.$$

Koska komponentit u_i tunnetaan, saadaan muodostettua lausekkeet komponenteille v_l. Seuraava askel on laskea vektori $\overline{y} = B^{-1}(\overline{v} - \overline{d})$. Kun tähän sijoitetaan tunnetut komponenttien v_l lausekkeet, saadaan n yhtälöä, joissa vasemmalla puolella on luvut $y_1, y_2, \ldots, y_n$ ja oikealla puolella toisen asteen polynomi, joka sisältää kertoimet $x_1, x_2, \ldots, x_n$. Yhtälöt ovat yleisessä muodossa

$$y_k = \sum_{1 \leq i,j \leq n} m_s x_i^a x_j^b, \quad m_s \in \mathbb{F}_q,\ a, b \in \{0, 1\},\ k = 1, 2, \ldots, n. \tag{1}$$

Nämä yhtälöt julkaistaan, ja niiden avulla lähettäjä saa selväkielisen tekstinsä $\overline{x} = (x_1, x_2, \ldots, x_n)$ muunnettua salakirjoitustekstiksi $\overline{y} = (y_1, y_2, \ldots, y_n)$ sijoittamalla komponentit x_i yhtälöihin (1).

Huomautus 2.3. Imai-Matsumoto -järjestelmän salaus on siis bijektiivinen kuvaus $\mathbb{F}_q^n \to \mathbb{F}_q^n$. Viestiyksikön pituus on tällöin aina n. Se miten viestiyksiköt esitetään vektoriavaruuden $\mathbb{F}_q^n$ alkioina, on käyttäjän mielivaltaisesti valittavissa.

Alla oleva kaavio havainnollistaa Imai-Matsumoto -järjestelmän rakentamista, viestin salaamista sekä salauksen avaamista.

Esimerkki 2.4. Muodostetaan yksinkertainen Imai-Matsumoto -järjestelmä. Valitaan $q = 2$, $n = 5$ ja olkoon $\mathbb{K} = \mathbb{F}_2[x]/\langle x^5 + x^4 + x^3 + x + 1 \rangle$. Käytetään kantaa $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\} = \{1, x, x^2, x^3, x^4\}$ ja valitaan $\theta = 3$,

Rakentaminen	**Salaaminen**	**Avaaminen**
$\overline{u} = A\overline{x} + \overline{c}$	$\overline{x} = (x_1, x_2, \ldots, x_n)$	$\overline{v} = B\overline{y} + \overline{d}$
$\Downarrow$	$\Downarrow$	$\Downarrow$
$\mathbf{v} = \mathbf{u}^h$	$\overline{y} = \sum_{1 \le i,j \le n} m_s x_i x_j$	$\mathbf{u} = \mathbf{v}^{h^{-1}}$
$\Downarrow$	$\Downarrow$	$\Downarrow$
$\overline{y} = B^{-1}(\overline{v} - \overline{d})$	$\overline{y} = (y_1, y_2, \ldots, y_n)$	$\overline{x} = A^{-1}(\overline{u} - \overline{c})$

Kuva 1: Imai-Matsumoto -järjestelmän rakentaminen ja viestin avaaminen

jolloin $h = 2^\theta + 1 = 9$ ja $h^{-1} = 7 \mod q^n - 1 = 2^5 - 1 = 31$. Lisäksi valitaan

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$\overline{c} = (1, 0, 1, 1, 1), \quad \overline{d} = (1, 0, 1, 0, 0)$. Määrätään seuraavaksi vektori

$$\overline{u} = A\overline{x} + \overline{c} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 + x_3 + x_4 + 1 = u_1 \\ x_2 + x_3 + x_5 = u_2 \\ x_1 + x_2 + x_5 + 1 = u_3 \\ x_2 + x_4 + 1 = u_4 \\ x_4 + x_5 + 1 = u_5 \end{pmatrix}.$$

Nyt $\mathbf{v} = \mathbf{u}^9 = (u_1\beta_1 + u_2\beta_2 + u_3\beta_3 + u_4\beta_4 + u_5\beta_5)^9$, josta saadaan laskemalla $\mod\ x^5 + x^4 + x^3 + x + 1$ vektorin $\mathbf{v}$ komponenteiksi valitun kannan suhteen

$$\begin{aligned} v_1 =& 1 + x_1^2 + x_1x_3 + x_1x_2 + x_4 + x_4x_5 + x_1x_4 + x_2x_4 + x_1 \\ & + x_2 + x_3x_5 + x_2^2 \\ v_2 =& x_5x_1 + x_3x_2 + x_1^2 + x_2x_5 + x_5^2 + x_4 + x_1x_4 + x_1 + x_3^2 + x_2 + x_3x_5 \\ v_3 =& x_1x_3 + x_1 + x_1x_2 + x_3x_2 + x_3x_4 + x_2 + x_3 + x_4^2 + x_3x_5 + x_2^2 \\ v_4 =& x_3x_4 + x_1^2 + x_5^2 + x_3 + 1 + x_1x_3 + x_1x_4 + x_2x_4 + x_4^2 + x_2^2 \\ v_5 =& x_3x_2 + 1 + x_5x_1 + x_3 + x_5 + x_5^2 + x_1x_3 + x_1x_2 + x_4 + x_1x_4 \\ & + x_3^2 + x_2 + x_4^2 + x_3x_5. \end{aligned} \tag{2}$$

Koska $\overline{y} = B^{-1}(\overline{v} - \overline{d})$, niin

$$\overline{y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 - 1 \\ v_2 \\ v_3 - 1 \\ v_4 \\ v_5 \end{pmatrix} = \begin{pmatrix} y_1 = v_5 \\ y_2 = v_4 + v_5 \\ y_3 = v_1 + v_2 + v_3 + v_4 + v_5 \\ y_4 = v_1 + v_3 + v_4 + v_5 \\ y_5 = v_3 + v_4 + 1 \end{pmatrix}.$$

Näin ollen saadaan yhtälöt selkotekstin $\overline{x}$ ja salatun viestin $\overline{y}$ välille, jotka julkaistaan:

$$\begin{aligned}
y_1 =& x_3x_2 + 1 + x_5x_1 + x_3 + x_5 + x_5^2 + x_1x_3 + x_1x_2 + x_4 + x_1x_4 + x_3^2 \\
&+ x_2 + x_4^2 + x_3x_5 \\
y_2 =& x_3x_4 + x_1^2 + x_2x_4 + x_2^2 + x_3x_2 + x_5x_1 + x_5 + x_1x_2 + x_4 \\
&+ x_3^2 + x_2 + x_3x_5 \\
y_3 =& 1 + x_1^2 + x_1 + x_3 + x_4 + x_5 + x_4^2 + x_1x_2 + x_4x_5 + x_3x_2 \\
&+ x_2^2 + x_2x_5 + x_5^2 \\
y_4 =& 1 + x_1x_4 + x_3^2 + x_2 + x_3 + x_5 + x_4^2 + x_3x_5 + x_5x_1 \\
&+ x_1x_2 + x_4x_5 + x_2^2 \\
y_5 =& x_1 + x_1x_2 + x_3x_2 + x_2 + x_3x_5 + x_1^2 + x_5^2 + x_1x_4 + x_2x_4.
\end{aligned} \tag{3}$$

Esimerkki 2.5. Käytetään edellisen esimerkin valintoja ja lähetetään viesti $\overline{x} = (1, 0, 1, 1, 0)$. Viesti salataan sijoittamalla vektorin $\overline{x}$ komponentit yhtälöihin (3):

$$\begin{aligned}
y_1 =& 0 + 1 + 0 + 1 + 0 + 0 + 1 + 0 + 1 + 1 + 1 + 0 + 1 + 0 = 7 \equiv 1 \mod 2 \\
y_2 =& 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 1 + 0 + 0 = 4 \equiv 0 \mod 2 \\
y_3 =& 1 + 1 + 1 + 1 + 1 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 0 = 6 \equiv 0 \mod 2 \\
y_4 =& 1 + 1 + 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 + 0 + 0 = 5 \equiv 1 \mod 2 \\
y_5 =& 1 + 0 + 0 + 0 + 0 + 1 + 0 + 1 + 0 = 3 \equiv 1 \mod 2.
\end{aligned}$$

Näin ollen lähetettävä salattu viestivektori on $\overline{y} = (1, 0, 0, 1, 1)$.

Avataan seuraavaksi näin saatu salattu viesti. Koska $\overline{y} = B^{-1}(\overline{v} - \overline{d})$, niin $\overline{v} = B\overline{y} + \overline{d}$. Nyt saadaan

$$\overline{v} = B\overline{y} + \overline{d} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Koska $\mathbf{u} = \mathbf{v}^7 = \mathbf{u}^{9^7} = \mathbf{u}^{63} = \mathbf{u}$, niin lasketaan nyt $\mathbf{v}^7 = (x + x^2 + x^3 + x^4)^7 = x = \mathbf{u}$. Nyt $\overline{u} = (0, 1, 0, 0, 0)$ ja lähetetty viesti saadaan selville laskemalla $\overline{x} = A^{-1}(\overline{u} - \overline{c})$.

$$\overline{x} = A^{-1}(\overline{u} - \overline{c}) = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0-1 \\ 1-0 \\ 0-1 \\ 0-1 \\ 0-1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Huomautus 2.6. Edellä esitetty on yksinkertaistus IM -järjestelmästä. Alkuperäisessä versiossa astetta n olevan kuntalaajennuksen $\mathbb{K}$ sijaan käytetään useita laajennuskuntia $\mathbb{K}_1, \ldots, \mathbb{K}_d$, jossa kunnan $\mathbb{K}_i$ aste on n_i ja $n = n_1 + \cdots + n_d$. Jokaisessa laajennuksessa valitaan oma eksponentti $h_i = q^{\theta_i} + 1$ ja syt$(h_i, q^{n_i} - 1) = 1$. Vektorin $\overline{u}$ n komponenttia jaetaan näihin kuntiin ja muuten edetään kuten edellä on kuvattu.

2.2 Järjestelmän murtaminen

Tässä kappaleessa esitetään, kuinka Imai-Matsumoto -järjestelmästä löytyvää heikkoutta hyväksikäyttäen järjestelmä voidaan murtaa osittain tuntematta käyttäjän valitsemaa vektoriavaruuden kantaa $\{\beta_1, \ldots, \beta_n\}$. Idean esitti ensimmäisenä Jacques Patarin vuonna 1995 [8].

Käytetään Luvun 2.1 mukaista Imai-Matsumoto -järjestelmää. Ensimmäiseksi otetaan yhtälö $\mathbf{v} = \mathbf{u}^h = \mathbf{u}^{q^\theta+1}$ ja korotetaan molemmat puolet potenssiin $q^\theta - 1$ sekä kerrotaan puolittain polynomilla $\mathbf{uv}$. Tällöin on voimassa

$$\mathbf{v}^{q^\theta-1} \cdot \mathbf{uv} = \mathbf{u}^{(q^\theta+1)^{q^\theta-1}} \cdot \mathbf{uv},$$

joka sievenee muotoon

$$\mathbf{uv}^{q^\theta} = \mathbf{u}^{q^{2\theta}-1} \cdot \mathbf{uv} = \mathbf{u}^{q^{2\theta}}\mathbf{v}. \tag{4}$$

Otetaan avuksi seuraava lause.

Lause 2.7. *Olkoon $\mathbb{K}$ äärellinen kunta, jonka karakteristika on q. Tällöin $L : \mathbb{K} \mapsto \mathbb{K}, L(\boldsymbol{v}) = \boldsymbol{v}^q$ on lineaarinen kuvaus.*

Todistus. Osoitetaan, että Määritelmän 1.6 ehdot toteutuvat. Olkoon $\mathbf{v}$,$\mathbf{w} \in \mathbb{K}$ ja $\lambda \in \mathbb{F}_q$.

1. Lauseen 1.13 nojalla

$$L(\mathbf{v} + \mathbf{w}) = (\mathbf{v} + \mathbf{w})^q = \mathbf{v}^q + \mathbf{w}^q = L(\mathbf{v}) + L(\mathbf{w}).$$

2. Lauseen 1.12 nojalla

$$L(\lambda\mathbf{v}) = (\lambda\mathbf{v})^q = \lambda^q\mathbf{v}^q = \lambda\mathbf{v}^q = \lambda L(\mathbf{v}).$$

□

Edellisen lauseen nojalla kunnassa $\mathbb{K}$ alkion korottaminen potenssiin q^k kaikilla $k \in \mathbb{Z}_+$ on lineaarinen kuvaus, jolloin kuvausta vastaa yksikäsitteinen matriisi $P^{(k)} = \{p_{ij}^{(k)}\}, 1 \leq i, j \leq n$. Tällöin

$$\beta_i^{q^k} = \sum_{j=1}^{n} p_{ij}^{(k)} \beta_j, \quad p_{ij}^{(k)} \in \mathbb{F}_q. \tag{5}$$

Kahden kantavektorin tulolle voidaan merkitä

$$\beta_i \beta_j = \sum_{l=1}^{n} m_{ijl} \beta_l, \quad m_{ijl} \in \mathbb{F}_q. \tag{6}$$

Aloitetaan yhtälöstä (4), joka voidaan kirjoittaa muodossa

$$\left(\sum_{j=1}^{n} u_j \beta_j \right) \left(\sum_{i=1}^{n} v_i \beta_i^{q^\theta} \right) = \left(\sum_{k=1}^{n} u_k \beta_k^{q^{2\theta}} \right) \left(\sum_{l=1}^{n} v_l \beta_l \right).$$

Yhtälön (5) nojalla saadaan

$$\left(\sum_{j=1}^{n} u_j \beta_j \right) \left(\sum_{1 \le i,\mu \le n} v_i p_{i\mu}^{(\theta)} \beta_\mu \right) = \left(\sum_{1 \le k,\rho \le n} u_k p_{k\rho}^{(2\theta)} \beta_\rho \right) \left(\sum_{l=1}^{n} v_l \beta_l \right).$$

Laskemalla nämä summien tulot yhtälöstä tulee

$$\sum_{1 \le i,j,\mu \le n} u_j v_i p_{i\mu}^{(\theta)} \beta_j \beta_\mu = \sum_{1 \le k,l,\rho \le n} u_k v_l p_{k\rho}^{(2\theta)} \beta_l \beta_\rho,$$

ja käyttämällä yhtälöä (6) pätee yhtälö

$$\sum_{1 \le i,j,\mu \le n} u_j v_i p_{i\mu}^{(\theta)} m_{j\mu l} \beta_l = \sum_{1 \le k,l,\rho \le n} u_k v_l p_{k\rho}^{(2\theta)} m_{l\rho l} \beta_l. \tag{7}$$

Vertaamalla kantavektorin β_l kertoimia saadaan tästä

$$\sum_{1 \le i,j,\mu \le n} u_j v_i p_{i\mu}^{(\theta)} m_{j\mu l} = \sum_{1 \le k,l,\rho \le n} u_k v_l p_{k\rho}^{(2\theta)} m_{l\rho l}. \tag{8}$$

Kun tunnetaan kertoimet $p_{i\mu}^{(\theta)}, p_{k\rho}^{(2\theta)}, m_{j\mu l}$ ja $m_{l\rho l}$ ja sijoitetaan yhtälöön (8) affiineista muunnoksista $\overline{u} = A\overline{x} + \overline{c}$ ja $\overline{v} = B\overline{y} + \overline{d}$ seuraavat yhtälöt $u_i = c_i + \sum_\delta a_{i\delta} x_\delta$ sekä $v_i = d_i + \sum_\sigma b_{i\sigma} y_\sigma$, saadaan yhtälö, joka on muotoa

$$\sum_{1 \le i,j \le n} \alpha_{ij} x_i y_j + \sum_{1 \le i \le n} (\beta_{il} x_i + \gamma_{il} y_i) + \delta_l = 0, \tag{9}$$

missä $\alpha_{ij}, \beta_{il}, \gamma_{il}$ ja δ_l ovat tuntemattomia kertoimia. Nyt kertoimia α_{ij} on n^2 kappaletta, kertoimia β_{il} ja γ_{il} molempia n kappaletta ja lisäksi yksi δ_l.

Näin ollen kertoimien lukumäärä on $n^2 + 2n + 1 = (n+1)^2$. Järjestelmän murtamiseen käytetään muotoa (9) olevia lineaarisia yhtälöitä.

Murrettavasta järjestelmästä ei tunneta kuin julkiset yhtälöt (3), mutta edellisen päättelyn perusteella yhtälö (9) on voimassa. Sijoittamalla selväkielisiä viestejä salausyhtälöihin (3) saadaan muodostettua selväkielisiä ja salattuja viestipareja $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$. Nämä sijoittamalla yhtälöön (9) saadaan lineaarisia yhtälöitä tuntemattomien muuttujien $\alpha_{ij}, \beta_{il}, \gamma_{il}$ ja δ_l suhteen. Lineaarialgebran avulla voidaan ratkaista nämä muuttujat ja muodostaa maksimaalinen joukko lineaarisesti riippumattomia yhtälöitä, jotka kaikki selväkielisen viestin ja sitä vastaavan salatun viestin muodostamat parit toteuttavat. Nämä yhtälöt ovat lineaarisia sekä joukon $\{x_1, \ldots, x_n\}$ että joukon $\{y_1, \ldots, y_n\}$ suhteen.

Huomautus 2.8. Suurin osa muodostetuista yhtälöistä seuraa yhtälöstä (7). On kuitenkin mahdollista, joskin epätodennäköistä, että joukkoon sisältyy yhtälö (tai useampia), joka ei seuraa siitä. Tällaisten yhtälöiden olemassaolo nopeuttaa järjestelmän murtamista.

Oletetaan, että kaikki saadut yhtälöt seuraavat yhtälöstä (7) ja on saatu muodostettua L kappaletta lineaarisesti riippumattomia yhtälöitä. Kaapatun viestin $\overline{y}_0$ koordinaatit sijoitetaan näihin yhtälöihin, jolloin saadaan L kappaletta lineaarisia yhtälöitä n muuttujan $x_1, \ldots, x_n$ suhteen. Näistä yhtälöistä kaikki eivät enää ole riippumattomia ja riippumattomien yhtälöiden määrä voi riippua vektorista $\overline{y}_0$. Toisin sanoen yhtälöryhmällä on useita ratkaisuja, joista oikea viesti $\overline{x}_0$ on yksi. Merkitään riippumattomien yhtälöiden lukumäärää M. Lineaarialgebran avulla tiedetään, että ratkaisuavaruus on vektoriavaruuden $\mathbb{F}_q^n$ $(n-M)$-dimensioinen lineaarinen aliavaruus. Näin ollen sijoituksen $\overline{y} = \overline{y_0}$ jälkeen yhtälöryhmällä on täsmälleen q^{n-M} ratkaisua.

Koska yhtälöt (7) ja (9) ovat yhtäpitäviä ja oletettiin, että kaikki jälkimmäiset seuraavat edellisestä, niiden ratkaisujen välillä on yksi-yhteen -vastaavuus. Tarkastellaan yhtälön (4) ratkaisuja, kun kiinnitetään $\mathbf{v} = \mathbf{v}_0$. Yhtälöllä on triviaali ratkaisu $\mathbf{u} = 0$ sekä "oikea"ratkaisu $\mathbf{u}_0 = \mathbf{v}_0^{h^{-1}}$. Jos $\mathbf{u}$ on jokin muu ratkaisu, niin tällöin

$$\mathbf{v}_0^{q^\theta - 1} = \mathbf{u}_0^{h(q^\theta - 1)} \quad \text{ja} \quad \mathbf{v}_0^{q^\theta - 1} = \mathbf{u}^{h(q^\theta - 1)},$$

mistä seuraa, että

$$\mathbf{u}_0^{h(q^\theta - 1)} = \mathbf{u}^{h(q^\theta - 1)} \quad \text{ja edelleen} \quad \mathbf{u}_0^{(q^\theta - 1)} = \mathbf{u}^{(q^\theta - 1)}.$$

Jälkimmäinen yhtälö saadaan korottamalla yhtälön molemmat puolet potenssiin h^{-1}. Tästä nähdään, että $\mathbf{u}$ eroaa ratkaisusta $\mathbf{u}_0$ tekijällä, joka on $(q^\theta - 1)$. ykkösjuuri kunnassa $\mathbb{K}$, toisin sanoen $\mathbf{u} = \mathbf{u}_0 \cdot \mathbf{r}$, missä $\mathbf{r} \in \mathbb{K}$ ja

$\mathbf{r}^{q^\theta - 1} = 1$. Toisaalta jos $\mathbf{s}$ on $(q^\theta - 1)$. ykkösjuuri kunnassa $\mathbb{K}$, niin $\mathbf{u} = \mathbf{u}_0 \cdot \mathbf{s}$ on nollasta eroava yhtälön (7) ratkaisu.

Ykkösjuurten lukumäärän selvittämiseksi todistetaan ensin seuraava lemma ja sen jälkeen lause, joiden avulla saadaan selville ykkösjuurten lukumäärä modulo p. Tulokset löytyvät Apostolin teoksesta [1].

Lemma 2.9. *Olkoon* $\text{syt}(x, n) = 1$, *ja olkoon* $\text{ord}\ x = d$ *modulo* n. *Tällöin*

$$\text{ord}\ x^k = \frac{\text{ord}\ x}{\text{syt}(k, d)}.$$

Erityisesti $\text{ord}\ x^k = \text{ord}\ x$, *jos ja vain jos* $\text{syt}(k, d) = 1$.

Todistus. Alkion x^k kertaluku on pienin sellainen positiivinen luku m, että

$$x^{mk} \equiv 1 \mod n.$$

Koska $\text{ord}\ x = d$, niin luku m on myös sellainen pienin positiivinen luku, että

$$mk \equiv 0 \mod d.$$

Tämä on yhtäpitävää sen kanssa, että

$$m \equiv 0 \mod \frac{d}{s},$$

missä $s = \text{syt}(k, d)$. Tämän kongruenssiyhtälön pienin positiivinen ratkaisu on d/s, joten

$$\text{ord}\ x^k = m = \frac{d}{s} = \frac{\text{ord}\ x}{\text{syt}(k, d)}.$$

□

Lause 2.10. *Olkoon* p *pariton alkuluku ja* d *mikä tahansa luvun* $p-1$ *positiivinen tekijä. Tällöin jokaisessa redusoidussa jäännösluokkasysteemissä modulo* p *on täsmälleen* $\varphi(d)$ *alkiota* x, *joille pätee* $\text{ord}\ x = d$. *Erityisesti, kun* $d = \varphi(p) = p - 1$, *on olemassa täsmälleen* $\varphi(p-1)$ *ykkösjuurta modulo* p.

Todistus. Määritellään joukko $A(d) = \{x \mid 1 \leq x \leq p-1$ ja $\text{ord}\ x = d \mod p\}$. Nyt luvut $1, 2, \ldots, p-1$ jakautuvat erillisiin joukkoihin $A(d)$, missä jokainen d on luvun $p-1$ tekijä, sillä alkion kertaluku jakaa aina ryhmän kertaluvun. Olkoon $f(d) = \#A(d)$. Tällöin $f(d) \geq 0$ kaikille d. Koska joukot $A(d)$ ovat erilliset ja jokainen $x = 1, 2, \ldots, p-1$ kuuluu johonkiin näistä joukoista, niin pätee

$$\sum_{d|p-1} f(d) = p - 1.$$

Toisaalta

$$\sum_{d|p-1} \varphi(d) = p - 1,$$

joten

$$\sum_{d|p-1} (\varphi(d) - f(d)) = 0.$$

Tämän summan jokainen termi on nolla, ja sen osoittamiseksi riittää osoittaa, että $f(d) \leq \varphi(d)$. Tällöin joko $f(d) = 0$ tai $f(d) = \varphi(d)$, toisin sanoen ehdosta $f(d) \neq 0$ seuraa, että $f(d) = \varphi(d)$.

Oletetaan, että $f(d) \neq 0$. Tällöin $A(d)$ on epätyhjä, joten on olemassa $a \in A(d)$. Tällöin ord $a = d$, mistä seuraa, että $a^d \equiv 1 \mod p$. Jokainen luvun a potenssi toteuttaa tämän kongruenssin, joten kaikki luvut $a, a^2, \ldots, a^d$ ovat kongruenssiyhtälön

$$x^d - 1 \equiv 0 \mod p$$

keskenään epäkongruentteja ratkaisuja. Kongruenssiyhtälöllä on korkeintaan d ratkaisua, koska moduloluku p on alkuluku, joten luvut $a, a^2, \ldots, a^d$ ovat sen kaikki ratkaisut. Tällöin joukon $A(d)$ jokainen alkio on muotoa a^k, $k = 1, 2, \ldots, d$. Lemman 2.9 nojalla ord $a^k = d$, jos ja vain jos $\text{syt}(k, d) = 1$. Näin ollen joukossa $A(d)$ on $\varphi(d)$ kappaletta lukuja, joiden kertaluku modulo p on d. Näin ollen $f(d) = \varphi(d)$, jos $f(d) \neq 0$.

□

Kunnan $\mathbb{K}$ nollasta eroavat alkiot muodostavat kertalukua $q^n - 1$ olevan syklisen ryhmän, joten Lauseen 2.10 nojalla $(q^\theta - 1)$. ykkösjuuria on olemassa $\text{syt}(q^\theta - 1, q^n - 1) = q^d - 1$ kappaletta, missä $d = \text{syt}(\theta, n)$. Kun lasketaan mukaan nollaratkaisu, saadaan yhtälön (7) ratkaisujen lukumääräksi q^d, jotka vastaavat myös yhtälön (9) ratkaisuja. Näin ollen $n - M = d = \text{syt}(\theta, n)$. Lukua d voidaan pitää mittana siitä, kuinka lähellä ollaan järjestelmän yksikäsitteistä murtamista. Ratkaisut on saatu rajattua d-dimensioiseen avaruuteen, jonka q^d vektorin joukosta etsitään oikeaa lähetettyä viestiä.

Kuinka suuri d voi olla? Seuraava lause antaa ylärajan luvulle d.

Lause 2.11. *Olkoon $n \in \mathbb{Z}_+$, q parillinen kokonaisluku ja θ sellainen kokonaisluku, että ehdot* $\text{syt}(q^\theta + 1, q^n - 1) = 1$ *ja* $q^\theta + 1 < q^n$ *toteutuvat. Tällöin* $d = \text{syt}(\theta, n) \leq n/3$.

Todistus. Tarkastellaan eri mahdollisuuksia.

1. $d = n$; nyt $\theta = kn$ jollakin $k \in \mathbb{Z}_+$. Tällöin

$$q^\theta + 1 = q^{kn} + 1 > q^n,$$

mikä on ristiriita. Siis $d \neq n$.

2. $d = n/2$; nyt $n = 2\theta$, joten

$$q^n - 1 = q^{2\theta} - 1 = (q^\theta - 1)(q^\theta + 1).$$

Näin ollen $\text{syt}(q^n - 1, q^\theta + 1) = q^\theta + 1$, mikä on jälleen ristiriita.

3. $d = n/3$; nyt $n = 3\theta$. Koska $q^\theta \equiv -1 \mod (q^\theta + 1)$, niin

$$q^n - 1 = q^{3\theta} - 1 \equiv (-1)^3 - 1 = -2 \mod (q^\theta + 1).$$

Tällöin $e = \text{syt}(q^\theta + 1, q^n - 1)$ jakaa luvun 2. Koska q on parillinen, ovat sekä $q^\theta + 1$ että $q^n - 1$ parittomia. Tästää seuraa, että $e = 1$ ja $d = n/3$ on mahdollinen.

□

Tämän perusteella oikean viestivektorin etsintä voidaan esitetyllä metodilla rajata aliavaruuteen, jonka dimensio on korkeintaan kolmasosa kaikkien viestivektorien avaruuden $\mathbb{F}_q^n$ dimensiosta. Tällä keinolla järjestelmää ei saada yksikäsitteisesti murrettua, mutta kaikkien mahdollisuuksien läpikäyminen nopeutuu huomattavasti. Jotta Imai-Matsumoto -järjestelmän turvallisuutta halutaan lisätä kestämään tällaiset murtoyritykset, pitää n moninkertaistaa, mikä puolestaan kasvattaa viestien salaamiseen ja avaamiseen kuluvaa aikaa.

2.3 MIIP-3 - Muunnos Imai-Matsumoto -järjestelmästä

Vuonna 1996 julkaisemassaan artikkelissa Patarin esitti muunnoksen Imai-Matsumoto -järjestelmästä. Hän kutsui sitä nimellä MIIP-3: Matsumoto-Imai with Improved Parameters of degree 3 [11].

Olkoon taas $\mathbb{K}$ astetta n oleva äärellisen kunnan $\mathbb{F}_q$ laajennuskunta ja käytetään samoja merkintöjä kuin aikaisemmin. Järjestelmä rakennetaan seuraavin askelin:

1. lasketaan affiinilla muunnoksella $\overline{u} = A\overline{x} + \overline{c}$,
2. lasketaan vektori $\mathbf{v} = \mathbf{u}^{1+q^r+q^s} \in \mathbb{K}$ siten, että $\text{syt}(h = 1 + q^r + q^s, q^n - 1) = 1$,
3. palautetaan toisella affiinilla muunnoksella $\overline{y} = B^{-1}(\overline{v} - \overline{d})$.

Näin saadaan salatun viestin komponenteille y_l julkiset yhtälöt

$$y_l = \sum_{1 \le i,j,k \le n} m_s x_i^a x_j^b x_k^c, \quad m_s \in \mathbb{F}_q,\ a, b, c \in \{0, 1\},\ l = 1, 2, \ldots, n. \qquad (10)$$

Viestin lähettäjä sijoittaa viestivektorin komponentit x_i näihin vastaanottajan julkisiin yhtälöihin ja laskee arvot y_l. Niistä muodostuva vektori $\overline{y} = (y_1, \ldots, y_n)$ lähetetään vastaanottajalle.

MIIP-3 eroaa Imai-Matsumoto -järjestelmästä salaisen eksponentin valinnassa, mikä tuottaa muuttujien x_i suhteen kolmatta astetta olevat yhtälöt komponenteille y_l. IM-järjestelmässä eksponentti h oli muotoa $h = q^\theta + 1$, jolla saatiin toisen asteen yhtälöt komponenteille y_l. Jos salainen eksponentti h valitaan hyvin, MIIP-3 ei murru Kappaleessa 2.2 esitetyllä tavalla. Kuitenkin huonolla eksponentin valinnalla saadaan aikaan järjestelmä, johon kyseinen menetelmä puree. Esimerkiksi, jos valitaan $q = 2$, $r = 1$ ja $s = 2$, saadaan aikaan

$$\mathbf{v} = \mathbf{u}^7.$$

Kertomalla puolittain vektorilla $\mathbf{uv}$ yhtälö saadaan muotoon

$$\mathbf{uv}^2 = \mathbf{u}^8\mathbf{v},$$

joka on samaa muotoa kuin yhtälö (4). Näin ollen järjestelmä on murrettavissa kuten alkuperäinen Imai-Matsumoto -järjestelmä. MIIP-3 on murrettavissa myös yleisessä tapauksessa. Menetelmä perustuu samoihin asioihin kuin seuraavaksi esiteltävän Pieni lohikäärme -järjestelmän murtaminen Kappaleessa 3.2.3 esiteltävällä menetelmällä, joten sitä ei esitetä tässä tutkielmassa. Lisätietoja löytyy Patarinin artikkelista [11].

3 Patarinin Pieni lohikäärme

Imai-Matsumoto -järjestelmä osoittautui haavoittuvaiseksi, joten Patarin teki siitä oman versionsa, jota hän kutsui Pieneksi lohikäärmeeksi (Little Dragon). Muutos IM-järjestelmään on hyvin pieni ja nämä kaksi järjestelmää rakentuvat hyvin samalla tavoin.

3.1 Järjestelmän rakenne

Pieni lohikäärme perustuu samanlaisiin rakenteisiin kuin Imai-Matsumoto. Olkoon $\mathbb{K}$ astetta n oleva kunnan F_q kuntalaajennus ja $\{\beta_1, \ldots, \beta_n\}$ kunnan $\mathbb{K}$ kanta $\mathbb{F}_q$-vektoriavaruutena. Kuntien $\mathbb{K}$ ja $\mathbb{F}_q$ alkiot esitetään kuten Kappaleessa 2.1. Valittu kanta pidetään tälläkin kertaa salassa. Merkitään selväkielisiä viestejä $\overline{x} \in \mathbb{F}_q^n$ ja salattuja viestejä $\overline{y} \in \mathbb{F}_q^n$. Kuten IM-järjestelmässä, myös Pienessä lohikäärmeessä käytetään vektoreita $\overline{u}, \overline{v} \in \mathbb{F}_q^n$.

Eksponentti h, $0 < h < q^n$, valitaan siten, että $h + 1$ on kahden eri q:n potenssin summa. Siis

$$h = q^r + q^s - 1, \quad r \neq s,$$

ja $\text{syt}(h, q^n - 1) = 1$. Nyt luvun q ei tarvitse olla parillinen, ja eksponentit r ja s ovat mielivaltaisesti valittavissa, kunhan h ja $q^n - 1$ ovat suhteellisia alkulukuja, toisin sanoen niiden suurin yhteinen tekijä on yksi. Valittu eksponentti h pidetään salassa, mutta koska mahdollisia eksponentteja on rajallinen ja suhteellisen pieni määrä, täytyy olettaa, että järjestelmän murtaja kokeilee kaikki mahdolliset eksponentit. Kuten IM-järjestelmässä, Pienen lohikäärmeen turvallisuus perustuu muihin seikkoihin.

Seuraavaksi valitaan kaksi salaista lineaarista munnosta, toisin sanoen kaksi kääntyvää $\mathbb{F}_q$-kertoimista $n \times n$ -matriisia A ja B. Alkuperäisessä artikkelissaan Patarin esitti, että valitaan kaksi affiinia muunnosta, kuten IM-järjestelmässä [11]. Tarkastelun yksinkertaistamiseksi tässä kappaleessa käytetään lineaarisia muunnoksia. Asetetaan nyt $\overline{u} = A\overline{x}$, $\overline{y} = B^{-1}\overline{v}$ ja $\mathbf{v} = \mathbf{u}^h \in \mathbb{K}$. Koska eksponentti h valittiin siten, että $h = q^r + q^s - 1$, saadaan yhtälö

$$\mathbf{v} = \mathbf{u}^{q^r + q^s - 1}.$$

Kertomalla puolittain vektorilla $\mathbf{u}$ saadaan

$$\mathbf{uv} = \mathbf{u}^{q^r + q^s} = \mathbf{u}^{q^r}\mathbf{u}^{q^s}. \tag{11}$$

Kuten Luvussa 2.1, tästä yhtälöstä saadaan yhtälöiden (5) ja (6) avulla

$$\sum_{1 \leq i,j \leq n} u_i v_j \beta_i \beta_j = \left(\sum_{i=1}^{n} u_i \beta_i^{q^r} \right) \left(\sum_{j=1}^{n} u_j \beta_j^{q^s} \right)$$

ja edelleen

$$\begin{aligned}\sum_{1\le i,j\le n} m_{ijl}u_iv_j\beta_l &= \left(\sum_{1\le i,\mu\le n} p_{i\mu}^{(r)}u_i\beta_\mu\right)\left(\sum_{1\le j,\nu\le n} p_{j\nu}^{(s)}u_j\beta_\nu\right)\\ &= \sum_{1\le i,j,\mu,\nu\le n} p_{i\mu}^{(r)}p_{j\nu}^{(s)}u_iu_j\beta_\mu\beta_\nu \qquad (12)\\ &= \sum_{1\le i,j,\mu,\nu\le n} p_{i\mu}^{(r)}p_{j\nu}^{(s)}u_iu_jm_{\mu\nu l}\beta_l,\end{aligned}$$

missä $m_{ijl}, p_{ij}^{(k)} \in \mathbb{F}_q$ tunnetaan. Vertaamalla β_l:n kertoimia molemmilla puolilla, saadaan

$$\sum_{1\le i,j\le n} m_{ijl}u_iv_j = \sum_{1\le i,j,\mu,\nu\le n} p_{i\mu}^{(r)}p_{j\nu}^{(s)}u_iu_jm_{\mu\nu l}. \qquad (13)$$

Käyttämällä valittuja lineaarisia muunnoksia $\overline{u} = A\overline{x}$ ja $\overline{v} = B\overline{y}$, ja tekemällä sijoitukset $u_i = \sum_\rho a_{i\rho}x_\rho$ ja $v_j = \sum_\sigma b_{j\sigma}y_\sigma$, saadaan n yhtälöä, jotka ovat muotoa

$$\sum_{1\le i,j\le n} c_{ijl}x_iy_j + \sum_{1\le i\le j\le n} d_{ijl}x_ix_j = 0, \quad l = 1, 2, \ldots, n. \qquad (14)$$

Nämä ovat Pienen lohikäärmeen julkiset salausyhtälöt. Jos halutaan lähettää viesti henkilölle A, etsitään hänen salausyhtälönsä ja sijoitetaan niihin viestin $\overline{x}$ komponentit $x_i, i = 1, 2, \ldots, n$. Tämän jälkeen ratkaistaan lineaariset yhtälöt muuttujien y_j suhteen, joista saadaan lähetettävä salattu viesti $\overline{y}$. Kaapattuaan salatun viestin järjestelmän murtajan on ratkaistava monimutkaisempi epälineaarinen yhtälöryhmä muuttujien x_i suhteen.

Esimerkki 3.1. Valitaan $q^n - 1 = 3^{10} - 1 = 59048$. Nyt muotoa $h = 3^r + 3^s - 1$ olevia eksponentteja, missä $r \neq s$, on 45 kappaletta, joista määrätyt ehdot $0 < h < 3^{10}$ ja $\text{syt}(h, q^n - 1) = 1$ toteuttavia on 41 kappaletta. Nämä on listattu liitteenä olevassa Taulukossa 2.

Vastaanotetun salatun viestin avaaminen tapahtuu Pienessä lohikäärmeessä samoin kun Imai-Matsumoto -järjestelmässä. Vastaanottaja laskee aluksi $\overline{v} = B\overline{y}$, jota vastaavan alkion $\mathbf{v} = \sum v_i\beta_i \in \mathbb{K}$ hän korottaa potenssiin $h^{-1} \mod q^n - 1$, jolloin hän saa vektorin $\mathbf{u} = u_i\beta_i$. Viesti saadaan selväkieliseksi laskemalla lopuksi $\overline{x} = A^{-1}\overline{u}$. Kuvassa 2 on havainnollistettu Pienen lohikäärmeen rakentaminen ja viestin avaaminen.

Esimerkki 3.2. Havainnollistetaan Pieni lohikäärme -järjestelmää yksinkertaisella esimerkillä. Valitaan samat parametrit kuin Esimerkissä 2.4, jolloin

Rakentaminen	**Salaaminen**	**Avaaminen**
$\mathbf{v} = \mathbf{u}^h$		$y_1, y_2, \ldots, y_n$
$\Downarrow$		$\Downarrow$
$\mathbf{uv} = \mathbf{u}^{q^r}\mathbf{u}^{q^s}$	$\overline{x} = (x_1, x_2, \ldots, x_n)$	$\overline{v} = B\overline{y}$
$\Downarrow$	$\Downarrow$	$\Downarrow$
sijoitus $\overline{u} = A\overline{x}, \overline{v} = B\overline{y}$	sijoitus yhtälöihin (14)	$\mathbf{v} = \sum v_i\beta_i$
$\Downarrow$	ja ratkaisu y_j suhteen	$\Downarrow$
$\sum_{1\le i,j\le n} c_{ijl}x_iy_j +$	$\Downarrow$	$\mathbf{u} = \mathbf{v}^{h^{-1}}$
$\sum_{1\le i\le j\le n} d_{ijl}x_ix_j = 0$	$\overline{y} = (y_1, y_2, \ldots, y_n)$	$\Downarrow$
		$\overline{x} = A^{-1}\overline{u}$

Kuva 2: Pienen lohikäärmeen rakentaminen, viestin salaaminen ja avaaminen.

$q = 2$, $n = 5$ ja $\mathbb{K} = \mathbb{F}_2[x]/\langle x^5 + x^4 + x^3 + x + 1\rangle$. Kannaksi valittiin $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\} = \{1, x, x^2, x^3, x^4\}$ ja valitaan nyt $r = 3$ ja $s = 1$, jolloin $h = 2^3 + 2^1 - 1 = 9$ ja $h^{-1} = 7 \mod q^n - 1 = 31$. Lisäksi valittiin kääntyvät matriisit

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Asetetaan nyt

$$\overline{u} = A\overline{x} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} x_1 + x_3 + x_4 \\ x_2 + x_3 + x_5 \\ x_1 + x_2 + x_5 \\ x_2 + x_4 \\ x_4 + x_5 \end{pmatrix}$$

ja

$$\overline{v} = B\overline{y} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix} = \begin{pmatrix} y_1 + y_4 + y_5 \\ y_3 + y_4 \\ y_1 + y_2 + y_5 \\ y_1 + y_2 \\ y_1 \end{pmatrix}.$$

Muodostetaan nyt muotoa (11) oleva yhtälö,

$$\mathbf{uv} = \mathbf{u}^8\mathbf{u}^2,$$

missä $\mathbf{u} = u_1\beta_1 + u_2\beta_2 + u_3\beta_3 + u_4\beta_4 + u_5\beta_5$ ja $\mathbf{v} = v_1\beta_1 + v_2\beta_2 + v_3\beta_3 + v_4\beta_4 + v_5\beta_5$. Kun lasketaan nämä modulo $x^5 + x^4 + x^3 + x + 1$ ja verrataan

kantavektorien β_i, $i = 1, \ldots, 5$ kertoimia puolittain, saadaan viisi muotoa (14) olevaa yhtälöä:

$$
\begin{aligned}
\text{I)}\quad & x_1y_4 + x_1y_5 + x_3y_4 + x_3y_5 + x_1y_2 + x_4y_3 + x_5y_3 + x_5y_4 + \\
& + x_2y_2 + x_2y_5 + x_1y_1 + x_2y_1 + x_4y_1 + x_4y_2 + x_4y_5 + x_5y_1 + \\
& x_5y_5 + x_1x_3 + x_3^2 + x_1x_2 + x_2^2 + x_2x_3 + x_1x_5 + x_2x_4 \\
& + x_2x_5 + x_4x_5 + x_5^2 = 0 \\
\text{II)}\quad & x_1y_3 + x_1y_4 + x_3y_3 + x_2y_4 + x_3y_5 + x_5y_4 + x_5y_5 + x_1y_1 + x_1y_2 \\
& + x_5y_3 + x_5y_4 + x_4y_5 + x_2y_1 + x_5y_1 + x_2^2 + x_1x_2 + x_1x_4 \\
& + x_3x_4 + x_2x_4 + x_2x_5 + x_5^2 = 0 \\
\text{III)}\quad & x_1y_2 + x_3y_1 + x_3y_2 + x_3y_5 + x_2y_3 + x_3y_3 + x_3y_4 + x_5y_3 + x_1y_4 \\
& + x_2y_5 + x_1y_1 + x_2y_1 + x_5y_2 + x_2y_2 + x_4y_2 + x_2x_3 + x_1x_4 \\
& + x_1x_5 + x_3x_5 + x_3^2 + x_1^2 + x_2x_5 + x_5^2 = 0 \\
\text{IV)}\quad & x_3y_5 + x_1y_3 + x_1y_4 + x_2y_3 + x_3y_1 + x_4y_3 + x_2y_5 + x_1y_1 \\
& + x_4y_5 + x_4y_2 + x_5y_1 + x_3^2 + x_3x_4 + x_1^2 + x_1x_3 + x_1x_2 + x_2^2 \\
& + x_1x_4 + x_1x_5 + x_2x_5 + x_4^2 + x_5^2 = 0 \\
\text{V)}\quad & x_3y_2 + x_2y_3 + x_2y_4 + x_1y_5 + x_3y_1 + x_4y_4 + x_5y_3 + x_4y_1 + x_1y_1 \\
& + x_3x_5 + x_1^2 + x_1x_2 + x_1x_4 + x_2x_3 + x_5^2 + x_2x_4 = 0.
\end{aligned}
\tag{15}
$$

Kaikki tähän asti tehty suoritetaan salassa ja valitut parametrit pidetään omana tietona. Järjestelmästä julkaistaan yhtälöt (15), joiden avulla viestit salataan.

Esimerkki 3.3. Salataan viesti $\overline{x} = (1, 0, 0, 0, 1)$ Esimerkin 3.2 järjestelmällä. Ensin sijoitetaan komponentit x_i yhtälöihin (15), jolloin saadaan

$$
\begin{aligned}
\text{I)}\quad & y_4 + y_5 + y_2 + y_3 + y_4 + y_1 + y_1 + y_5 + 1 + 1 \\
& = y_2 + y_3 = 0 \\
\text{II)}\quad & y_3 + y_4 + y_4 + y_5 + y_1 + y_2 + y_3 + y_4 + y_1 + 1 \\
& = y_2 + y_4 + y_5 + 1 = 0 \\
\text{III)}\quad & y_2 + y_3 + y_4 + y_1 + y_2 + 1 + 1 + 1 \\
& = y_1 + y_3 + y_4 + 1 = 0 \\
\text{IV)}\quad & y_3 + y_4 + y_1 + y_1 + 1 + 1 + 1 \\
& = y_3 + y_4 + 1 = 0 \\
\text{V)}\quad & y_5 + y_3 + y_1 + 1 + 1 \\
& = y_1 + y_3 + y_5 = 0.
\end{aligned}
$$

Ratkaisemalla tämä yhtälöryhmä muuttujien y_i suhteen, saadaan salattu viesti $\overline{y} = (0, 0, 0, 1, 0)$, joka lähetetään vastaanottajalle.

Viesti avaaminen tapahtuu samoin kuin IM-järjestelmässä. Ensin lasketaan

$$\overline{v} = B\overline{y} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Tätä vastaava kunnan $\mathbb{K}$ alkio korotetaan nyt potenssiin h^{-1}, jolloin saadaan $\mathbf{u} \in \mathbb{K}$. Nyt $\mathbf{u} = \mathbf{v}^{h^{-1}} = \mathbf{v}^7 = (1+x)^7 = x^4+x+1 \mod x^5+x^4+x^3+x+1$. Tämän perusteella $\overline{u} = (1,1,0,0,1)$ ja viesti saadaan avattua laskemalla

$$\overline{x} = A^{-1}\overline{u} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

3.2 Järjestelmän murtaminen

Vaikka Patarin loi parannetun järjestelmän, Pienestä lohikäärmeestä ei tullut aukotonta. Se kestää yksinkertaisen raakaa lineaarialgebraa käyttävän kryptoanalyysin, kuten seuraavaksi osoitetaan. Kuitenkin nähdään, että järjestelmässä eksponentin h valinta täytyy tehdä huolella, sillä tietyillä eksponenteilla järjestelmä murtuu helposti. Lopuksi esitetään metodi, jolla Pieni lohikäärme murtuu millä tahansa käytetyllä eksponentilla.

3.2.1 Raaka kryptoanalyysi

Yritetään murtaa Pieni lohikäärme käyttämällä lineaarialgebraa. Koska mahdollisia eksponentteja h on varsin vähän, oletetaan, että valittu eksponentti tunnetaan. Järjestelmässä käytettyä kantaa ei tunneta, mutta sen tilalle voidaan valita mikä tahansa kanta. Tällöin lineaariset yhtälöt alkioiden $\overline{u}$ ja $\overline{x}$ sekä $\overline{v}$ ja $\overline{y}$ välillä muuttuvat, mutta ne ovat edelleen lineaarisia, jolloin niitä vastaavat matriisit A' ja B'. Valittua omaa kantaa käyttämällä johdetaan vastaavat muotoa (13) olevat yhtälöt. Käyttämällä murrettavan järjestelmän julkaistuja yhtälöitä, muodostetaan useita selkotekstin ja salatun tekstin pareja $(x_1, \ldots, x_n, y_1, \ldots, y_n)$. Nämä sijoitetaan yhtälöihin

$$\overline{u} = A'\overline{x}, \quad \overline{v} = B'\overline{y},$$

jotka ovat komponenttien u_i ja v_j esitykset tuntemattomien matriisien A' ja B' $2n^2$ alkion suhteen. Nämä sijoitetaan itse muodostettuihin muotoa (13)

oleviin yhtälöihin. Jokainen selkotekstin ja salatun tekstin pari tuottaa n yhtälöä, joissa tuntemattomia ovat matriisien A' ja B' alkiot. Nämä yhtälöt ovat muotoa

$$\sum_{1\leq i,j\leq n} m_{ijl}a'_{ij}b'_{kl}x_iy_j = \sum_{1\leq i,j,\mu,\nu\leq n} m_{\mu\nu l}p^{(r)}_{i\mu}p^{(s)}_{j\nu}a'_{ij}a'_{kl}x_ix_j.$$

Näin saaduissa yhtälöissä esiintyy muotoa $a_{ij}b_{kl}$ tai $a_{ij}a_{kl}$ olevia tuntemattomien muuttujien tuloja. Koska $n\times n$-matriisissa on korkeintaan n^2 erisuurta alkiota, erilaisia kahden alkion tuloja on korkeintaan n^4 kummassakin tapauksessa, joten voidaan sanoa, että niitä on $\mathcal{O}(n^4)$ kappaletta. Nämä yhtälöt ovat neliöllisiä, mutta ne voidaan muokata lineaarisiksi sijoittamalla uudet muuttujat w_p yhtälöihin, joista jokainen w_p vastaa tiettyä tuntemattomien muuttujien tuloa $a_{ij}b_{kl}$ tai $a_{ij}a_{kl}$. Seuraavaksi halutaan lineaarialgebraa käyttämällä ratkaista nämä muuttujat w_p ja lopulta niiden avulla alkuperäiset $2n^2$ tuntematonta matriisien A' ja B' alkiota. Tätä varten on generoitava riittävästi yhtälöitä muuttujien w_p suhteen sijoittamalla pareja $(x_1,\ldots,x_n,y_1,\ldots,y_n)$ julkisiin yhtälöihin.

Muuttujien w_p sijoituksen jälkeen yhtälöt ovat

$$\sum_{1\leq i,j\leq n} m_{ijl}w_px_iy_j = \sum_{1\leq \mu,\nu\leq n, 1\leq i\leq j\leq n} m_{\mu\nu l}p^{(r)}_{i\mu}p^{(s)}_{j\nu}w_sx_ix_j,$$

missä w_p, w_s ovat jotkin $\mathcal{O}(n^4)$ muuttujasta. Muistetaan, että $m_{ijl}, m_{\mu\nu l}, p^{(r)}_{i\mu}$ ja $p^{(s)}_{j\nu}$ riippuvat valitusta kannasta ja ne tunnetaan. Tulot $x_iy_j, x_ix_j \in \mathbb{F}_q$ vaihtelevat sen mukaan, minkälaisia pareja on generoitu julkisista yhtälöistä. Näin ollen ainoat tuntemattomat ovat muuttujat w_p. Kertoimia x_iy_j on nyt n^2 kappaletta ja kertoimia x_ix_j $n(n+1)/2$ kappaletta.

Muodostetaan nyt jokaiselle yhtälölle $l = 1,\ldots,n$ kuvaus Φ_l joukolta $\mathbb{F}_q^{n^2+n(n+1)/2}$ $\mathcal{O}(n^4)$ muuttujan w_p lineaaristen yhtälöiden avaruudelle. Olkoon $\overline{z} = (z_1, z_2, \ldots, z_{n^2+n(n+1)/2})$. Asetetaan nyt

$$\Phi_l(\overline{z}) = \sum_{1\leq i,j\leq n} m_{ijl}w_pz_p + \sum_{1\leq k,\mu,\nu\leq n, 1\leq i\leq j\leq n} m_{\mu\nu l}p^{(r)}_{i\mu}p^{(s)}_{j\nu}w_sz_s,$$

missä alkion $\overline{z}$ n^2 ensimmäistä komponenttia sijoitetaan järjestyksessä kertoimien z_p paikalle ja loput $n(n+1)/2$ komponenttia sijoitetaan järjestyksessä kertoimien z_s paikalle.

Nyt jokainen yhtälö muuttujien w_p suhteen tulee olemaan jonkun kuvauksen Φ_l, $l = 1,\ldots,n$, kuvajoukossa. Jokaisen kuvajoukon dimensio on korkeintaan $n^2 + n(n+1)/2$, joten lineaarisesti riippumattomia yhtälöitä on mahdollista generoida korkeintaan $\mathcal{O}(n^3)$ kappaletta. Toisin sanoen, koska

kertoimia z_i on korkeintaan $n^2 + n(n+1)/2$ kappaletta ja kuvauksia Φ_l n kappaletta, on lineaarisesti riippumattomien yhtälöiden määrä muuttujien w_p suhteen korkeintaan

$$n\Big(n^2 + \frac{n(n+1)}{2}\Big) = n^3 + \frac{n^3+n^2}{2} = \frac{3}{2}n^3 + \frac{1}{2}n^2 = \mathcal{O}(n^3).$$

Koska muuttujia w_p on $\mathcal{O}(n^4)$ kappaletta, niin riippumattomia yhtälöitä ei ole tarpeeksi kaikkien muuttujien ratkaisemiseen. Näin ollen alkuperäiset $2n^2$ tuntematonta matriisien A' ja B' alkiota jäävät ratkaisematta eikä järjestelmää saada murrettua.

3.2.2 Heikot eksponentit

Olkoon $\mathbb{K}$ astetta n oleva kunnan $\mathbb{F}_2$ kuntalaajennus. Tämän kunnan ympärille rakennettu Pieni lohikäärme -järjestelmä on haavoittuvainen, jos eksponentti h valitaan huonosti. Kappaleessa 3.1 esitettiin, että eksponentin h on täytettävä ehdot $h = q^r + q^s - 1$ ja $\text{syt}(h, q^n - 1) = 1$ ja nyt on valittu $q = 2$. Tarkastellaan nyt yhtälöä

$$\mathbf{v} = \mathbf{u}^h. \tag{16}$$

Eksponentti h *on heikko*, jos yhtälöstä (16) saadaan operaatioilla

1. korotetaan molemmat puolet johonkin potenssiin a, jolle $\text{syt}(a, 2^n - 1) = 1$,
2. kerrotaan yhtälö puolittain joillakin vektorien $\mathbf{u}$ ja $\mathbf{v}$ potensseilla,

yhtälö

$$\mathbf{v}^{2^{i_1}+2^{i_2}+\cdots+2^{i_k}}\mathbf{u}^{2\alpha} = \mathbf{v}^{2^{j_1}+2^{j_2}+\cdots+2^{i_{k'}}}\mathbf{u}^{2\beta}, \tag{17}$$

missä kakkosen potenssien määrä eksponenteissa on melko pieni, esimerkiksi $k, k' \leq 5$.

Huomautus 3.4. Yhtälöt (16) ja (17) ovat yhtäpitäviä ainoastaan silloin, kun $q = 2$. Jos q on jokin muu alkuluvun potenssi, niin yhtälöllä (17) on jokaisen nollasta eroavan ratkaisun $\mathbf{u}$,$\mathbf{v}$ lisäksi ratkaisut $\alpha\mathbf{u}$,$\mathbf{v}$ kaikille nollasta eroaville $\alpha \in \mathbb{F}_q$, koska Lauseen 1.12 nojalla $\alpha^q = \alpha$.

Esimerkki 3.5. Olkoon $\mathbb{K}$ astetta 6 oleva kunnan $\mathbb{F}_2$ kuntalaajennus. Tällöin $h = 2^4 + 2^2 - 1 = 19$ on heikko eksponentti, sillä korottamalla yhtälön (16) molemmat puolet kuutioon ja kertomalla puolittain vektorilla $\mathbf{u}^8$ saadaan muotoa (17) oleva yhtälö

$$\mathbf{v}^{1+2}\mathbf{u}^{2^3} = \mathbf{u}^{65} = \mathbf{u}^2 \mod 2^6 - 1 = 63.$$

Tässä yhtälössä $k = 2$, $k' = 0$, $\alpha = 3$ ja $\beta = 1$.

Tarkastellaan, kuinka järjestelmä murretaan, kun eksponentti on heikko. Lauseen (2.7) nojalla kuvaukset $\mathbf{v} \mapsto \mathbf{v}^{2^{i_\mu}}$ ovat lineaarisia kaikille $\mathbf{v} \in \mathbb{K}$. Muokataan nyt yhtälöä (17) kuten aikaisemmin käyttämällä hyväksi yhtälöitä (5) ja (6). Nyt yhtälön vasemmasta puolesta saadaan

$$\begin{aligned}\mathbf{v}^{2^{i_1}+2^{i_2}+\cdots+2^{i_k}}\mathbf{u}^{2\alpha} &= \left(\sum_{s_1=1}^{n} v_{s_1}\beta_{s_1}^{2^{i_1}}\right)\cdots\left(\sum_{s_k=1}^{n} v_{s_k}\beta_{s_k}^{2^{i_k}}\right)\left(\sum_{s_0=1}^{n} u_{s_0}\beta_{s_0}^{2^{\alpha}}\right)\\ &= \left(\sum_{1\le s_1,\mu\le n} p_{s_1\mu}^{(i_1)} v_{s_1}\beta_\mu\right)\cdots\left(\sum_{1\le s_k,\nu\le n} p_{s_k\nu}^{(i_k)} v_{s_k}\beta_\nu\right)\left(\sum_{1\le s_0,\lambda\le n} p_{s_0\lambda}^{(\alpha)} u_{s_0}\beta_\lambda\right)\\ &= \sum_{1\le\mu,\nu,\lambda,s_0\le n,1\le s_1\le\cdots\le s_k\le n} p_{s_1\mu}^{(i_1)}\cdots p_{s_k\nu}^{(i_k)} p_{s_0\lambda}^{(\alpha)} m_{l_1} v_{s_1}\cdots v_{s_k} u_{s_0}\beta_m.\end{aligned}$$

Vastaavasti yhtälön oikeasta puolesta saadaan

$$\sum_{1\le\gamma,\delta,\epsilon,t_0\le n,1\le t_1\le\cdots\le t_{k'}\le n} p_{t_1\gamma}^{(j_1)}\cdots p_{t_{k'}\delta}^{(j_{k'})} p_{t_0\epsilon}^{(\beta)} m_{l_2} v_{t_1}\cdots v_{t_{k'}} u_{t_0}\beta_m.$$

Vertaamalla kantavektorin β_m kertoimia saadaan sijoittamalla komponentit u_i, v_j yhtälöistä $u_i = \sum_p a_{ip}x_p$ ja $v_j = \sum_s b_{js}y_s$ aikaiseksi yhtälöt

$$\begin{aligned}&\sum_{1\le s_1\le\cdots\le s_k\le n,1\le s_0\le n} e_{s_1,\ldots,s_k,s_0,l}\, y_{s_1}y_{s_2}\cdots y_{s_k}x_{s_0}\\ &= \sum_{1\le t_1\le\cdots\le t_k\le n,1\le t_0\le n} f_{t_1,\ldots,t_{k'},t_0,l}\, y_{t_1}y_{t_2}\cdots y_{t_{k'}}x_{t_0},\end{aligned} \tag{18}$$

$l = 1, 2, \ldots, n$, missä

$$e_{s_1,\ldots,s_k,s_0,l} = p_{s_1\mu}^{(i_1)}\cdots p_{s_k\nu}^{(i_k)} p_{s_0\lambda}^{(\alpha)} m_{l_1} b_{s_1e_1}\cdots b_{s_ke_k} a_{s_0e_0} \in \mathbb{F}_q$$

ja

$$f_{t_1,\ldots,t_{k'},t_0,l} = p_{t_1\gamma}^{(j_1)}\cdots p_{t_{k'}\delta}^{(j_{k'})} p_{t_0\epsilon}^{(\beta)} m_{l_2} b_{t_1f_1}\cdots b_{t_{k'}f_{k'}} a_{t_0f_0} \in \mathbb{F}_q.$$

Oletetaan taas, että järjestelmän salainen eksponentti h tunnetaan ja se on edellä esitetyssä mielessä heikko, jolloin yhtälöstä (16) seuraa yhtälö (17). Tällöin tiedetään, että kaikki selkotekstin ja salatun tekstin parit toteuttavat n muotoa (18) olevaa yhtälöä. Toisaalta jokaista salattua viestiä $\overline{y}$ vastaa täsmälleen yksi selkokielinen viesti $\overline{x}$. Näin ollen salattu viesti sijoitetaan lineaariseen yhtälöryhmään, josta saadaan yksikäsitteinen ratkaisu $\overline{x} = (x_1, \ldots, x_n)$.

Tätä varten on ensin selvitettävä tuntemattomat muuttujat $e_{s_1,\ldots,s_k,s_0,l}$ ja $f_{t_1,\ldots,t_{k'},t_0,l}$. Generoidaan taas useita pareja $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, jotka sijoitetaan yhtälöihin (18), joista jokainen tuottaa n lineaarista yhtälöä tuntemattomien suhteen. Olkoon $z = \max\{k, k'\}$. Koska jokainen u_i ja v_i voidaan

esittää n termin summana, niiden tulot muodostavat yhtälöihin (18) $\mathcal{O}(n^{z+1})$ termiä. Koska näitä yhtälöitä on n kappaletta, niin tällöin tuntemattomia muuttujia on $\mathcal{O}(n^{z+2})$. Sijoittamalla yhtä monta viestiparia $(x_1, \ldots, y_n)$ yhtälöihin saadaan riittävästi lineaarisesti riippumattomia yhtälöitä muuttujien $e_{s_1,\ldots,s_k,s_0,l}$ ja $f_{t_1,\ldots,t_{k'},t_0,l}$ suhteen, jotta ne voidaan ratkaista. Koska yhtälöt ovat nyt lineaarisia muuttujien x_i suhteen, saadaan järjestelmä murrettua. Kaapattu viesti voidaan avata sijoittamalla sen komponentit y_i yhtälöihin (18) ja ratkaisemalla niistä komponentit x_i.

3.2.3 Coppersmith-Patarin -menetelmä

Mikäli Pienen lohikäärmeen salainen eksponentti valitaan huolimattomasti, järjestelmän murtaminen helpottuu huomattavasti. Vaikka eksponentin valinta tehtäisiin huolella, järjestelmän murtaminen on silti mahdollista, vaikkakin hieman työläämpää. Tarkastellaan nyt menetelmää, jolla se voidaan tehdä [11].

Määritelmä 3.6. Olkoon V, W ja X vektoriavaruuksia kunnan $\mathbb{K}$ yli. Kuvaus $B : V \times W \mapsto X$ on *bilineaarinen*, jos

1. kuvaus $B_w : V \mapsto X$, $v \to B(v, w)$, kaikille $w \in W$ on lineaarinen ja
2. kuvaus $B_v : W \mapsto X$, $w \to B(v, w)$, kaikille $v \in V$ on lineaarinen.

Toisin sanoen jos bilineaarisen kuvauksen kumpi tahansa muuttuja kiinnitetään, tuloksena on lineaarinen kuvaus toisen muuttujan suhteen.

Olkoon Y $\mathbb{F}_q$-kertoiminen n-dimensioinen vektoriavaruus, joka sisältää kaikki mahdolliset salatut viestit $\overline{y} = (y_1, \ldots, y_n)$. Oletetaan nyt, että on olemassa sellainen bilineaarinen kuvaus

$$* : Y \times Y \mapsto Y, \quad (\overline{y}, \overline{y}') \to \overline{y}'' = \overline{y} * \overline{y}',$$

että ehdoista $\overline{v} = B\overline{y}$, $\overline{v}' = B\overline{y}'$ ja $\overline{v}'' = B\overline{y}''$ seuraa $\mathbf{v}'' = \mathbf{v}\mathbf{v}'$. Toisin sanoen, kuvauksesta $*$ tulee kunnan $\mathbb{K}$ kertolaskuoperaatio, kun kuvaus muunnetaan matriisin B avulla vektoreille $\overline{v}$. Järjestelmän murtamiseen kuitenkin riittää, että kuvaus $*$ täyttää seuraavan ehdon: on olemassa sellainen nollasta eroava $\mu \in \mathbb{K}$, että matriisia B käyttämällä saadut vektorit toteuttavat yhtälön

$$\mathbf{v}'' = \mu\mathbf{v}\mathbf{v}'. \tag{19}$$

Olkoon $\overline{y}$ salattu viesti. Määritellään nyt $\overline{y}'' = \overline{y} * \overline{y}$. Seuraavaksi määritellään $\overline{y}''' = \overline{y} * \overline{y}''$ ja jatketaan samoin. Näin saadaan määriteltyä

$$\overline{y}^{(j)} = \overline{y} * \overline{y}^{(j-1)}, \quad j = 2, 3, \ldots, h^{-1}.$$

Samoin saadaan

$$\overline{v}^{(j)} = B\overline{y}^{(j)}, \quad j = 1, 2, \ldots, h^{-1}.$$

Tässä on muistettava tehdä ero sille, onko eksponentin ympärille kirjoitettu sulkeet vai ei. Eksponentti (j) tarkoittaa nyt operaation $*$ j-kertaista iteraatiota, mutta eksponentti j tarkoittaa tavallista vektorin potenssiin korotusta. Koska määriteltiin $\overline{y}'' = \overline{y} * \overline{y}$, niin kertomalla puolittain matriisilla B saadaan

$$B\overline{y}'' = B(\overline{y} * \overline{y}) = B\overline{y} * B\overline{y}.$$

Koska $\overline{v} = B\overline{y}$, tämä on yhtäpitävää yhtälön

$$\mathbf{v}'' = \mathbf{v} * \mathbf{v} = \mu\mathbf{v}\mathbf{v}$$

kanssa. Tässä on käytetty hyväksi tietoa, että operaation $*$ on toteutettava yhtälö (19). Samoin pätee

$$\mathbf{v}''' = \mu\mathbf{v}\mathbf{v}'' = \mu\mathbf{v}^3$$

ja yleisesti

$$\mathbf{v}^{(j)} = \mu^{j-1}\mathbf{v}^j, \quad j = 1, 2, \ldots h^{-1}.$$

Näistä valitaan lähempään tarkasteluun viimeisin yhtälö, missä $j = h^{-1}$. Koska $\mathbf{u} = \mathbf{v}^{h^{-1}}$, niin

$$\mathbf{v}^{(h^{-1})} = \mu^{h^{-1}-1}\mathbf{v}^{h^{-1}}$$

$$\mathbf{v}^{(h^{-1})}\mu^{-(h^{-1}-1)} = \mathbf{v}^{h^{-1}} = \mathbf{u}.$$

Olkoon M alkiolla $\mu^{-(h^{-1}-1)} \in \mathbb{K}$ kertomista vastaava matriisi valitun kannan $\beta_1, \ldots, \beta_n$ suhteen. Tällöin pätee

$$\overline{x} = A^{-1}\overline{u} = A^{-1}M\overline{v}^{(h^{-1})} = A^{-1}MB\overline{y}^{(h^{-1})} = C\overline{y}^{(h^{-1})}, \tag{20}$$

missä on merkitty $C = A^{-1}MB$. Matriisi $C = \{c_{ij}\}, 1 \leq i, j \leq n$, alkiot saadaan selvitettyä lineaarialgebralla. Generoidaan taas selkotekstin ja salatun tekstin pareja $\overline{x}_l = (x_{1l}, \ldots, x_{nl}), \overline{y}_l = (y_{1l}, \ldots, y_{nl}), l = 1, \ldots, L$. Salatut tekstit korotetaan operaatiolla $*$ potenssiin h^{-1} ja ne sijoitetaan yhtälöön (20). Jokainen generoitu pari tuottaa nyt n lineaarista yhtälöä matriisin C alkioiden suhteen. Pareja voi joutua generoimaan hieman enemmän kuin n kappaletta, sillä alkioiden c_{ij} esiintyminen yhtälöissä riippuu käytetyistä pareista. Kuitenkin jollakin $L > n$ saadaan riittävä määrä yhtälöitä, joiden avulla saadaan selville kaikki n^2 alkiota c_{ij}. Kun matriisi C tunnetaan, pystytään yhtälön (20) avulla murtamaan kaikki salatut viestit $\overline{y}$ helposti, olettaen että kuvaus $*$ tunnetaan. Enää täytyy löytää kuvaus, joka täyttää edellä mainitut ehdot.

Merkitään nyt kaikille $l = 1, \ldots, n$ yhtälön (14) ensimmäistä summaa $\delta_l = \delta_l(x_1, \ldots, x_n, y_1, \ldots, y_n)$ ja olkoon $\overline{\delta} = (\delta_1, \ldots, \delta_n)$. Nyt summa δ_l seuraa yhtälön (13) vasemmasta puolesta matriisien A ja B kautta, joka puolestaan saatiin yhtälön (11) vasemman puolen tulosta $\mathbf{uv}$. Vaikka yhtälöitä (11), (13), matriiseja A ja B sekä vektoriavaruuden $\mathbb{K}$ kantaa $\beta_1, \ldots, \beta_n$ ei tunneta, tiedetään kuitenkin, että yhtälöt ovat voimassa. Koska $\mathbb{K}$ on myös kunta, niin kaikille $\lambda \in \mathbb{K}$ pätee

$$\lambda(\mathbf{uv}) = \mathbf{u}(\lambda\mathbf{v}).$$

Koska alkiolla λ kertominen on lineaarinen kuvaus, on olemassa sellaiset $n \times n$-matriisit S ja T, $s_{ij}, t_{ij} \in \mathbb{F}_q$, $1 \leq i, j \leq n$, että kaikille pareille $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{F}_q^{2n}$ matriisin $S\overline{\delta}$ l. rivi on

$$(S\overline{\delta})_l = \sum_{1 \leq i,j \leq n} c_{ijl} x_i (T\overline{y})_j, \tag{21}$$

missä $(T\overline{y})_j$ on matriisin $T\overline{y}$ j. rivi. Perustellaan nyt tämä väite.

Matriisi $S\overline{\delta}$ on nyt

$$S\overline{\delta} = \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1n} \\ s_{21} & s_{22} & \ldots & s_{2n} \\ \vdots & & \ddots & \\ s_{n1} & s_{n2} & \ldots & s_{nn} \end{pmatrix} \begin{pmatrix} \sum_{1 \leq i,j \leq n} c_{ij1} x_i y_j \\ \sum_{1 \leq i,j \leq n} c_{ij2} x_i y_j \\ \vdots \\ \sum_{1 \leq i,j \leq n} c_{ijn} x_i y_j \end{pmatrix} =$$

$$\begin{pmatrix} s_{11} \sum_{1 \leq i,j \leq n} c_{ij1} x_i y_j + s_{12} \sum_{1 \leq i,j \leq n} c_{ij2} x_i y_j + \cdots + s_{1n} \sum_{1 \leq i,j \leq n} c_{ijn} x_i y_j \\ s_{21} \sum_{1 \leq i,j \leq n} c_{ij1} x_i y_j + s_{22} \sum_{1 \leq i,j \leq n} c_{ij2} x_i y_j + \cdots + s_{2n} \sum_{1 \leq i,j \leq n} c_{ijn} x_i y_j \\ \vdots \\ s_{n1} \sum_{1 \leq i,j \leq n} c_{ij1} x_i y_j + s_{n2} \sum_{1 \leq i,j \leq n} c_{ij2} x_i y_j + \cdots + s_{nn} \sum_{1 \leq i,j \leq n} c_{ijn} x_i y_j \end{pmatrix},$$

jolloin sen l. rivi voidaan kirjoittaa

$$(S\overline{\delta})_l = \sum_{1 \leq i,j,k \leq n} c_{ijl} s_{lk} x_i y_j.$$

Matriisi $T\overline{y}$ on nyt

$$T\overline{y} = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & \ldots & t_{2n} \\ \vdots & & \ddots & \\ t_{n1} & t_{n2} & \ldots & t_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} t_{11} y_1 + t_{12} y_2 + \cdots + t_{1n} y_n \\ t_{21} y_1 + t_{22} y_2 + \cdots + t_{2n} y_n \\ \vdots \\ t_{n1} y_1 + t_{n2} y_2 + \cdots + t_{nn} y_n \end{pmatrix},$$

joten yhtälön (21) oikeasta puolesta saadaan

$$\sum_{1\leq i,j\leq n} c_{ijl}x_i(T\overline{y})_j = \sum_{1\leq i,j\leq n} c_{ijl}x_i(t_{j1}y_1 + t_{j2}y_2 + \cdots + t_{jn}y_n)$$
$$= \sum_{1\leq i,j,k\leq n} c_{ijl}t_{jk}x_iy_j.$$

Näin ollen yhtälö (21) pätee, kun löydetään sellaiset matriisit S ja T, että $c_{ijl}s_{lk} = c'_{ijl}t_{lk}$ kunnassa $\mathbb{F}_q$.

Näin ollen, jos tunnettaisiin matriisi B ja tietyllä alkiolla λ kertomisen matriisi Λ järjestelmän rakentajan valitsemassa kannassa, voitaisiin asettaa $T = B^{-1}\Lambda B$ ja $S = \Lambda$. Tällöin $\lambda\mathbf{v}$ on vektoria $B^{-1}\Lambda B\overline{y}$ vastaava alkio, ja yhtälön (21) oikea puoli on alkiota $\mathbf{u}(\lambda\mathbf{v})$ vastaavan vektorin β_l-komponentti. Toisaalta yhtälön (21) vasemman puolen l. komponentti vastaa vektorin $\lambda(\mathbf{uv})$ β_l-komponenttia, koska δ_l on vektorin $\mathbf{uv}$ β_l-komponentti, kuten aikaisemmin todettiin.

Matriisit B ja Λ ovat tuntemattomia, mutta tiedetään, että edellä mainitut ehdot toteuttavat matriisit S ja T ovat olemassa. Tällaisten matriisien T joukko, jotka toteuttavat yhtälön (21) on vähintään n-dimensioinen vektoriavaruus kunnan F_q yli. Se sisältää matriisien joukon $B^{-1}\Lambda B$, missä Λ käy läpi kaikki mahdolliset alkiolla $\lambda \in \mathbb{K}$ kertomista vastaavat matriisit. Oletetaan yksinkertaisuuden vuoksi, että matriisien T vektoriavaruuden dimensio on tasan n, eli se sisältää ainoastaan muotoa $B^{-1}\Lambda B$ olevat matriisit. Olkoon $T_1, \ldots, T_n$ kyseisen vektoriavaruuden kanta, jolloin mielivaltainen ratkaisu T voidaan kirjoittaa muodossa $T = t_1T_1 + \cdots t_nT_n$, missä $\bar{t} = (t_1, \ldots, t_n) \in \mathbb{F}_q^n$. Tällainen kanta löydetään yhtälöistä (21) ajattelemalla matriisien S ja T $2n^2$ alkiota muuttujina ja generoimalla riittävästi pareja $(x_1, \ldots, x_n, y_1, \ldots, y_n)$. Kuten aiemmin, nämä parit sijoitetaan muuttujien suhteen lineaarisiin yhtälöihin ja ratkaistaan yhtälöryhmä.

Oletetaan, että on edellä kuvatulla tavalla löydetty vektoriavaruuden kanta $T_1, \ldots, T_n$, ja on olemassa kuvaus $f : \mathbb{K} \mapsto \mathbb{F}_q^n, f(\lambda) = \bar{t}$. Nyt kuvaus f sisältää n kappaletta funktioita $f_i : \mathbb{K} \mapsto \mathbb{F}_q, f_i(\lambda) = t_i$, joista saadaan alkiota λ vastaava matriisi T. Toisin sanoen kaikille $\lambda \in \mathbb{K}$ on voimassa yhtälö

$$\sum f_i(\lambda)T_i = B^{-1}\Lambda B,$$

missä Λ on alkiolla λ kertomisen matriisi kannassa $\beta_1, \ldots, \beta_n$. Nyt tällainen kuvaus f on lineaarinen vektoriavaruudelta $\mathbb{K}$ ratkaisumatriisien T avaruudelle. Olkoon g_i sellainen kuvaus vektoreilta $\overline{y}$ avaruudelle F_q, joka määrittää ensin vektorin

$$\overline{v} = B\overline{y}.$$

Seuraavaksi kuvataan tätä vastaava alkio $\mathbf{v}$ edellä määritetyllä kuvauksella f_i, jolloin saadaan alkio t_i. Alkiosta $\overline{y}$ saadaan siis kuvauksella g_i alkio t_i:

$$g_i(\overline{y}) \to t_i.$$

Jos tunnettaisiin matriisi B ja kuvaus f, operaatio $*$ voitaisiin määritellä

$$\overline{y}'' = \overline{y} * \overline{y}' = \sum_{i=1}^{n} g_i(\overline{y}) T_i \overline{y}'. \tag{22}$$

Tällöin olisi voimassa $\mathbf{v}'' = \mathbf{v}\mathbf{v}'$, sillä

$$\begin{aligned} \overline{y}'' = \overline{y} * \overline{y}' &= \sum_{i=1}^{n} g_i(\overline{y}) T_i \overline{y}' = \sum_{i=1}^{n} t_i T_i \overline{y}' \\ &= T\overline{y}' = B^{-1} V B \overline{y}', \end{aligned}$$

missä V on alkiolla $\mathbf{v}$ kertomisen matriisi. Kertomalla yhtälö puolittain matriisilla B, saadaan

$$\mathbf{v}'' = B\overline{y}'' = BB^{-1}VB\overline{y}' = \mathbf{v}\mathbf{v}'.$$

Edelleen riittää löytää kuvaus, joka toteuttaa yhtälön (19). Kiinnitetään jokin nollasta eroava $\mu \in \mathbb{K}$ ja merkitään kaikille $\lambda \in \mathbb{K}$ alkiolla $\mu\lambda$ kertomisen matriisia Λ' kannan $\beta_1, \ldots, \beta_n$ suhteen. Oletetaan, että $\overline{t} = f(\lambda)$ on lineaarinen siten, että kiinnitetylle alkiolle μ pätee $\sum f_i(\lambda) T_i = B^{-1}\Lambda' B$, kaikille $\lambda \in \mathbb{K}$, ja asetetaan kuvaus g kuten edellä. Nyt, jos tällainen g tunnettaisiin, voitaisiin määritellä kuvaus $*$ kuten yhtälö (22). Tällöin olisi $\mathbf{v}'' = \mu\mathbf{v}\mathbf{v}'$ eli juuri sellainen kuvaus kuin murtamiseen tarvitaan.

Kuvauksen $*$ täytyy olla kommutatiivinen, koska se toteuttaa yhtälön (19), johon osallistuvat vektorit ovat kaikki kunnan $\mathbb{K}$ alkioita. Olkoon $G = \{g_{ij}\}, 1 \leq i, j \leq n$ lineaarista kuvausta $g : g(\overline{y}) = G\overline{y}$ vastaava matriisi. Merkitään matriisin G i. riviä G_i. Jos tunnettaisiin matriisi G, voitaisiin määritellä $*$ asettamalla

$$\overline{y} * \overline{y}' = \sum_{i=1}^{n} G_i \overline{y} T_i \overline{y}'. \tag{23}$$

Matriisin G alkiot g_{ij} ovat tuntemattomia ja yhtälön (23) operaatio on kommutatiivinen, toisin sanoen

$$\sum_{i=1}^{n} G_i \overline{y} T_i \overline{y}' = \sum_{i=1}^{n} G_i \overline{y}' T_i \overline{y}.$$

Merkitään $(T_i)_{\sigma\tau}$ matriisin T_i alkiota rivillä σ ja sarakkeessa τ. Valitaan nyt $\overline{y}$ sellaiseksi luonnollisen kannan vektoriksi, jonka j_1. komponentti on 1, $\overline{y} = e_{j_1}$. Vastaavasti valitaan $\overline{y}' = e_{j_2}$. Matriisin rivin G_i kertominen luonnollisen kannan vektorilla säilyttää rivin j_i. alkion ja muuttaa muut nolliksi. Matriisin T_i kertominen luonnollisen kannan vektorilla vastaavasti säilyttää sarakkeen j_i ennallaan ja muuttaa muut alkiot nolliksi. Verrataan nyt k_0. komponentteja eli niitä termejä edellisessä yhtälössä, joissa esiintyy matriisin T_i rivin k_0 alkioita. Koska kyseisellä rivillä on vain yksi nollasta eroava alkio, saadaan yhtälö

$$\sum_{i=1}^{n} G_{ij_1}(T_i)_{k_0 j_2} = \sum_{i=1}^{n} G_{ij_2}(T_i)_{k_0 j_1}.$$

Koska luonnollisen kannan vektorille j_i on n eri vaihtoehtoa ja jokaiselle $k_0 = 1, 2, \ldots, n$ voidaan muodostaa edellinen yhtälö, saadaan kaiken kaikkiaan n^3 yhtälöä tuntemattomien G_{ij} suhteen. Nyt on olemassa vähintään n-dimensioinen ratkaisuavaruus, koska jokaista $\mu \in \mathbb{K}$ vastaa yksi $n \times n$-matriisi G. Käytännössä on epätodennäköistä, että olisi sellaisia ratkaisuja G, joita ei saada edellä esitetyllä tavalla. Täytyy siis löytää yksi nollasta eroava ratkaisumatriisi G tästä n-dimensioisesta avaruudesta. Kun sopiva ratkaisu on löydetty, määritellään operaatio $*$ kuten yhtälössä (23), joka toteuttaa ehdon (19). Tämän jälkeen järjestelmä on murrettu, sillä kaapattu viesti voidaan avata yhtälöllä (20). Viestivektoria $\overline{y}$ operoidaan kuvauksella (23) h^{-1} kertaa, jonka jälkeen viesti saadaan avattua kertomalla tulos matriisilla C.

4 Paranneltuja lohikäärmeitä

Patarin osoitti itse, että Pieni lohikäärme ei ole turvallinen. Hän esitti toisen samankaltaisen järjestelmän nimeltään Iso lohikäärme, joka ainakin joissain tapauksissa vaikutti kestävän Kappaleen 3.2.3 mukaiset hyökkäykset. Kaksi muuta esiteltävää muunnelmaa ovat tutkijakolmikon Rajesh P. Singh, Anupam Saikia ja B.K. Sarma luomuksia. Ne eroavat kaikista edellä esitetyistä järjestelmistä siinä, että kätkettävä kuvaus on monomin sijasta polynomi. Tässä luvussa käsitellään ainoastaan äärellisiä kuntia $\mathbb{F}_{2^n}$, jolloin jokaisen alkion vasta-alkio on kyseinen alkio itse.

4.1 Iso lohikäärme

Olkoon F_q äärellinen kunta, jonka karakteristika on 2, $\mathbb{K}$ sen astetta n oleva kuntalaajennus sekä $\beta_1, \ldots, \beta_n$ $\mathbb{F}_q$-kertoimisen vektoriavaruuden $\mathbb{K}$ kanta. Käytetään vastaavia merkintöjä kuin Luvussa 3 sekä affiineja muunnoksia $\overline{u} = A\overline{x} + \overline{c}$ ja $\overline{v} = B\overline{x} + \overline{d}$. Matriisit A ja B sekä vektorit $\overline{c}$ ja $\overline{d}$ yhdessä vektoriavaruuden kannan kanssa pidetään salassa. Salainen eksponentti h valitaan niin, että se on muotoa

$$h = q^{r_1} + q^{r_2} - q^{s_1} - q^{s_2}$$

ja se toteuttaa ehdon $\text{syt}(h, q^n - 1) = 1$. Lisäksi valitaan sellainen salassa pidettävä lineaarinen kuvaus $\psi : \mathbb{K} \mapsto \mathbb{K}$, että kuvaus

$$\mathbf{v} \mapsto \psi(\mathbf{v})\mathbf{v}^{-1}$$

on injektio joukolle $\mathbb{K}^*$. Nyt vektorien $\mathbf{u}$ ja $\mathbf{v}$ välinen bijektiivinen yhteys on

$$\mathbf{u}^h = \psi(\mathbf{v})\mathbf{v}^{-1} \tag{24}$$

kaikille $\mathbf{u},\mathbf{v} \in \mathbb{K}, \mathbf{v} \neq 0$. Kun tähän sijoitetaan valittu eksponentti h ja kerrotaan puolittain vektoreilla $\mathbf{v}$ ja $\mathbf{u}^{q^{s_1}+q^{s_2}}$, saadaan yhtälö

$$\mathbf{u}^{q^{r_1}+q^{r_2}}\mathbf{v} = \mathbf{u}^{q^{s_1}+q^{s_2}}\psi(\mathbf{v}). \tag{25}$$

Esimerkki 4.1. Olkoot α sellainen kokonaisluku, että $\text{syt}(\alpha, n) = 1$, ja $\mu, \nu \in \mathbb{K}^*$. Tällöin kuvausta

$$\psi(\mathbf{v}) = \mu\mathbf{v}^{q^\alpha}$$

käyttämällä voidaan muodostaa kuvaus, joka täyttää vaaditun ehdon eli on injektio joukolle $\mathbb{K}^*$, kun $q = 2$. Tällöin

$$\mathbf{v} \mapsto \psi(\mathbf{v})\mathbf{v}^{-1} = \mu\mathbf{v}^{2^\alpha}\mathbf{v}^{-1} = \mu\mathbf{v}^{2^\alpha - 1}.$$

Koska $\text{syt}(\alpha, n) = 1$, niin $\text{syt}(2^\alpha - 1, 2^n - 1) = 1$ ja alkiolle $\mu\mathbf{v}^{2^\alpha - 1}$ löytyy käänteisalkio, joten kuvaus on bijektio. Mille tahansa luvulle q kuvauksen

$$\psi(\mathbf{v}) = \mu\mathbf{v} + \nu$$

avulla saadaan myös muodostettua ehdon täyttävä kuvaus, sillä

$$\mathbf{v} \mapsto \psi(\mathbf{v})\mathbf{v}^{-1} = (\mu\mathbf{v} + \nu)\mathbf{v}^{-1} = \mu\mathbf{v}\mathbf{v}^{-1} + \nu\mathbf{v}^{-1} = \mu + \nu\mathbf{v}^{-1}.$$

Koska $\mu, \nu, \mathbf{v}^{-1} \in \mathbb{K}^*$, niin alkion $\mathbf{v} \neq 0$ kuva on aina joukossa $\mathbb{K}^*$. Näin ollen kuvauksen $\psi(\mathbf{v})\mathbf{v}^{-1}$ ydin koostuu ainoastaan nolla-alkiosta. Lauseen 1.8 nojalla tästä seuraa, että kuvaus on injektio.

Aloittamalla yhtälöstä (25) ja käyttämällä hyväksi yhtälöitä (5) ja (6) sekä edellä valittuja affiineja muunnoksia ja etenemällä Kappaleessa 3.1 esitetyllä tavalla, saadaan muodostettua Ison lohikäärmeen n julkista salausyhtälöä. Yleisesti ne ovat muotoa

$$\begin{aligned} &\sum_{1 \leq i,j,k \leq n} a_{ijk} x_i x_j y_k + \sum_{1 \leq i,j \leq n} b_{ij} x_i x_j + \sum_{1 \leq i,k \leq n} c_{ik} x_i y_k \\ &+ \sum_{1 \leq i \leq n} d_i x_i + \sum_{1 \leq k \leq n} e_k y_k + f_0 = 0. \end{aligned} \tag{26}$$

Viestin lähettäjä sijoittaa viestivektorin komponentit x_i näihin yhtälöihin ja ratkaisee sen jälkeen lineaarisen yhtälöryhmän muuttujien y_l suhteen. Vastaanottaja laskee vastaanotetusta viestistä vektorin $\overline{v} = B\overline{y} + \overline{d}$ ja käyttää yhtälöä (24) vektorin $\mathbf{u}$ ratkaisemiseksi. Lopuksi viesti avataan laskemalla $\overline{x} = A^{-1}(\overline{u} - \overline{c})$.

Jos kuvaus ψ on yleisesti tiedossa, vektori $\psi(\mathbf{v})$ on kenen tahansa laskettavissa. Jos nyt kerrotaan yhtälö (25) puolittain vektorilla $\mathbf{u}^{-q^{r_1} - q^{r_2} + 1}$, saadaan yhtälö

$$\mathbf{u}\mathbf{v} = \mathbf{u}^{q^{s_1} + q^{s_2} - q^{r_1} - q^{r_2} + 1}\psi(\mathbf{v}).$$

Tämä yhtälö vastaa Pienen lohikäärmeen yhtälöä (11), jolloin järjestelmä on altis samanlaiselle hyökkäykselle kuin Kappaleessa 3.2.3.

4.2 Permutaatiopolynomeista

Tässä Kappaleessa tutustutaan lyhyesti permutaatiopolynomeihin, joita käytetään eräissä Pienen lohikäärmeen muunnoksissa [13],[14]. Osoittautuu, että Imai-Matsumoto ja Pieni lohikäärme perustuvat myös yksinkertaisen permutaatiopolynomin - monomin x^h - käyttöön.

Määritelmä 4.2. Olkoon p alkuluku, n jokin positiivinen kokonaisluku ja $\mathbb{F}_q$ äärellinen kunta, missä $q = p^n$. Polynomi $f(x) \in \mathbb{F}_q[X]$ on *permutaatiopolynomi*, jos se on bijektio joukolta $\mathbb{F}_q$ itselleen. Tällöin polynomi f on kunnan $\mathbb{F}_q$ *permutaatio*.

Lause 4.3. *Polynomi f on permutaatiopolynomi, jos yksi seuraavista ehdoista pätee:*

1. *$f : \mathbb{F}_q \mapsto \mathbb{F}_q$ on surjektio,*
2. *$f : \mathbb{F}_q \mapsto \mathbb{F}_q$ on injektio,*
3. *yhtälöllä $f(x) = a$ on ratkaisu kunnassa $\mathbb{F}_q$ kaikille $a \in \mathbb{F}_q$,*
4. *yhtälöllä $f(x) = a$ on yksikäsitteinen ratkaisu kunnassa $\mathbb{F}_q$ kaikille $a \in \mathbb{F}_q$.*

Todistus. Kohdat 1. ja 2. seuraavat suoraan siitä, että kuvaus on joukolta $\mathbb{F}_q$ itselleen, sillä lähtö- ja maalijoukossa on yhtä monta alkiota. Jos yhtälöllä $f(x) = a$ on ratkaisu kunnassa $\mathbb{F}_q$ kaikille $a \in \mathbb{F}_q$, niin f on surjektio ja siten bijektio. Jos yhtälöllä $f(x) = a$ on yksikäsitteinen ratkaisu kunnassa $\mathbb{F}_q$ kaikille $a \in \mathbb{F}_q$, niin ehdosta $f(x) = f(y) = a$ seuraa, että $x = y$. Näin ollen f on injektio ja siten bijektio. □

Määritelmä 4.4. Polynomi $L(x) \in \mathbb{F}_{q^n}[X]$ on *p-polynomi* tai *linearisoitu polynomi* kunnan $\mathbb{F}_q$ yli, jos

$$L(x) = \sum_{i=0}^{k} \alpha_i x^{q^i}, \quad \alpha_i \in \mathbb{F}_{q^n}.$$

Alkiota $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ vastaavaa p-polynomia kunnassa $\mathbb{F}_{2^n}$ merkitään

$$L_\alpha(x) = \sum_{i=0}^{n-1} \alpha_i x^{2^i}.$$

Huomautus 4.5. Määritelmän 4.4 mukainen p-polynomi on lineaarinen kuvaus. Lisäksi Lauseen 1.8 nojalla se on permutaatiopolynomi, jos ja vain jos sen ainoa juuri kunnassa $\mathbb{F}_{q^n}$ on 0.

Esimerkki 4.6. Olkoon $\mathbb{F}_{2^3}$ kunnan $\mathbb{F}_2$ kuntalaajennus, jonka konstruoinnissa käytetään jaotonta polynomia $x^3 + x + 1$. Valitaan nyt $\alpha = (1, 1, 0)$, jolloin sitä vastaava p-polynomi on

$$L_\alpha(x) = \sum_{i=0}^{3-1} \alpha_i x^{2^i} = 1 \cdot x + 1 \cdot x^2 + 0 \cdot x^{2^2} = x + x^2.$$

Määritelmä 4.7 sekä Lause 4.8 löytyvät teoksesta [9].

Määritelmä 4.7. Olkoon Tr sellainen kuvaus kunnalta F_{q^n} kunnalle F_q, että

$$Tr(x) = x + x^q + x^{q^2} + \cdots + x^{q^{(n-1)}}.$$

Tällöin $Tr(x)$ on alkion x *jälki* ja Tr on *jälkifunktio*. Toisin sanoen alkion x jälki on sen konjugaattien summa kunnan $\mathbb{F}_q$ suhteen.

Perustellaan nyt, miksi jälkifunktion kuva on joukossa $\mathbb{F}_q$. Olkoon $f(x) \in \mathbb{F}_q[X]$ alkion $\alpha \in \mathbb{F}_{q^n}$ minimipolynomi, jonka aste d jakaa luvun n. Tällöin alkion α karakteristinen polynomi on $g(x) = f(x)^{m/d} \in \mathbb{F}_q[X]$. Koska minimipolynomi f on jaoton kunnassa $\mathbb{F}_q[X]$ ja $\deg f = d$, niin sen juuret kunnassa $\mathbb{F}_{q^n}$ ovat $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. Alkion α konjugaatit ovat erilliset jos ja vain jos minimipolynomin aste on n. Koska nyt näin ei ole, niin konjugaatit ovat $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ n/d-kertaisina. Koska $g(x) = f(x)^{m/d}$, niin nämä ovat myös karakteristisen polynomin g juuret. Tällöin

$$\begin{aligned}
g(x) =& x^n + a_{n-1}x^{n-1} + \cdots + a_0 \\
=& (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{(n-1)}}) \\
=& (\alpha^{q+1} + (-\alpha-\alpha^q)x + x^2)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{(n-1)}}) \\
=& (-\alpha^{q^2+q+1} + (\alpha^{q+1}+\alpha^{q^2+1}+\alpha^{q^2+q})x + (-\alpha-\alpha^q-\alpha^{q^2})x^2 + x^3) \\
& \cdot (x-\alpha^{q^3})\cdots(x-\alpha^{q^{(n-1)}}) \\
& \vdots \\
=& x^n - \left(\sum_{i=0}^{n-1} \alpha^{q^i}\right) x^{(n-1)} + \left(\sum_{0\le i<j<n} \alpha^{q^i+q^j}\right) x^{(n-2)} + \cdots \\
& - \left(\sum_{0\le i_1<i_2<\cdots<i_{(n-1)}<n} \alpha^{q^{i_1}+q^{i_2}+\cdots+q^{i_{(n-1)}}}\right) x + \alpha^{q^{(n-1)}+q^{(n-2)}+\cdots+q+1},
\end{aligned}$$

ja kertoimia vertailemalla huomataan, että

$$-a_{n-1} = \sum_{i=0}^{n-1} \alpha^{q^i} = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{(n-1)}} = Tr(\alpha).$$

Koska polynomin g kertoimet $a_i \in \mathbb{F}_q$, niin myös $Tr(\alpha) \in \mathbb{F}_q$.

Lause 4.8. *Jälkifunktiolla Tr on seuraavat ominaisuudet:*

1. $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$ *kaikille* $\alpha, \beta \in \mathbb{F}_{q^n}$,

2. $Tr(c\alpha) = cTr(\alpha)$ *kaikille* $c \in \mathbb{F}_q$ *ja* $\alpha \in \mathbb{F}_{q^n}$,

3. $Tr(\alpha^q) = Tr(\alpha)$ *kaikille* $\alpha \in \mathbb{F}_{q^n}$.

Todistus. Olkoon $\alpha, \beta \in \mathbb{F}_{q^n}$ ja $c \in \mathbb{F}_q$.

1. Nyt Lauseen 1.13 nojalla

$$\begin{aligned} Tr(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{(n-1)}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{(n-1)}}+\beta^{q^{(n-1)}} \\ &= \alpha+\alpha^q+\cdots+\alpha^{q^{(n-1)}}+\beta+\beta^q+\cdots+\beta^{q^{(n-1)}} \\ &= Tr(\alpha)+Tr(\beta). \end{aligned}$$

2. Nyt Lauseen 1.12 nojalla $c^{q^i} = c$ kaikille $i = 1, \ldots, n-1$. Näin ollen

$$\begin{aligned} Tr(c\alpha) &= c\alpha+c^q\alpha^q+c^{q^2}\alpha^{q^2}+\cdots+c^{q^{(n-1)}}\alpha^{q^{(n-1)}} \\ &= c\alpha+c\alpha^q+c\alpha^{q^2}+\cdots+c\alpha^{q^{(n-1)}} \\ &= cTr(\alpha). \end{aligned}$$

3. Lauseen 1.13 nojalla $\alpha^{q^n} = \alpha$, joten

$$Tr(\alpha^q) = \alpha^q+\alpha^{q^2}+\cdots+\alpha = Tr(\alpha).$$

□

Huomautus 4.9. Lauseen 4.8 kohtien 1. ja 2. nojalla jälkifunktio on lineaarinen kuvaus.

Esimerkki 4.10. Olkoon $\mathbb{F}_{2^3}$ kunnan $\mathbb{F}_2$ kuntalaajennus, jonka konstruoinnissa käytetään jaotonta polynomia x^3+x+1. Olkoon γ tämän polynomin juuri kyseisessä kuntalaajennuksessa. Tällöin $\gamma^3+\gamma+1 = 0$, toisin sanoen $\gamma^3 = \gamma+1$. Nyt kunnan alkiot ovat

$$\{0,1,\gamma,\gamma^2,\gamma^3,\gamma^4,\gamma^5,\gamma^6\} = \{0,1,\gamma,\gamma^2,1+\gamma,\gamma+\gamma^2,1+\gamma+\gamma^2,1+\gamma^2\}.$$

Alkion $1+\gamma+\gamma^2 = \gamma^5$ jälki on

$$\begin{aligned} Tr(1+\gamma+\gamma^2) &= 1+\gamma+\gamma^2+(1+\gamma+\gamma^2)^2+(1+\gamma+\gamma^2)^{2^2} \\ &= 1+\gamma+\gamma^2+(\gamma^5)^2+(\gamma^5)^4 = 1+\gamma+\gamma^2+\gamma^{10}+\gamma^{20} \\ &= 1+\gamma+\gamma^2+\gamma^3+\gamma^6 = 1+\gamma+\gamma^2+1+\gamma+1+\gamma^2 = 1. \end{aligned}$$

Lemma 4.11. 1. *Jokainen lineaarinen muotoa* $ax+b, a \neq 0$, *oleva polynomi kunnan* $\mathbb{F}_q$ *yli on permutaatiopolynomi.*
2. *Monomi* x^k *on permutaatiopolynomi jos ja vain jos* $\text{syt}(k, q-1) = 1$.

Todistus.

1. Olkoon $f(x) = ax + b \in \mathbb{F}_q[X]$ ja oletetaan, että $f(x) = f(y)$. Nyt

$$ax + b = ay + b.$$

Lisätään molemmille puolille $-b$, jolloin saadaan $ax = ay$. Kerrotaan puolittain alkiolla a^{-1}, jolloin

$$a^{-1}ax = a^{-1}ay.$$

Tästä seuraa, että $x = y$, joten kuvaus f on injektio ja Lauseen 4.3 nojalla permutaatiopolynomi.

2. Olkoon $f(x) = x^k$ permutaatiopolynomi ja g ryhmän $\mathbb{F}_q^*$ generaattori, jolloin $x = g^i, 1 \leq i \leq q-1$ kaikille $x \in \mathbb{F}_q^*$. Tehdään vastaoletus, että $d = \text{syt}(k, q-1) \neq 1$. Nyt $f(x) = x^k = (g^i)^k = (g^k)^i$. Alkion g^k generoiman ryhmän kertaluku on pienin positiivinen luku n, jolle $g^{kn} = 1$. Tämä pätee jos ja vain jos $(q-1)/d$ jakaa luvun n ja pienin tällainen luku n on $(q-1)/d$. Koska $d > 1$, niin $n < q-1$ ja kuvaus $f(x) = x^k$ ei ole surjektio. Tämä on ristiriita, sillä x^k on permutaatiopolynomi. Näin ollen $\text{syt}(k, q-1) = 1$.

Oletetaan, että $\text{syt}(k, q-1) = 1$. Olkoon g ryhmän $\mathbb{F}_q^*$ generaattori. Tällöin $x = g^i, y = g^j \in \mathbb{F}_q^*$ joillekin $1 \leq i, j \leq q-1$. Nyt ehdosta $f(x) = f(y)$ seuraa

$$x^k = (g^i)^k = (g^k)^i = (g^k)^j = (g^j)^k = y^k.$$

Yhtälö pätee jos ja vain jos $i = j$, jolloin $x = g^i = y$. Näin ollen f on injektio ja Lauseen 4.3 nojalla permutaatiopolynomi.

□

Lemma 4.12. *Olkoon* r *ja* k *positiivisia kokonaislukuja. Polynomi* $f(x) = x^{2^{2^r k}+2^r} + x^{2^{2^r k}} + x^{2^r} \in \mathbb{F}_{2^n}[X]$ *on permutaatiopolynomi jos ja vain jos* $2^{2^r k}+2^r$ *ja* $2^n - 1$ *ovat suhteellisia alkulukuja.*

Todistus. Koska permutaatiopolynomi on bijektiivinen kuvaus, niin kahden permutaatiopolynomin muodostama yhdistetty kuvaus on myös bijektiivinen permutaatiopolynomi. Kun yhdistetään polynomit $x+1$ ja f, saadaan Lauseen 1.13 nojalla

$$\begin{aligned} f(x+1) &= (x+1)^{2^{2^r k}+2^r} + (x+1)^{2^{2^r k}} + (x+1)^{2^r} \\ &= (x+1)^{2^{2^r k}}(x+1)^{2^r} + (x+1)^{2^{2^r k}} + (x+1)^{2^r} \\ &= (x^{2^{2^r k}}+1)(x^{2^r}+1) + (x+1)^{2^{2^r k}} + (x+1)^{2^r} \\ &= x^{2^{2^r k}+2^r} + x^{2^{2^r k}} + x^{2^r} + 1 + x^{2^{2^r k}} + 1 + x^{2^r} + 1 \\ &= x^{2^{2^r k}+2^r} + 1. \end{aligned}$$

Lemman 4.11 nojalla $f(x+1)$ on permutaatiopolynomi jos ja vain jos $2^{2^r k} + 2^r$ ja $2^n - 1$ ovat suhteellisia alkulukuja. Koska $x+1$ on permutaatiopolynomi, niin $f(x)$ on permutaatiopolynomi jos ja vain jos $2^{2^r k} + 2^r$ ja $2^n - 1$ ovat suhteellisia alkulukuja. □

Lause 4.13. *Olkoot k ja r positiivisia kokonaislukuja. Polynomi $g(x) = (x^{2^{2^r k}} + x^{2^r} + \alpha)^l + x$ on permutaatiopolynomi kunnassa F_{2^n}, jos $Tr(\alpha) = 1$ ja l on sellainen positiivinen kokonaisluku, että $l(2^{2^r k} + 2^r) \equiv 1 \mod 2^n - 1$.*

Todistus. Jälkifunktion lineaarisuuden perusteella $Tr(x^{2^{2^r k}} + x^{2^r} + \alpha) = Tr(x^{2^{2^r k}}) + Tr(x^{2^r}) + Tr(\alpha)$. Nyt soveltamalla Lausetta 1.13 saadaan

$$\begin{aligned} Tr(x^{2^{2^r k}}) &= x^{2^{2^r k}} + (x^{2^{2^r k}})^2 + (x^{2^{2^r k}})^{2^2} + \cdots + (x^{2^{2^r k}})^{2^{(n-1)}} \\ &= x^{2^{2^r k}} + (x^2)^{2^{2^r k}} + (x^{2^2})^{2^{2^r k}} + \cdots + (x^{2^{(n-1)}})^{2^{2^r k}} \\ &= (x + x^2 + x^{2^2} + \cdots + x^{2^{(n-1)}})^{2^{2^r k}} \\ &= (Tr(x))^{2^{2^r k}} = Tr(x) \end{aligned}$$

ja

$$\begin{aligned} Tr(x^{2^r}) &= x^{2^r} + (x^{2^r})^2 + (x^{2^r})^{2^2} + \cdots + (x^{2^r})^{2^{(n-1)}} \\ &= x^{2^r} + (x^2)^{2^r} + (x^{2^2})^{2^r} + \cdots + (x^{2^{(n-1)}})^{2^r} \\ &= (x + x^2 + x^{2^2} + \cdots + x^{2^{(n-1)}})^{2^r} \\ &= (Tr(x))^{2^r} = Tr(x), \end{aligned}$$

koska $Tr(x) \in \{0, 1\}$. Näin ollen $Tr(x^{2^{2^r k}} + x^{2^r} + \alpha) = Tr(\alpha) = 1$, joten $x^{2^{2^r k}} + x^{2^r} + \alpha \neq 0$ kaikille $x \in \mathbb{F}_{2^n}$.

Olkoon $\beta \in \mathbb{F}_{2^n}$. Nyt $g(x) = \beta$ on

$$(x^{2^{2^r k}} + x^{2^r} + \alpha)^l + x = \beta,$$

joka on yhtäpitävä yhtälön

$$(x^{2^{2^r k}} + x^{2^r} + \alpha)^l = x + \beta$$

kanssa. Korottamalla molemmat puolet potenssiin $2^{2^r k} + 2^r$, saadaan

$$(x^{2^{2^r k}} + x^{2^r} + \alpha)^{l(2^{2^r k}+2^r)} = x^{2^{2^r k}} + x^{2^r} + \alpha = (x+\beta)^{2^{2^r k}+2^r}.$$

Tämä voidaan kirjoittaa myös muotoon

$$x^{2^{2^r k}} + x^{2^r} + \alpha + (x+\beta)^{2^{2^r k}+2^r} = 0.$$

Merkitään $h(x) = x^{2^{2^r k}} + x^{2^r} + \alpha + (x+\beta)^{2^{2^r k}+2^r}$. Koska tämä johdettiin lähtien yhtälöstä $g(x) = \beta$, niin riittää osoittaa, että $h(x)$ on permutaatiopolynomi. Tarkastellaan yhtälöä

$$\begin{aligned} h(x+\beta) &= (x+\beta)^{2^{2^r k}} + (x+\beta)^{2^r} + \alpha + (x+\beta+\beta)^{2^{2^r k}+2^r} \\ &= x^{2^{2^r k+2^r}} + x^{2^{2^r k}} + x^{2^r} + \beta^{2^{2^r k}} + \beta^{2^r} + \alpha = 0. \end{aligned}$$

Lemman 4.12 nojalla $x^{2^{2^r k+2^r}} + x^{2^{2^r k}} + x^{2^r}$ on permutaatiopolynomi. Näin ollen yhtälöllä $h(x+\beta) = 0$ on yksikäsitteinen ratkaisu kaikille $\beta \in \mathbb{F}_{2^n}$, sillä

$$x^{2^{2^r k+2^r}} + x^{2^{2^r k}} + x^{2^r} = \beta^{2^{2^r k}} + \beta^{2^r} + \alpha,$$

missä $\beta^{2^{2^r k}} + \beta^{2^r} + \alpha$ on jokin tietty kunnan $\mathbb{F}_{2^n}$ alkio. Lauseen 4.3 nojalla $h(x+\beta)$ on siten permutaatiopolynomi. Merkitään $u(x) = x + \beta$, jolloin $h(x+\beta) = h(u(x))$ on bijektio kunnalta $\mathbb{F}_{2^n}$ itselleen. Lemman 4.11 nojalla $u(x) = x + \beta$ on permutaatiopolynomi. Näin ollen kuvauksen $h(x)$ lähtöjoukko on koko kunta $\mathbb{F}_{2^n}$. Koska $h(u(x))$ on surjektio, ja sen maalijoukko on sama kuin kuvauksella $h(x)$, niin kuvaus $h(x)$ on tällöin surjektio. Lauseen 4.3 nojalla $h(x)$ on siten permutaatiopolynomi. Tästä seuraa, että $g(x)$ on permutaatiopolynomi. □

Määritelmä 4.14. Olkoon $x = (x_0, x_1, \ldots, x_{n-1}) \in F_2^n$. Alkion x *paino* $w(x)$ on sen nollasta eroavien komponenttien lukumäärä.

Lemma 4.15. *Olkoon $\beta \in \mathbb{F}_{2^n}$ sellainen, että $w(\beta)$ on parillinen. Tällöin $Tr(L_\beta(x)) = 0$.*

Todistus. Sovelletaan Lausetta 1.13, jolloin saadaan

$$\begin{aligned} (L_\beta(x))^2 &= \left(\sum_{i=0}^{n-1} \beta_i x^{2^i}\right)^2 = (\beta_0 x + \beta_1 x^2 + \beta_2 x^{2^2} + \cdots + \beta_{n-1} x^{2^{(n-1)}})^2 \\ &= \beta_0 x^2 + \beta_1 x^{2^2} + \beta_2 x^{2^3} + \cdots + \beta_{n-1} x^{2^n} \\ &= \beta_{n-1} x + \beta_0 x^2 + \beta_1 x^{2^2} + \beta_2 x^{2^3} + \cdots + \beta_{n-2} x^{2^{(n-1)}}. \end{aligned}$$

Näin ollen neliöön korottaminen siirtää p-polynomin kertoimia aina askeleen verran vasemmalle. Nyt

$$\begin{aligned}
Tr(L_\beta(x)) =& \sum_{i=0}^{n-1} \beta_i x^{2^i} + \left(\sum_{i=0}^{n-1} \beta_i x^{2^i} \right)^2 + \cdots + \left(\sum_{i=0}^{n-1} \beta_i x^{2^i} \right)^{2^{(n-1)}} \\
=& \beta_0 x + \beta_1 x^2 + \beta_2 x^{2^2} + \cdots + \beta_{n-1} x^{2^{(n-1)}} \\
&+ \beta_{n-1} x + \beta_0 x^2 + \beta_1 x^{2^2} + \cdots + \beta_{n-2} x^{2^{(n-1)}} + \cdots \\
&+ \beta_1 x + \beta_2 x^2 + \beta_3 x^{2^2} + \cdots + \beta_0 x^{2^{(n-1)}} \\
=& (\beta_0 + \beta_1 + \beta_2 + \cdots + \beta_{n-1}) x + (\beta_0 + \beta_1 + \beta_2 + \cdots + \beta_{n-1}) x^2 \\
&+ \cdots + (\beta_0 + \beta_1 + \beta_2 + \cdots + \beta_{n-1}) x^{2^{(n-1)}}.
\end{aligned}$$

Koska $w(\beta)$ on parillinen, niin summassa $\beta_0+\beta_1+\beta_2+\cdots+\beta_{n-1}$ on parillinen määrä ykkösiä. Näin ollen jokainen yllä olevan polynomin kerroin on nolla ja $Tr(L_\beta(x)) = 0$. □

Lause 4.16. *Olkoon n pariton positiivinen kokonaisluku ja $\beta \in \mathbb{F}_{2^n}$ sellainen, että $w(\beta)$ on parillinen ja p-polynomin $L_\beta(x)$ ainoat juuret kunnassa $\mathbb{F}_{2^n}$ ovat 0 ja 1. Olkoot k_1 ja k_2 sellaiset ei-negatiiviset kokonaisluvut, että* $\mathrm{syt}(2^{k_1} + 2^{k_2}, 2^n - 1) = 1$ *ja l sellainen positiivinen kokonaisluku, että $(2^{k_1} + 2^{k_2})l \equiv 1 \mod 2^n - 1$. Olkoon $\gamma \in \mathbb{F}_{2^n}$ sellainen, että $Tr(\gamma) = 1$. Tällöin*

$$f(x) = (L_\beta(x) + \gamma)^l + Tr(x)$$

on permutaatiopolynomi kunnassa $\mathbb{F}_{2^n}$.

Todistus. Olkoot x ja y sellaiset erisuuret kunnan $\mathbb{F}_{2^n}$ alkiot, että $f(x) = f(y)$. Tällöin $Tr(x) \neq Tr(y)$, sillä muutoin ehdosta $f(x) = f(y)$ seuraa, että

$$(L_\beta(x) + \gamma)^l = (L_\beta(y) + \gamma)^l.$$

Korotetaan tämä puolittain potenssiin $2^{k_1} + 2^{k_2}$, jolloin saadaan

$$(L_\beta(x) + \gamma)^{l(2^{k_1}+2^{k_2})} = (L_\beta(y) + \gamma)^{l(2^{k_1}+2^{k_2})}$$

ja edelleen

$$L_\beta(x) + \gamma = L_\beta(y) + \gamma.$$

Vähennetään yhtälön molemmilta puolilta γ ja siirretään termit vasemmalle puolelle, jolloin yhtälö saadaan muotoon

$$L_\beta(x) + L_\beta(y) = \sum_{i=0}^{n-1} \beta_i x^{2^i} + \sum_{i=0}^{n-1} \beta_i y^{2^i} = \sum_{i=0}^{n-1} \beta_i (x+y)^{2^i} = L_\beta(x+y) = 0.$$

Koska $x \neq y$ ja polynomin L_β ainoat juuret ovat 0 ja 1, niin $x+y=1$. Koska n on pariton, niin

$$Tr(x) + Tr(y) = Tr(x+y) = Tr(1) = 1 + 1^2 + \cdots + 1^{2^{(n-1)}} = 1$$

mistä seuraa, että $Tr(x) \neq Tr(y)$. Nyt voidaan olettaa, että $Tr(x) = 0$ ja $Tr(y) = 1$. Tällöin ehdosta $f(x) = f(y)$ seuraa

$$(L_\beta(x) + \gamma)^l = (L_\beta(y) + \gamma)^l + 1.$$

Korottamalla molemmat puolet potenssiin $2^{k_1} + 2^{k_2}$ saadaan

$$\begin{aligned} L_\beta(x) + \gamma &= (L_\beta(x) + \gamma)^{l(2^{k_1}+2^{k_2})} \\ &= ((L_\beta(y) + \gamma)^l + 1)^{2^{k_1}+2^{k_2}} \\ &= (L_\beta(y) + \gamma)^{l(2^{k_1}+2^{k_2})} + (L_\beta(y) + \gamma)^{l2^{k_1}} + (L_\beta(y) + \gamma)^{l2^{k_2}} + 1 \\ &= L_\beta(y) + \gamma + (L_\beta(y) + \gamma)^{l2^{k_1}} + (L_\beta(y) + \gamma)^{l2^{k_2}} + 1. \end{aligned}$$

Käyttämällä jälkifunktiota ja Lausetta 4.8 yhtälön molemmille puolille saadaan yhtälön vasemmasta puolesta

$$Tr(L_\beta(x) + \gamma) = Tr(L_\beta(x)) + Tr(\gamma)$$

ja oikeasta puolesta

$$\begin{aligned} &Tr(L_\beta(y) + \gamma + (L_\beta(y) + \gamma)^{l2^{k_1}} + (L_\beta(y) + \gamma)^{l2^{k_2}} + 1) \\ &= Tr(L_\beta(y)) + Tr(\gamma) + Tr((L_\beta(y) + \gamma)^{l2^{k_1}}) + Tr((L_\beta(y) + \gamma)^{l2^{k_2}}) + Tr(1) \\ &= Tr(L_\beta(y)) + Tr(\gamma) + Tr((L_\beta(y) + \gamma)^l) + Tr((L_\beta(y) + \gamma)^l) + Tr(1). \end{aligned}$$

Näin ollen

$$Tr(\gamma) = Tr(\gamma) + Tr(1),$$

sillä Lemman 4.15 nojalla $Tr(L_\beta(x)) = Tr(L_\beta(y)) = 0$. Yllä olevan yhtälön perusteella $Tr(1) = 0$, mikä on ristiriita, sillä n on pariton. Näin ollen ehdosta $x \neq y$ seuraa, että $f(x) \neq f(y)$. Täten polynomi f on injektio ja Lauseen 4.3 nojalla permutaatiopolynomi. □

4.3 Pieni lohikäärme kaksi

Singh, Sarma ja Saikia pitivät Patarinin Pientä lohikäärmettä mielenkiintoisena ja tehokkaana salausjärjestelmänä, minkä takia he suunnittelivat siitä oman parannellun versionsa [13]. Järjestelmä hyödyntää huomattavasti monimutkaisempaa permutaatiopolynomia kuin edeltäjänsä.

4.3.1 Järjestelmän rakenne

Pieni lohikäärme kaksi -järjestelmän rakentamiseen käytetään Lauseen 4.13 mukaista permutaatiopolynomia $g(x) = (x^{2^r k} + x^{2^r} + \alpha)^l + x$. Kaikki tällaiset polynomit eivät käy, sillä julkisten yhtälöiden halutaan olevan neliöllisiä. Tämä onnistuu valitsemalla eksponentiksi l joko 2^t+1 tai 2^t-1. Tällöinkään ei yleisesti voida sanoa, että g olisi permutaatiopolynomi, mutta esimerkiksi valitsemalla $r = 0$, $n = 2m-1$, $k = m$ ja $l = 2^m - 1$ näin on, sillä $2^{2^r k} + 2^r = 2^m + 1$ ja

$$(2^m-1)(2^m+1) = 2^{2m}-1 = 2^{2m-1}\cdot 2-1 = 2^n\cdot 2-1 \equiv 1\cdot 2-1 = 1 \mod 2^n-1.$$

Muitakin vaihtoehtoja on, kunhan l on muotoa $2^i - 2^j$ ja edelliset ehdot täyttyvät. Kuitenkin mahdollisia eksponentteja on varsin vähän, joten on oletettava, että järjestelmän murtoa yrittävä tuntee sen.

Valitaan siis polynomiksi $g(x) = (x^{2^m}+x+\alpha)^{2^m-1}+x$, missä α on salassa pidettävä alkio. Valitaan lisäksi kaksi salaista affiinia muunnosta $s(\overline{x}) = A\overline{x}+\overline{c} = \overline{u}$ sekä $t(\overline{y}) = B\overline{y}+\overline{d} = \overline{v}$. Nyt vektorien $\mathbf{u}$ ja $\mathbf{v}$ välinen yhteys on

$$(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m-1} + \mathbf{u} = \mathbf{v}. \tag{27}$$

Kerrotaan yhtälö (27) puolittain polynomilla $\mathbf{u}^{2^m} + \mathbf{u} + \alpha$ ja sievennetään lauseketta, jolloin saadaan

$$\begin{aligned}
&(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m} + (\mathbf{u}+\mathbf{v})(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)\\
&= ((\mathbf{u}^{2^m} + \mathbf{u}) + \alpha)^{2^m} + \mathbf{u}^{2^m+1} + \mathbf{u}^2 + \mathbf{u}\alpha + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}\mathbf{v} + \mathbf{v}\alpha\\
&= (\mathbf{u}^{2^m} + \mathbf{u})^{2^m} + \alpha^{2^m} + \mathbf{u}^{2^m+1} + \mathbf{u}^2 + \mathbf{u}\alpha + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}\mathbf{v} + \mathbf{v}\alpha = 0.
\end{aligned}$$

Koska valittiin $n = 2m-1$ ja Lauseen 1.12 perusteella $\mathbf{u}^{2^n} = \mathbf{u}$, niin

$$(\mathbf{u}^{2^m})^{2^m} = \mathbf{u}^{2^m 2^m} = \mathbf{u}^{2^{2m}} = \mathbf{u}^{2^{n+1}} = \mathbf{u}^{2^n}\mathbf{u}^{2^n} = \mathbf{u}^2.$$

Nyt edellinen yhtälö saadaan muotoon

$$\begin{aligned}
&(\mathbf{u}^{2^m})^{2^m} + \mathbf{u}^{2^m} + \alpha^{2^m} + \mathbf{u}^{2^m+1} + \mathbf{u}^2 + \mathbf{u}\alpha + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}\mathbf{v} + \mathbf{v}\alpha\\
&= \mathbf{u}^2 + \mathbf{u}^{2^m} + \alpha^{2^m} + \mathbf{u}^{2^m+1} + \mathbf{u}^2 + \mathbf{u}\alpha + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}\mathbf{v} + \mathbf{v}\alpha = 0.
\end{aligned}$$

Koska termit $\mathbf{u}^2$ kumoavat toisensa, saadaan lopulta

$$\mathbf{u}^{2^m+1} + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}\mathbf{v} + \mathbf{u}\alpha + \mathbf{u}^{2^m} + \mathbf{v}\alpha + \alpha^{2^m} = 0. \tag{28}$$

Kun tähän sijoitetaan komponenttien u_i ja v_j lausekkeet valituista affiineista muunnoksista ja lasketaan vastaavalla tavalla kuin Pientä lohikäärmettä rakentaessa, saadaan järjestelmän julkiset yhtälöt, jotka ovat muotoa

$$\sum_{1\leq i,j\leq n} a_{ij}x_ix_j + \sum_{1\leq i,j\leq n} b_{ij}x_iy_j + \sum_{1\leq k\leq n} c_ky_k + \sum_{1\leq k\leq n} d_kx_k + e_l = 0, \qquad (29)$$

missä $a_{ij}, b_{ij}, c_k, d_k, e_l \in \mathbb{F}_2$. Viestin lähettäjä sijoittaa viestivektorin $\overline{x}$ komponentit näihin yhtälöihin ja ratkaisee lineaarisen yhtälöryhmän komponenttien y_j suhteen saadakseen salatun viestin $\overline{y}$, jonka lähettää vastaanottajalle.

Viestin avaaminen tapahtuu seuraavin askelin.

1. Käytetään valittua affiinia muunnosta ja lasketaan $\overline{v} = B\overline{y} + \overline{d}$.
2. Lasketaan vektori $\mathbf{z}_1 = \alpha + 1 + \mathbf{v} + \mathbf{v}^{2^m}$.
3. Lasketaan vektorit $\mathbf{z}_2 = \mathbf{z}_1^{2^m-1}$ ja $\mathbf{z}_3 = \mathbf{v} + 1 + \mathbf{z}_2$.
4. Lasketaan $\overline{x_1} = s^{-1}(\overline{v} + 1)$ sekä $\overline{x_2} = s^{-1}(\overline{z_3})$.

Nyt joko $\overline{x_1}$ tai $\overline{x_2}$ on oikea viesti, joka pitäisi olla helposti pääteltävissä. Perustellaan seuraavaksi tämä avausalgoritmi.

Lisätään yhtälön (27) molemmille puolille vektori $\mathbf{u}$ ja korotetaan sen jälkeen puolittain potenssiin 2^m+1. Koska $(2^m+1)(2^m-1) \equiv 1 \mod 2^n-1$, saadaan tästä

$$\begin{aligned}\mathbf{u}^{2^m} + \mathbf{u} + \alpha &= (\mathbf{u}+\mathbf{v})^{2^m+1} = (\mathbf{u}+\mathbf{v})^{2^m}(\mathbf{u}+\mathbf{v}) \\ &= (\mathbf{u}^{2^m} + \mathbf{v}^{2^m})(\mathbf{u}+\mathbf{v}) = \mathbf{u}^{2^m+1} + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{v}^{2^m}\mathbf{u} + \mathbf{v}^{2^m+1}.\end{aligned}$$

Tämä voidaan kirjoittaa myös muotoon

$$\mathbf{u}^{2^m} + \mathbf{u} + \mathbf{u}^{2^m+1} + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{v}^{2^m}\mathbf{u} + \mathbf{v}^{2^m+1} = \alpha.$$

Lisätään ylläolevan yhtälön molemmille puolille termit $\mathbf{v}^{2^m}$, $\mathbf{v}$ ja 1 ja järjestellään termejä, jolloin saadaan

$$\begin{aligned}&\mathbf{u}^{2^m+1} + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}^{2^m} + \mathbf{v}^{2^m}\mathbf{u} + \mathbf{v}^{2^m+1} + \mathbf{v}^{2^m} + \mathbf{u} + \mathbf{v} + 1 \\ &= \mathbf{v} + \mathbf{v}^{2^m} + \alpha + 1.\end{aligned}$$

Koska

$$\begin{aligned}(\mathbf{u}+\mathbf{v}+1)^{2^m+1} &= (\mathbf{u}+\mathbf{v}+1)^{2^m}(\mathbf{u}+\mathbf{v}+1) = (\mathbf{u}^{2^m} + \mathbf{v}^{2^m} + 1)(\mathbf{u}+\mathbf{v}+1) \\ &= \mathbf{u}^{2^m+1} + \mathbf{u}^{2^m}\mathbf{v} + \mathbf{u}^{2^m} + \mathbf{v}^{2^m}\mathbf{u} + \mathbf{v}^{2^m+1} + \mathbf{v}^{2^m} + \mathbf{u} + \mathbf{v} + 1,\end{aligned}$$

niin tästä saadaan

$$(\mathbf{u}+\mathbf{v}+1)^{2^m+1} = \mathbf{v}+\mathbf{v}^{2^m}+\alpha+1. \tag{30}$$

Siinä tapauksessa, kun $(\mathbf{u}^{2^m}+\mathbf{u}+\alpha)^{2^m-1}=1$, jolloin yhtälö (27) on muotoa $\mathbf{u}=\mathbf{v}+1$, saadaan viesti avattua affiinilla muunnoksella $\overline{x_1}=s^{-1}(\overline{u})=s^{-1}(\overline{v}+1)$. Jos $\mathbf{u}\neq\mathbf{v}+1$, niin korottamalla yhtälön (30) molemmat puolet potenssiin 2^m-1 saadaan

$$(\mathbf{u}+\mathbf{v}+1)^{(2^m+1)(2^m-1)} = \mathbf{u}+\mathbf{v}+1 = (\mathbf{v}+\mathbf{v}^{2^m}+\alpha+1)^{2^m-1}.$$

Nyt voidaan merkitä

$$\mathbf{u} = \mathbf{v}+1+(\mathbf{v}+\mathbf{v}^{2^m}+\alpha+1)^{2^m-1} = \mathbf{v}+1+\mathbf{z}_1^{2^m-1} = \mathbf{v}+1+\mathbf{z}_2.$$

Näin ollen viesti voidaan avata affiinilla muunnoksella

$$\overline{x_2} = s^{-1}(\overline{u}) = s^{-1}(\overline{v}+1+\overline{z_2}) = s^{-1}(\overline{z_3}).$$

Esimerkki 4.17. Rakennetaan Pieni lohikäärme kaksi -järjestelmä laajennuskuntaan $\mathbb{F}_{2^3}$. Nyt $n=2m-1=3$, joten $m=2$. Valitaan jaoton polynomi x^3+x+1 ja olkoon γ sen juuri laajennuskunnassa, jolloin $\gamma^3+\gamma+1=0$. Nyt kunnan $\mathbb{F}_{2^3}$ alkiot ovat

$$\{0,1,\gamma,\gamma^2,1+\gamma,\gamma+\gamma^2,1+\gamma+\gamma^2,1+\gamma^2\}.$$

Valitaan salaiseksi alkioksi $\alpha=1+\gamma+\gamma^2=\gamma^5$, jolle Esimerkin 4.10 perusteella $Tr(\alpha)=1$. Affiineja muunnoksia varten valitaan matriisit

$$A=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix} \quad \text{ja} \quad B=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$$

sekä vektorit $\overline{c}=(1,0,1)$ ja $\overline{d}=(0,1,0)$. Käytetään vektoriavaruuden kantaa $\{1,\gamma,\gamma^2\}$. Nyt saadaan muodostettua vektorit $\overline{u}=(x_1+x_2+1,x_2+x_3,x_3+1)$ ja $\overline{v}=(y_1+y_2+y_3,y_2+y_3,y_3)$ ja näitä vastaavat kunnan F_{2^3} alkiot ovat $\mathbf{u}=(x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2$ sekä $\mathbf{v}=(y_1+y_2+y_3)+(y_2+y_3)\gamma+(y_3)\gamma^2$.

Yhtälö (28) on nyt muodossa

$$\mathbf{u}^{2^2+1}+\mathbf{u}^{2^2}\mathbf{v}+\mathbf{u}\mathbf{v}+\mathbf{u}\alpha+\mathbf{u}^{2^2}+\mathbf{v}\alpha+\alpha^{2^2}=0.$$

Lasketaan aluksi kaikki ylläolevan yhtälön termit erikseen. Koska lasketaan kunnassa $\mathbb{F}_{2^3}$, niin potenssiin korotukset eivät vaikuta polynomien kertoimiin. Näin ollen saadaan

$$
\begin{aligned}
\mathbf{u}^{2^2+1} =&((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)^4\\
&\cdot((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)\\
=&[(x_1+x_2+1)^2+(x_2+x_3)^2+(x_2+x_3)(x_3+1)+(x_3+1)^2]\\
&+[(x_1+x_2+1)(x_2+x_3)+(x_2+x_3)(x_1+x_2+1)+(x_1+x_3)^2\\
&+(x_3+1)(x_1+x_2+1)+(x_3+1)^2]\gamma\\
&+[(x_1+x_2+1)(x_3+1)+(x_2+x_3)(x_1+x_2+1)+(x_2+x_3)^2\\
&+(x_2+x_3)(x_3+1)+(x_3+1)(x_2+x_3)]\gamma^2,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{u}^{2^2}\mathbf{v} =&((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)^4\\
&\cdot((y_1+y_2+y_3)+(y_2+y_3+1)\gamma+y_3\gamma^2)\\
=&[(x_1+x_2+1)(y_1+y_2+y_3)+(x_2+x_3)(y_2+y_3+1)\\
&+(x_2+x_3)y_3+(x_3+1)y_3]\\
&+[(x_1+x_2+1)(y_2+y_3+1)+(x_2+x_3)(y_2+y_3+1)\\
&+(x_2+x_3)(y_1+y_2+y_3)+(x_3+1)(y_1+y_2+y_3)+(x_3+1)y_3]\gamma\\
&+[(x_1+x_2+1)y_3+(x_2+x_3)(y_2+y_3+1)+(x_2+x_3)y_3\\
&+(x_2+x_3)(y_1+y_2+y_3)+(x_3+1)(y_2+y_3+1)]\gamma^2,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{uv} =&((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)\\
&\cdot((y_1+y_2+y_3)+(y_2+y_3+1)\gamma+y_3\gamma^2)\\
=&[(x_1+x_2+1)(y_1+y_2+y_3)+(x_2+x_3)y_3+(x_3+1)(y_2+y_3+1)]\\
&+[(x_1+x_2+1)(y_2+y_3+1)+(x_2+x_3)(y_1+y_2+y_3)\\
&+(x_2+x_3)y_3+(x_3+1)(y_2+y_3+1)+(x_3+1)y_3]\gamma\\
&+[(x_1+x_2+1)y_3+(x_2+x_3)(y_2+y_3+1)\\
&+(x_3+1)(y_1+y_2+y_3)+(x_3+1)y_3]\gamma^2,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{u}\alpha =&((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)\gamma^5\\
=&[(x_1+x_2+1)+(x_2+x_3)+(x_3+1)]\\
&+[(x_1+x_2+1)]\gamma+[(x_1+x_2+1)+(x_2+x_3)]\gamma^2,
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{u}^{2^2} =&((x_1+x_2+1)+(x_2+x_3)\gamma+(x_3+1)\gamma^2)^4\\
=&[(x_1+x_2+1)]+[(x_2+x_3)+(x_3+1)]\gamma+[(x_2+x_3)]\gamma^2,
\end{aligned}
$$

$$\begin{aligned}\mathbf{v}\alpha =&((y_1+y_2+y_3)+(y_2+y_3+1)\gamma+y_3\gamma^2)\gamma^5\\ =&[(y_1+y_2+y_3)+(y_2+y_3+1)+y_3]\\ &+[(y_1+y_2+y_3)]\gamma+[(y_1+y_2+y_3)+(y_2+y_3+1)]\gamma^2,\end{aligned}$$

sekä $\alpha^{2^2}=(\gamma^5)^4=\gamma^{20}=\gamma^6=1+\gamma^2$.

Yhtälö (28) on yhtä suuri kuin nolla jos ja vain jos jokainen komponentti on nolla. Poimitaan yllä olevista termien yhtälöistä komponenttien kertoimet, jolloin saadaan jokaiselle kolmesta komponentista oma yhtälönsä. Sieventämällä näitä saadaan järjestelmän julkisiksi yhtälöiksi

$$\begin{aligned}&x_2x_3+x_2y_2+x_2y_3+x_3y_3+x_1+x_2+y_1+y_2+y_3=0\\ &x_3x_1+x_2x_3+x_3y_1+x_3y_2+x_2y_2+x_2+x_3+y_2+y_3+1=0\\ &x_2x_1+x_2y_1+x_2y_2+x_3y_2+x_3y_3+x_2+y_3+1=0.\end{aligned}$$

Esimerkki 4.18. Jatketaan edellisen esimerkin järjestelmällä ja lähetetään vastaanottajalle viesti $\overline{x}=(0,1,1)$. Sijoittamalla komponentit x_i julkisiin yhtälöihin, saadaan kolme yhtälöä

$$\begin{aligned}&1+y_2+y_3+y_3+1+y_1+y_2+y_3=y_1+y_3=0\\ &1+y_1+y_2+y_2+1+1+y_2+y_3+1=y_1+y_2+y_3=0\\ &y_1+y_2+y_2+y_3+1+y_3+1=y_1=0.\end{aligned}$$

Ratkaisemalla yhtälöryhmä saadaan salatun viestin komponentit ja $\overline{y}=(0,0,0)$. Tämä viesti lähetetään vastaanottajalle.

Avataan nyt sama vastaanotettu viesti $\overline{y}=(0,0,0)$. Ensimmäisessä vaiheessa lasketaan $\overline{v}=B\overline{y}+\overline{d}=\overline{d}=(0,1,0)$, sillä $\overline{y}$ on nollavektori. Tätä vastaava alkio laajennuskunnassa $\mathbb{F}_{2^3}$ on $\mathbf{v}=\gamma$. Koska valittiin $n=3=2m-1$, niin $m=2$. Nyt voidaan laskea

$$\begin{aligned}\mathbf{z}_1&=\alpha+1+\gamma+\gamma^{2^m}=1+\gamma+\gamma^2+1+\gamma+\gamma^4\\ &=\gamma^2+\gamma^4=\gamma^2+\gamma+\gamma^2=\gamma.\end{aligned}$$

Tästä saadaan $\mathbf{z}_2=\mathbf{z}_1^{2^m-1}=\gamma^3=1+\gamma$ ja $\mathbf{z}_3=\mathbf{v}+1+\mathbf{z}_2=\gamma+1+\gamma+1=0$. Käytetään nyt affiinia muunnosta s^{-1} alkioita $\mathbf{v}+1$ ja $\mathbf{z}_3$ vastaaviin vektoreihin $\overline{v}+1=(1,1,0)$ ja $\overline{z_3}=(0,0,0)$. Matriisin A käänteismatriisi on $A^{-1}=B$. Viestivektoreiksi saadaan nyt

$$\overline{x_1}=s^{-1}(\overline{v}+1)=A^{-1}(\overline{v}+1-\overline{c})=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}$$

ja

$$\overline{x_2} = s^{-1}(\overline{z_3}) = A^{-1}(\overline{z_3} - \overline{c}) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Nyt tiedettiin, että alkuperäinen lähetetty viesti oli $\overline{x} = (0, 1, 1)$, joka saatiin jälkimmäisellä muunnoksella. Oikeassa tilanteessa viestiä ei tietenkään tiedetä etukäteen, mutta sen voi tarkistaa salaamalla avatut viestit samalla järjestelmällä. Toinen viesteistä tuottaa vastaanotetun viestin ja on tällöin oikea vaihtoehto.

4.3.2 Järjestelmän turvallisuus

Pieni lohikäärme kaksi julkaistiin vuonna 2009 ja sen luojat pitivät sitä turvallisena kaikkia silloin tunnettuja hyökkäyksiä vastaan. Tarkastellaan nyt lyhyesti heidän väittämiään järjestelmän turvallisuudesta.

Järjestelmä rakennetaan permutaatiopolynomista $(x^{2^{rk}}+x^{2^r}+\alpha)^{2^m-1}+x$, joten se ei murru käyttämällä Kappaleissa 2.2 ja 3.2.3 esitettyjä hyökkäyksiä. Koska alkio α on salainen, joten kun polynomi esitetään muodossa $\sum_{i=0}^{d} \delta_i x^i$, missä d on polynomin aste, osa kertoimista δ_i on 0 tai 1, mutta osa riippuu alkiosta α. Lisäksi käytettävän polynomin aste on luvun n funktio, koska valittiin $m = (n+1)/2$.

Differentiaalisella kryptoanalyysilla on onnistuttu murtamaan salausjärjestelmiä, joiden polynomit ovat neliöllisiä, kuten esimerkiksi Luvussa 2 esitetty Imai-Matsumoto [5]. Tässä menetelmässä tutkitaan julkisen avaimen differentiaalia. Julkinen avain on jokin kuvaus G ja sen *differentiaali* on erotus $dG_k(x) = G(x+k) - G(x)$. Neliöllisen kuvauksen differentiaali on affiini kuvaus, josta voidaan valita tutkittavaksi lineaarinen osa. Salaisesta avaimesta voidaan saada tietoa analysoimalla kyseisen kuvauksen ydintä tai astetta. Kun tunnetaan järjestelmän julkinen avain ja saadaan tietoa epälineaarisesta osasta (x^{q^i+1}), joillakin tietyillä parametreilla järjestelmät ovat murrettavissa. Pieni lohikäärme kaksi käyttää kuitenkin polynomia $(x^{2^{rk}}+x^{2^r}+\alpha)^{2^m-1}+x$ monomin (x^{q^i+1}) sijasta, joten tämä hyökkäys ei toimi järjestelmän murtamiseen.

Jotkin järjestelmät ovat murrettavissa, kun usean muuttujan polynomit muunnetaan yhden muuttujan polynomeiksi. Tämänkin polynomin aste tulee olemaan luvun n funktio ja on osoitettu, että aste ja nollasta eroavien termien lukumäärä kyseisessä polynomissa ovat $\mathcal{O}(n^n)$ [7]. Tällaisen polynomin juurten etsintäalgoritmien kompleksisuus on polynomiaikainen polynomin asteen suhteen. Näin ollen algoritmi on kokonaisuudessaan eksponenttiaikainen ja kestää liian kauan.

Sijoittamalla salatun viestin julkisiin yhtälöihin, saadaan n neliöllistä yhtälöä muuttujien $x_i, i = 1, \ldots, n$ suhteen ja Gröbnerin kantaa käyttämällä voidaan hyökätä järjestelmän kimppuun. Gröbnerin kannan määrittämisen laskennallinen kompleksisuus riippuu vahvasti käytetystä algoritmista, mutta yleisesti ottaen se on eksponenttiaikaista. Koska Pieni lohikäärme kakkosen julkinen avain sisältää sekä muuttujia x_i että y_j, jokainen salattu viesti tuottaa erilaisen yhtälöryhmän. Tämä yhdessä sen kanssa, että käytetyn polynomin aste on verrannollinen lukuun n, johtaa siihen, että tässä tapauksessa ei olisi olemassa polynomiaikaista algoritmia Gröbnerin kannan laskemiseen. Samaan perusteluun nojaa myös relinearisaation tai XL- ja FXL-algoritmien toimimattomuus. Jos näitä algoritmeja halutaa käyttää sellaisessa tapauksessa, että riippumattomien yhtälöiden lukumäärä on yhtä suuri kuin muuttujien lukumäärä, kyseisten algoritmien kompleksisuus on 2^n.

Pieni lohikäärme kaksi ei kuitenkaan pysynyt kauaa murtamattomana. Jo seuraavana vuonna esitettiin menetelmä, jolla järjestelmä saadaan murrettua [4]. Jos järjestelmässä on käytetty affiineja muunnoksia s ja t sekä kuvausta f, joka on permutaatiopolynomi, niin julkiset yhtälöt saadaan kuvauksella

$$y = (p_1, \ldots, p_n) = t \circ f \circ s(x_1, \ldots, x_n),$$

missä p_i ovat neliöllisiä polynomeja muuttujien x_i ja y_j suhteen. Järjestelmä murretaan muodostamalla ekvivalentit kuvaukset s', t' ja f', joita käyttämällä viestit voidaan avata. Kuvausten muodostamisen laskennallinen kompleksisuus on $\mathcal{O}(n^3)$, joten kyseinen algoritmi on polynomiaikainen.

Samana vuonna julkaistussa tutkimuksessa järjestelmän kestävyyttä tutkittiin laskennallisesti käyttämällä MutantXL2-algoritmia (MXL2) [2]. Tutkimuksessa käytetty tietokone pystyi murtamaan Pieni lohikäärme kakkosen, kun julkisen avaimen pituus oli $n \leq 229$ bittiä. Avaimen pituuden ollessa $n = 229$ tietokoneelta kului aikaa vain hieman yli kaksi ja puoli tuntia. Lisää algoritmin vaatimia aikoja on liitteenä olevassa Taulukossa 3. Samalla väitettiin, että Pieni lohikäärme kaksi murtuisi aina 389 bittiin asti alle vuorokaudessa, kun käytössä on 128 gigatavua muistia.

4.4 Poly-Dragon

Singh, Sarma ja Saikia esittivät myös toisen Pienen lohikäärmeen parannuksen, jossa käytetään kahta eri permutaatiopolynomia [14]. Järjestelmä on nimeltää Poly-Dragon ja se rakentuu vastaavasti, kuin Pieni lohikäärme kaksi.

4.4.1 Järjestelmän rakenne

Poly-Dragon -järjestelmä rakentuu Lauseiden 4.13 ja 4.16 mukaisille permutaatiopolynomeille

$$g(x) = (x^{2^{rk}} + x^{2^r} + \alpha)^l + x \text{ ja } f(x) = (L_\beta(x) + \gamma)^j + Tr(x).$$

Valitaan nyt $r = 0$, $n = 2m - 1$, $k = m$, $k_1 = 0$, $k_2 = m$, $l = 2^m - 1$ ja $j = 2^m - 1$. Tällöin

$$2^{2^{rk}} + 2^r = 2^m + 1,\ 2^{k_1} + 2^{k_2} = 2^m + 1$$

ja kuten Kappaleessa 4.3.1 perusteltiin

$$(2^m - 1)(2^m + 1) \equiv 1 \mod 2^n - 1,$$

joten $f(x) = (L_\beta(x) + \gamma)^{2^m-1} + Tr(x)$ ja $g(x) = (x^{2^m} + x + \alpha)^{2^m-1} + x$ ovat permutaatiopolynomeja. Valitaan alkiot α, β ja γ sekä affiinit muunnokset $s(\overline{x}) = A\overline{x} + \overline{c} = \overline{u}$ ja $t(\overline{y}) = B\overline{y} + \overline{d} = \overline{v}$, jotka pidetään salassa.

Selkotekstin ja salatun tekstin välinen yhteys on nyt $g(s(x)) = f(t(y))$ eli

$$(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m-1} + \mathbf{u} = (L_\beta(\mathbf{v}) + \gamma)^{2^m-1} + Tr(\mathbf{v}). \tag{31}$$

Kun yllä oleva kerrotaan puolittain polynomilla $(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)(L_\beta(\mathbf{v}) + \gamma)$ ja järjestelemällä termejä tästä saadaan

$$\begin{aligned}&(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m}(L_\beta(\mathbf{v}) + \gamma) + \mathbf{u}(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)(L_\beta(\mathbf{v}) + \gamma)\\ &+ (\mathbf{u}^{2^m} + \mathbf{u} + \alpha)(L_\beta(\mathbf{v}) + \gamma)^{2^m} + Tr(\mathbf{v})(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)(L_\beta(\mathbf{v}) + \gamma) = 0.\end{aligned}$$

Merkitään $Tr(\mathbf{v}) = \zeta_y \in \{0, 1\}$. Kun sijoitetaan yllä olevaan yhtälöön affiineista muunnoksista s ja t saatavat komponentit u_i ja v_j, saadaan n yhtälöä

$$\begin{aligned}&\sum_{1\le,i,j,k\le n} a_{ijk}x_ix_jy_k + \sum_{1\le,i,j\le n} b_{ij}x_ix_j + \sum_{1\le,i,j\le n} (c_{ij} + \zeta_y)x_iy_j\\ &+ \sum_{1\le k\le n} (d_k + \zeta_y)y_k + \sum_{1\le k\le n} (e_k + \zeta_y)x_k + f_l = 0,\end{aligned} \tag{32}$$

missä kertoimet $a_{ijk}, b_{ij}, c_k, d_k, e_k, f_l \in \mathbb{F}_2$. Komponentteja x_i ja y_j on kumpiakin n kappaletta, joten jokaisessa yhtälössä on $\mathcal{O}(n^3)$ termiä ja yhteensä kaikissa yhtälöissä $\mathcal{O}(n^4)$ kappaletta. Patarin osoitti, että määrää on mahdollista pienentää $\mathcal{O}(n^3)$ kappaleeseen kirjoittamalla yhtälöt (32) kahtena yhtälöryhmänä, joissa esiintyy korkeintaan neliöllisiä termejä [11]. Tämä ei vaikuta järjestelmän turvallisuuteen ja algoritmi on polynomiaikainen. Muutoksen

jälkeen julkiset salausyhtälöt koostuvat kahdesta n yhtälön yhtälöryhmästä, jotka ovat muotoa

$$\sum_{1\leq k\leq n} g_k y_k + \sum_{1\leq i,j\leq n} (b_{ij}+\zeta_y)x_i y_j + \sum_{1\leq k\leq n} (d_k+\zeta_y)y_k + \sum_{1\leq k\leq n} (e_k+\zeta_y)x_k + f_l = 0,$$

missä $g_k = \sum_{1\leq i,j,k\leq n} h_{ijk}x_i x_j$.

Nyt viestin lähettäjä ei tunne vektoria $\mathbf{v}$, joten hän ei voi laskea jälkeä $Tr(\mathbf{v}) = \zeta_y$. Näin ollen hän sijoittaa ensin viestivektorin komponentit x_i ja $\zeta_y = 0$ julkisiin yhtälöihin. Tämän jälkeen hän ratkaisee lineaarisen yhtälöryhmän komponenttien y_j suhteen. Näistä muodostuu salattu viesti $\overline{y}' = (y_1, \ldots, y_n)$. Toisessa vaiheessa hän sijoittaa komponentit x_i ja $\zeta_y = 1$ ja ratkaisee jälleen yhtälöryhmän. Näin hän saa toisen viestivektorin $\overline{y}'' = (y_1, \ldots, y_n)$. Lopuksi hän lähettää molemmat vektorit vastaanottajalle.

Viesti avataan seuraavilla operaatioilla.

1. Lasketaan vektorit $t(\overline{y}') = B\overline{y}' + \overline{d} = \overline{v_1}$ ja $t(\overline{y}'') = \overline{v_2}$.
2. Lasketaan $L_\beta(\mathbf{v}_1) + \gamma = \mathbf{z}_1$ sekä $L_\beta(\mathbf{v}_2) + \gamma = \mathbf{z}_2$.
3. Korotetaan edellisessä vaiheessa saadut vektorit potenssiin $2^m - 1$, $\mathbf{z}_3' = \mathbf{z}_1^{2^m-1}$ ja $\mathbf{z}_4' = \mathbf{z}_2^{2^m-1}$.
4. Lasketaan $\mathbf{z}_3' + Tr(\mathbf{v}_1) = \mathbf{z}_3$ ja $\mathbf{z}_4' + Tr(\mathbf{v}_2) = \mathbf{z}_4$.
5. Seuraavaksi lasketaan $\mathbf{z}_3^{2^m} + \mathbf{z}_3 + \alpha + 1 = \mathbf{z}_5$ sekä $\mathbf{z}_4^{2^m} + \mathbf{z}_4 + \alpha + 1 = \mathbf{z}_6$.
6. Korotetaan saadut vektori potenssiin $2^m - 1$, $\mathbf{z}_5^{2^m-1} = \mathbf{z}_7$ ja $\mathbf{z}_6^{2^m-1} = \mathbf{z}_8$.
7. Lopuksi käytetään affiinia muunnosta s^{-1} ja lasketaan $\overline{x}_1 = s^{-1}(\overline{z_3} + 1), \overline{x}_2 = s^{-1}(\overline{z_4} + 1), \overline{x}_3 = s^{-1}(\overline{z_3} + \overline{z_7} + 1)$ ja $\overline{x}_4 = s^{-1}(\overline{z_4} + \overline{z_8} + 1)$.

Nyt jokin vektoreista $\overline{x}_1, \overline{x}_2, \overline{x}_3$ tai $\overline{x}_4$ on oikea viesti. Perustellaan tässä vaiheessa avausalgoritmin toiminta.

Merkitään $\mathbf{z} = (L_\beta(\mathbf{v}) + \gamma)^{2^m-1} + Tr(\mathbf{v})$. Nyt yhtälö (31) saa muodon

$$(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m-1} + \mathbf{u} = \mathbf{z}.$$

Tämä on samaa muotoa kuin yhtälö (27), missä $\mathbf{v} = \mathbf{z}$. Näin ollen tekemällä samat laskutoimitukset kuin Kappaleessa 4.3.1 tästä seuraa muotoa (30) oleva yhtälö

$$(\mathbf{u} + \mathbf{z} + 1)^{2^m+1} = \mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1.$$

Jos $(\mathbf{u}^{2^m} + \mathbf{u} + \alpha)^{2^m-1} = 1$, niin $\mathbf{u} = \mathbf{z} + 1$ ja viesti voidaan avata laskemalla affiini muunnos $\overline{x} = s^{-1}(\overline{u}) = s^{-1}(\overline{z}+1)$. Jos taas $\mathbf{u} \neq \mathbf{z}+1$, niin korottamalla edellinen yhtälö puolittain potenssiin $2^m - 1$ saadaan

$$(\mathbf{u} + \mathbf{z} + 1)^{(2^m+1)(2^m-1)} = \mathbf{u} + \mathbf{z} + 1 = (\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1)^{2^m-1},$$

joka voidaan kirjoittaa muotoon

$$\mathbf{u} = \mathbf{z} + 1 + (\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1)^{2^m-1}.$$

Tarkastelemalla avausalgoritmin askelia, huomataan että $\mathbf{z} = \mathbf{z}_3$ (tai $\mathbf{z} = \mathbf{z}_4$). Näin ollen

$$\begin{aligned}
\mathbf{u} &= \mathbf{z} + 1 + (\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1)^{2^m-1} \\
&= \mathbf{z}_3 + 1 + (\mathbf{z}_3 + \mathbf{z}_3^{2^m} + \alpha + 1)^{2^m-1} \\
&= \mathbf{z}_3 + 1 + \mathbf{z}_5^{2^m-1} \\
&= \mathbf{z}_3 + 1 + \mathbf{z}_7,
\end{aligned}$$

joten viesti saadaan avattua laskemalla $\overline{x} = s^{-1}(\overline{u}) = s^{-1}(\overline{z_3} + \overline{z_7} + 1)$.

Salaamalla avatut viestit samalla järjestelmällä jotkin kaksi viestiä tuottavat salatut viestit $\overline{y}'$ ja $\overline{y}''$ ja toiset kaksi voidaan hylätä. Kahdesta jäljelle jäävästä viestistä on usein mahdollista päätellä oikea viesti. Varmuus saadaan tarkistamalla onko $\mathbf{u} = \mathbf{z} + 1$. Tämän perusteella voidaan sanoa kummalla laskutavalla saatu jäljelle jääneistä viesteistä on oikea.

4.4.2 Järjestelmän turvallisuus

Järjestelmän luojat pitivät vuonna 2009 sitä turvallisena kaikkia silloin tunnettuja hyökkäyksiä vastaan. Tarkastellaan hieman heidän esittämiään väittämiä järjestelmän turvallisuudesta. Kaikki Kappaleessa 4.3.2 esitetyt perustelut esitettiin myös Poly-Dragon -järjestelmälle, sillä siinäkin käytetään muotoa $(x^{2^r k} + x^{2^r} + \alpha)^{2^m-1} + x$ olevaa polynomia.

Poly-Dragon lisää turvallisuutta siten, että polynomi $(L_\beta(x)+\gamma)^j + Tr(x)$ muodostetaan salaisten alkioiden β ja γ avulla. Jos nyt polynomi esitetään muodossa $\sum_{i=0}^{d} \epsilon_i x^i$, missä d on polynomin aste, kaikki kertoimet ϵ_i ovat tuntemattomia. Lisäksi tämänkin polynomin aste on verrannollinen lukuun n.

Järjestelmää voi yrittää murtaa yhtälöillä, jotka ovat lineaarisia selkotekstin suhteen, mutta epälineaarisia salatun tekstin suhteen. Merkitään taas $\mathbf{z} = (L_\beta(\mathbf{v}) + \gamma)^{2^m-1} + Tr(\mathbf{v})$. Järjestelmän avausalgoritmia perusteltaessa johdettiin yhtälö

$$\mathbf{u} + \mathbf{z} + 1 = (\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1)^{2^m-1}.$$

Jos $\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1 \neq 0$, niin saadaan tästä

$$(\mathbf{u} + \mathbf{z} + 1)(\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1) + (\mathbf{z} + \mathbf{z}^{2^m} + \alpha + 1)^{2^m} = 0.$$

Tämä johtaa yhtälöihin, jotka ovat lineaarisia muuttujien x_i suhteen ja epälineaarisia muuttujien y_i suhteen. Koska $\mathbf{z}$ johtaa astetta $w(2^m - 1)$ oleviin yhtälöihin, joten yllä oleva relaatio johtaa epälineaarisiin yhtälöihin, joiden aste on $2w(2^m - 1)$. Näin ollen tämä hyökkäys ei ole toteutettavissa.

Myös Poly-Dragon -järjestelmä on mahdollista murtaa laskennallisesti samalla MXL2-algoritmilla, kuin Pieni lohikäärme kaksi [2]. Tutkimuksissa osoittautui, että näiden kahden järjestelmän kompleksisuus samalla muuttujien lukumäärällä on oleellisesti sama. Tietokone onnistui murtamaan Poly-Dragon -järjestelmän, kun $n \leq 299$ bittiä. Tapauksessa $n = 299$ järjestelmän murtaminen kesti hieman yli 11 tuntia. Lisää algoritmin vaatimia aikoja on liitteena olevassa Taulukossa 3. Samalla esitettiin väite, että Poly-Dragon olisi mahdollista murtaa aina 339 bittiin asti alle 20 tunnissa, jos käytössä on 128 gigatavua muistia.

5 Nykytilanne

Tässä tutkielmassa on tarkasteltu usean muuttujan julkisen avaimen salausjärjestelmiä, jotka on tarkoitettu nimenomaan salausalgoritmeiksi. MPKC-järjestelmät ovat usein myös käytännöllisiä allekirjoitusalgoritmeja ja siinä roolissa ne ovat olleet menestyksekkäämpiä. Edelleen moni järjestelmä perustuu Patarinin vuonna 1996 esittämään Hidden Field Equations-järjestelmään (HFE) [12]. Tällaisia ovat esimerkiksi Oil and Vinegar (OV) ja Hidden Field Equations with Vinegar and Minus (HFEV-). Ne ovat kestäneet erilaisia hyökkäyksiä 15-20 vuotta ja niiden turvallisuustason uskotaan olevan erittäin korkea [3].

Oil and Vinegar-järjestelmässä valitaan oil- ja vinegar-muuttujia yhtä monta kappaletta. Tähän esitetyssä muunnoksessa Unbalanced Oil and Vinegar -järjestelmässä (UOV) muuttujia valitaan eri suuret määrät. Rainbow-järjestelmää voidaan kuvailla monikerroksisena versiona UOV-järjestelmästä. Samalla se pienentää avaimen ja allekirjoitusten kokoa sekä tehostaa järjestelmän turvallisuutta ja laskennallista tehokkuutta.

Kuten kaikki tutkielmassa esitetyt järjestelmät, moni tämän tyypin salausjärjestelmistä on murrettu hyvin pian julkaisunsa jälkeen, joten turvallisten ja tehokkaiden järjestelmien luonti on vaikeaa. Tällä hetkellä turvallisina MPKC-järjestelminä pidetään esimerkiksi Perturbed Matsumoto-Imai with Plus- sekä Internally Perturbed HFE with Plus - järjestelmiä, mutta niiden käyttö on monimutkaisempaa ja tehottomampaa kuin allekirjoitusalgoritmien. Uusia kandidaatteja MPKC-järjestelmiksi ovat SimpleMatrix, SRP, ZHFE ja HFERP [3],[6].

MPKC-järjestelmien etuna voidaan pitää niiden nopeutta, jossa ne voittavat monet kilpailijansa. Toinen etu on järjestelmien laskennallinen vaatimattomuus. Niissä käytetään yksinkertaisia aritmeettisia operaatioita suhteellisen pienissä äärellisissä kunnissa. Tämän takia ne ovat hyviä vaihtoehtoja pienille laitteille, kuten älykorteille ja piirilevyille kuten myös Internet of Things -sovelluksille. Lisäksi MPKC-allekirjoitukset ovat lyhyempiä kuin missään muissa allekirjoitusalgoritmeissa [3]. Suurin haittapuoli näissä järjestelmissä on kuitenkin julkisen avaimen suuri pituus, joka on paljon suurempi kuin esimerkiksi RSA-järjestelmässä.

Järjestelmän turvallisuustaso bitteinä voidaan määritellä niin, että järjestelmän turvallisuuden sanotaan olevan n bittiä, jos sen murtamiseen vaaditaan 2^n operaatiota. Seuraavassa Taulukossa 1 on esitetty kuinka monta yhtälöä MPKC-järjestelmässä on oltava, jotta saavutetaan tietty turvallisuustaso bitteinä. Luku vaihtelee käytetyn äärellisen kunnan alkioiden lukumäärän muuttuessa. Esitetyt luvut toimivat siinä tapauksessa, että järjestelmä käyttää jotain kuvausta $f : \mathbb{F}^n \mapsto \mathbb{F}^n$ [3]. Tästä nähdään, että käyttämällä

suurta äärellistä kuntaa tarvittavien yhtälöiden määrä pienenee suhteellisen vähän verrattuna pieneen äärelliseen kuntaan.

Turvallisuustaso	Yhtälöiden lukumäärä		
	$\mathbb{F}_{16}$	$\mathbb{F}_{31}$	$\mathbb{F}_{256}$
80	30	28	26
100	39	36	33
128	51	48	43
192	80	75	68
256	110	103	93

Taulukko 1: Pienin määrä yhtälöitä, joilla saavutetaan tietty turvallisuustaso.

Lähdeluettelo

[1] Apostol, T. M.: *Introduction to Analytic Number Theory*; Springer Science+Business Media Inc., New York, 1976.

[2] Buchmann J., Bulygin S., Ding J., Mohamed W.S.A.E., Werner F. (2010) *Practical Algebraic Cryptanalysis for Dragon-Based Cryptosystems. In: Heng SH., Wright R.N., Goi BM. (eds) Cryptology and Network Security. CANS 2010. Lecture Notes in Computer Science, vol 6467.* Springer, Berlin, Heidelberg. pp. 140-155.

[3] Ding, J., Petzoldt, A.: *Current State on Multivariate Cryptography. In: IEEE Security & Privacy, Volume 15 Issue 4*; 2017, pp. 28-36.

[4] Fada Li, Xiaobin Lu, Yang Wang, Li Tian, Wansu Bao: *Cryptanalysis of Little Dragon Two multivariate public key cryptosystem. 2010 International Conference on Computer Application and System Modeling*; 2010, Volume 9, pp. V9-292 - V9-294.

[5] Fouque, PA., Granboulan, L., Stern, J.: *Differential Cryptanalysis for Multivariate Schemes. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494.* Springer, Berlin, Heidelberg, 2005, pp. 341 - 353.

[6] Ikematsu, Y., Perlner, R., Smith-Tone, D., Takagi, T., Vates, J.: *HFERP - A New Multivariate Encryption Scheme. In: Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings.* pp. 396-416.

[7] Kipnis, A., Shamir, A.: *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. CRYPTO '99, LNCS Vol. 1666.*: 1999, pp. 19-30.

[8] Koblitz, N.: *Algebraic Aspects of Cryptography*; Springer-Verlag, Berlin Heidelberg New York, 1998.

[9] Lidl, R., Niederreiter, H.: *Finite Fields, Second edition*; Cambridge University Press, 1997.

[10] Matsumoto T., Imai H.: *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Barstow d. et. al. (eds) Advances in Cryptology - EUROCRYPT '88*; Springer, Berlin, Heidelberg, 1988, pp. 419-453.

[11] Patarin, J.: *Asymmetric cryptography with a hidden monomial, Advances in Cryptology - Crypto '96.*; Springer-Verlag, Berlin Heidelberg, 1996, pp. 45-60.

[12] Patarin, J.: *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, Advances in Cryptology - EUROCRYPT '96*; 1996, pp. 33-48.

[13] Singh, R.P., Saikia, A., Sarma, B.K.: *Little Dragon Two: An Efficient Multivariate Public Key Cryptosystem. International Journal of Network Security and Its Applications*; 2010, Vol.2(2), pp. 1-10.

[14] Singh, R.P., Saikia, A., Sarma, B.K.: *Poly-Dragon: An Efficient Multivariate Public Key Cryptosystem. Journal of Mathematical Cryptology*; 2011, Vol.4(4), pp. 349-364.

Liitteet

Liite 1

Alla olevassa taulukossa on esitetty kaikki Esimerkin 3.1 valinnoilla tutkitut mahdolliset eksponentit Pieni lohikäärme -salausjärjestelmään, missä $h = 3^r + 3^s - 1$.

r, s	$3^r + 3^s - 1$	$\text{syt}(h, 3^{10} - 1)$	r, s	$3^r + 3^s - 1$	$\text{syt}(h, 3^{10} - 1)$
$9, 8$	26 243	1	$9, 7$	21 869	1
$9, 6$	20 411	1	$9, 5$	19 925	1
$9, 4$	19 763	1	$9, 3$	19 709	1
$9, 2$	19 691	1	$9, 1$	19 685	1
$9, 0$	19 683	1	$8, 7$	8747	1
$8, 6$	7289	1	$8, 5$	6803	1
$8, 4$	6641	1	$8, 3$	6587	1
$8, 2$	6569	1	$8, 1$	6563	1
$8, 0$	6561	1	$7, 6$	2915	11
$7, 5$	2429	1	$7, 4$	2267	1
$7, 3$	2213	1	$7, 2$	2195	1
$7, 1$	2189	11	$7, 0$	2187	1
$6, 5$	971	1	$6, 4$	809	1
$6, 3$	755	1	$6, 2$	737	11
$6, 1$	731	1	$6, 0$	729	1
$5, 4$	323	1	$5, 3$	269	1
$5, 2$	251	1	$5, 1$	245	1
$5, 0$	243	1	$4, 3$	107	1
$4, 2$	89	1	$4, 1$	83	1
$4, 0$	81	1	$3, 2$	35	1
$3, 1$	29	1	$3, 0$	27	1
$2, 1$	11	11	$2, 0$	9	1
$1, 0$	3	1	-	-	-

Taulukko 2: Pienen lohikäärmeen eksponenttikandidaatit.

Liite 2

Alla olevassa taulukossa on esitetty MutantXL2-algoritmin tarvitsemia aikoja Pieni lohikäärme kaksi- ja PolyDragon -järjestelmien murtamiseen eri julkisen avaimen n pituuden arvoilla. Taulukossa n kertoo järjestelmän julkisen avaimen pituuden ja muuttujien lukumäärän, toisessa sarakkeessa on tietokoneen vaatima muistitila megatavuina ja aika on ilmoitettu sekunteina, paitsi jos sen on erikseen ilmoitettu olevan tunteina (h) [2].

Pieni lohikäärme kaksi			Poly-Dragon	
n	muistia, MB	aika	muistia, MB	aika
79	211	22	224	31
89	346	40	285	39
99	545	73	454	71
109	844	122	674	117
119	1251	217	1473	347
129	2380	458	1573	312
139	3387	742	2253	451
149	3490	692	3151	659
159	4545	1146	4318	960
169	6315	1613	5812	1449
179	8298	2025	7698	1907
189	10697	2635	14154	3782
199	13772	1 h	12944	3633
209	17431	1, 32 h	16472	6730
219	29856	2, 81 h	20736	8165
229	25847	2, 60 h	36617	4, 13 h
239	-	-	31922	3, 62 h
249	-	-	39098	4, 34 h
259	-	-	47512	6, 51 h
⋮	⋮	⋮	⋮	⋮
299	-	-	95317	11, 28 h

Taulukko 3: MXL2-algoritmin suoriutuminen Pieni lohikäärme kaksi- sekä Poly-Dragon -järjestelmien murtamisessa.