Digitaalinen käteinen

LuK-tutkielma
Ilkka Alanärä
Matemaattisten tieteiden tutkinto-ohjelma
Oulun yliopisto
Syksy 2018

Sisältö

Johdanto

Käteisellä rahalla on monia huonoja puolia ja sen käytön lopettamista onkin harkittu vakavasti nykyisessä yhteiskunnassamme. Käteistä pidetään, ihan aiheellisesti, turvattomana, kömpelönä ja kalliina ylläpitää. Kauppojen kassoihin kertyy päivän aikana tuhansia euroja houkuttelemaan varkaita. Käteinen myös mahdollistaa alatason korruptiota, sillä käteinen on harmaan talouden ja rikollisen toiminnan pyörittämisessä isossa roolissa.

Toisaalta käteisellä on monia hyviä puolia verrattuna nykyisin käytössä oleviin vaihtoehtoihin. Kaikki vaihtoehtoiset järjestelmät tarvitsevat verkkoyhteyksiä toimiakseen. Kun maksat kaupassa kortilla kassa varmentaa pankista katteen, lukuunottamatta luottokorttia ja pieniä ostoksia, tai tehdessäsi tilisiirtoa käytät lähes poikkeuksetta jotakin tietoliikenneyhteyttä. Mahdollisessa kriisitilanteessa, tai muussa tilanteessa, jossa verkkoyhteydet eivät toimi, on käteinen välttämätön maksuväline.

Täydellisen käteisestä luopumisen sijaan onkin mahdollista toteuttaa järjestelmä, jolla päästään eroon käteisen rahan kalliista ylläpitokustannuksista niin, että nykyisen käteisen rahan ominaisuudet voidaan säilyttää. Lisäksi tämän käteistä vastaavan rahan turvallinen säilyttäminen on helpompaa ja halvempaa kuin nykyisten kolikoiden ja seteleiden.

Tutkielmassa tutustutaan digitaaliseen käteiseen, jolla olisi mahdollista korvata nykyinen käteisjärjestelmä ilman muutoksia käteisen ominaisuuksiin ja käyttöön. Esiteltävä järjestelmä on teknisesti ja matemaattisesti täysin käyttökelpoinen ja skaalautuva, joten sillä olisi mahdollista korvata olemassa oleva käteinen, mutta luonnollisestikaan se ei ole ainoa vaihtoehto. Järjestelmä pohjautuu äärellisiin kuntiin, niiden primitiivialkioihin ja kongruenssilaskentaan, joten lukijalla oletetaan olevan pohjatiedot näistä algebran aiheista.

Tutkielmassa on käytetty pääasiassa teosta Introduction to Cryptography with Coding Theory[1].

1 Käsitteet

Määritelmä 1.1. Olkoon $n \in \mathbb{Z}_{\geq 2}$. Luku $g \in \{1, 2, ..., n-1\}$ on *primitiivijuuri* (mod n), jos $\mathbb{Z}_n^* = \langle g \rangle$, eli g generoi ryhmän $\mathbb{Z}_n^*$.

Lause 1.2. *(Fermat'n pieni lause)*
Jos p on alkuluku ja a sellainen kokonaisluku, että $p \nmid a$, niin

$$a^{p-1} \equiv 1 \text{ (mod } p\text{)}.$$

Lause 1.3. *Olkoon p alkuluku, g primitiivijuuri (mod p) ja $n \in \mathbb{Z}$*

$$g^n \equiv 1 \text{ (mod } p\text{) jos ja vain jos } n \equiv 0 \text{ (mod } p\text{-}1\text{)}.$$

Todistus.
"$\Longleftarrow$" Jos $n \equiv 0 \pmod{p-1}$, niin $n = (p-1)m$ jollakin $m \in \mathbb{Z}$. Tällöin, Fermat'n pienen lauseen nojalla $g^n \equiv (g^m)^{p-1} \equiv 1 \pmod{p}$.
"$\Longrightarrow$" Olkoon $g^n \equiv 1 \pmod{p}$. Osoitetaan, että $p-1$ jakaa luvun n, eli jaetaan n luvulla $p-1$ ja yritetään osoittaa, että jakojäännös on 0. Merkitään $n = (p-1)q + r$, missä $0 \leq r < p-1$ eli q on jakaja ja r jakojäännös. Tällöin $1 \equiv g^n \equiv (g^q)^{p-1} g^r \equiv 1 \cdot g^r \equiv g^r \pmod{p}$. Mikäli $r > 0$, niin g:n potenssit $g, g^2, g^3, ... \pmod{p}$ tuottavat keskenään kongruentit luvut aina r potenssin välein eli $g^{r+1} \equiv g, g^{r+2} \equiv g^2, ... \pmod{p}$. Tällöin g:n potensseina saadaan r lukua ja koska $r < p-1$, niin g ei generoi ryhmää p, mikä on ristiriita oletuksen, että g on primitiivijuuri modulo p, kanssa. Ainoa vaihtoehto on, että $r = 0$ joten $n = (p-1)q$ eli $p-1 \mid n$. □

Lause 1.4. *Olkoon p alkuluku, g primitiivijuuri (mod p) ja $j,k \in \mathbb{Z}$.*

$$g^j \equiv g^k \text{ (mod } p\text{) jos ja vain jos } j \equiv k \text{ (mod } p\text{-}1\text{)}.$$

Todistus.
"$\Longrightarrow$" Oletetaan, että $j \geq k$, jos näin ei ole niin vaihdetaan j ja k keskenään. Tällöin kongruenssista $g^j \equiv g^k \pmod{p}$ seuraa, kun se kerrotaan puolittain luvulla g^{p-1-k}, että $g^j(g^{p-1-k}) \equiv g^k(g^{p-1-k}) \pmod{p}$. Tästä saadaan potenssin laskusääntöjen mukaan $g^{j+p-1-k} \equiv g^{k+p-1-k} \pmod{p}$ mistä edelleen

potenssin laskusääntöjen mukaan $g^{j-k}g^{p-1} \equiv g^{p-1} \pmod{p}$. Lauseen 1.2 perusteella $a^{p-1} \equiv 1 \pmod{p}$, joten $g^{j-k} \equiv 1 \pmod{p}$ ja tästä edelleen Lauseen 1.3 perusteella $j - k \equiv 0 \pmod{p-1}$ eli $j \equiv k \pmod{p-1}$.
"$\Longleftarrow$" Mikäli $j \equiv k \pmod{p-1}$, niin $j-k \equiv 0 \pmod{p-1}$ ja edelleen lauseen 1.3 perusteella $g^{j-k} \equiv 1 \pmod{p}$. Kun kerrotaan puolittain luvulla g^k saadaan, että $g^{j-k}g^k \equiv g^k \pmod{p}$. Tästä saadaan potenssin laskusääntöjen mukaan $g^{j-k+k} \equiv g^k \pmod{p}$ ja edelleen $g^j \equiv g^k \pmod{p}$. □

1.1 Diskreetin logaritmin ongelma

Olkoon $H = \langle\beta\rangle$, $\#H = h$, missä β ja h tunnetaan. Valitaan $y \in H$ vapaasti. Määritä tällöin $\log_\beta y$, kun h=ISO.

Esimerkki 1.5. Jos valitaan $h = 2^{1000}$, $1 \leq r \leq h-1$. Tällöin

$$r = e_{t-1}2^{t-1} + \cdots + e_0, t \leq 1000.$$

Potenssin a^r laskemiseen tarvitaan ainoastaan ≤ 1000 laskutoimitusta, kun taas diskreetin logaritmin $\log_\beta y$ määrääminen vaatii jopa 2^{1000} laskua H:ssa, eli käytännössä potenssiinkorotus on nopeaa ja logaritmin määrittäminen äärettömän hidasta.

Huomautus 1.6. $2^{10} = 1024$ ja $1000 = 10^3$, joten voidaan arvioida, että $2^{10} \approx 10^3$ ja sen perusteella edelleen, että $2^{1000} = 2^{10^{100}} = 10^{3^{100}} = 10^{300}$.

2 Digitaalisen käteisen vaatimukset

Jotta digitaalisesta rahasta voidaan puhua nykyistä käteistä vastaavana vaihdantavälineenä on sillä oltava tuntemamme käteisen kaltaiset ominaisuudet. Vaikka modernit kopio- ja tulostinlaitteet ovat erittäin kehittyneitä ja voivat näennäisesti tuottaa kopioita käyttämistämme seteleistä, niin seteleissä on kuitenkin olemassa useita väärentämistä hankaloittavia turvatekijöitä, joiden avulla setelin vastaanottaja voi tunnistaa aidon setelin väärennöksestä.

Digitaalisen informaation, datan, tapauksessa jäljet eivät kuitenkaan ole yhtä selvät, vaan alkuperäisestä datasta tehty kopio vastaa aitoa täydellisesti eikä niitä siten voida erottaa toisistaan. On siis mahdollista, että joku, jolla on hallussaan alkuperäinen digitaalinen kolikko voi luoda siitä useita kopioita. Luonnollisesti kopiointi tulee voida estää jollakin tavalla. Eräs mahdollisuus tähän olisi se, että keskuspankki, joka on laskenut digitaaliset kolikot liikkeelle, pitää kirjaa jokaisesta olemassa olevasta kolikosta ja niiden omistajista. Jokaisen kolikon ja niiden omistajien seurantaa puolestaan aiheuttaa sen ongelman ettei digitaalisen käteisen käyttö olisi anonyymiä, mikä on yksi nykyisen käteisen perusominaisuuksista. Myös ajoittaiset yhteysongelmat keskuspankin ja rahan vastaanottajan välillä ovat mahdollisia, joten olisi suotavaa, että rahan vastaanottava taho voisi varmentaa sen aitouden ilman yhteydenottoa pankkiin.

Voidaankin määritellä kuusi tärkeää ominaisuutta, jotka digitaalisella käteisellä tulisi olla:

1. Rahansiirtojen tulee tapahtua turvallisesti tietoverkkojen yli.
2. Rahaa ei voi kopioida tai käyttää kahdesti.
3. Rahan käyttäjän anonymiteetti tulee säilyttää. Maksun saajan tai pankin ei ole mahdollista selvittää käyttäjää, ellei ole syytä epäillä vilppiä.
4. Rahansiirrot voidaan suorittaa ilman jatkuvaa verkkoyhteyttä, eli keskuspankin kanssa ei tarvitse kommunikoida siirron aikana.
5. Rahaa voidaan siirtää vapaasti käyttäjien välillä.
6. Jokainen digitaalinen kolikko voidaan jakaa pienempiin osuuksiin.

3 Digitaalisen käteisen käytön valmistelu

3.1 Osalliset

Käteisen luontiin, hallintaan ja käyttöön osallistuu kolme tekijää: pankki, käyttäjä ja myyjä.

3.2 Järjestelmän luonti

Digitaalisen käteisen luonti tapahtuu jonkin keskitetyn hallinnon, esimerkiksi Suomen keskuspankin, toimesta seuraavasti.

Lause 3.1. *Valitaan suuri alkuluku p siten, että $q = (p-1)/2$ on myös alkuluku. Valitaan g siten, että se on primitiivijuuren neliö modulo p. Tästä seuraa, että*

$$g^{k_1} \equiv g^{k_2} \pmod{p} \text{ jos ja vain jos } k_1 \equiv k_2 \pmod{q}.$$

Todistus.
"$\Longrightarrow$" Olkoon $g = r^2 \pmod{p}$. Tällöin kongruenssista $g^j \equiv g^k \pmod{p}$ seuraa sijoittamalla $g = r^2$, että $(r^2)^j \equiv (r^2)^k \pmod{p}$ ja edelleen potenssin laskusääntöjen mukaan $r^{2j} \equiv r^{2k} \pmod{p}$, joten Lauseen 1.4 perusteella $2j \equiv 2k \pmod{p-1}$. Kun jaetaan puolittain luvulla 2 niin myös moduloluku $p-1$ jaetaan luvulla 2, koska $syt(2, p-1) = 2 \neq 1$. Tällöin $j \equiv k \pmod{(p-1)/2}$ ja edelleen $j \equiv k \pmod{q}$.
"$\Longleftarrow$" Olkoon $r^2 = g \pmod{p}$. Kongruenssista $k_1 \equiv k_2 \pmod{q}$ seuraa sijoittamalla $q = ((p-1)/2)$, että $k_1 \equiv k_2 \pmod{(p-1)/2}$ ja tästä edelleen, kun kerrotaan puolittain kahdella, että $2k_1 \equiv 2k_2 \pmod{(p-1)}$. Lauseen 1.4 perusteella tästä saadaan, että $r^{2k_1} \equiv r^{2k_2} \pmod{p}$ ja potenssin laskusäännöillä $(r^2)^{k_1} \equiv (r^2)^{k_2}$ ja edelleen sijoituksella $r^2 = g$ saadaan $g^{k_1} \equiv g^{k_2}$ □

Valitaan kaksi satunnaista ja salassapidettävää eksponenttia ja määritellään g_1 ja g_2 siten, että ne saadaan korottamalla g valittuihin eksponentteihin mod p. Käytetyt eksponentit hävitetään, sillä niiden säilyttämisestä ei

ole mitään hyötyä ja mikäli hakkeri saisi ne selville, niin koko järjestelmän turvallisuus olisi vaarassa. Saadut luvut

$$g,\ g_1 \text{ ja } g_2$$

julkistetaan. Lisäksi valitaan kaksi julkista hajautusfunktiota joista ensimmäinen, H, ottaa syötteenä viisialkioisen monikon kokonaislukuja ja antaa tulosteena kokonaisluvun modulo q. Jälkimmäinen, H_0, ottaa syötteenä neljäalkioisen monikon kokonaislukuja ja antaa tulosteena kokonaisluvun modulo q.

3.3 Pankki

Pankki valitsee salaisen tunnisteluvun x ja laskee sen jälkeen

$$h \equiv g^x, \quad h_1 \equiv g_1^x \quad \text{ja} \quad h_2 \equiv g_2^x \pmod{p}.$$

Luvut $h,\ h_1$ ja h_2 julkaistaan ja niitä käytetään pankin tunnistamiseen.

3.4 Käyttäjä

Käyttäjä valitsee salaisen tunnisteluvun u ja laskee sen avulla itselleen tilinumeron

$$I \equiv g_1^u \pmod{p}.$$

Tilinumero I lähetetään pankille, joka säilöö sen yhdessä käyttäjän tunnistetietojen kanssa, mutta käyttäjä ei lähetä lukua u pankille. Pankki lähettää käyttäjälle luvun

$$z' \equiv (Ig_2)^x \pmod{p}.$$

3.5 Myyjä

Myyjä valitsee itselleen tunnisteluvun M ja ilmoittaa sen pankille.

4 Digitaalisen käteisen käyttö

4.1 Digitaalisen kolikon luonti

Käyttäjä ottaa yhteyttä pankkiin ja ilmoittaa haluavansa kolikon. Pankki haluaa käyttäjältä todistuksen henkilöllisyydestä, aivan kuten jos käyttäjä nostaa nykyisin käytössä olevaa käteistä rahaa pankkitililtään. Tässä järjestelmässä jokainen luotu kolikko on keskenään yhtä arvokas. Kolikkoa kuvataan kuusialkioisella monikolla

$$(A,\ B,\ z,\ a,\ b,\ r).$$

Vaikka tämä voi kuulostaa turhan monimutkaiselta, niin se on pakollista, jotta voidaan taata käyttäjän anonymiteetti ja samanaikaisesti estää yksittäisen kolikon käyttö kahteen kertaan. Edellä mainitut luvut saadaan seuraavasti:

1. Pankki valitsee satunnaisen luvun w, joka on eri jokaiselle luodulle kolikolle, ja suorittaa laskutoimitukset

   $$g_w \equiv g^w \quad \text{ja} \quad \beta \equiv (Ig_2)^w \pmod{p},$$

   ja lähettää luvut g_w ja β käyttäjälle.

2. Käyttäjä valitsee salaisen ja satunnaisen viisialkioisen monikon

   $$(s,\ x_1,\ x_2,\ \alpha_1,\ \alpha_2).$$

3. Käyttäjä suorittaa laskutoimitukset

   $$A \equiv (Ig_2)^s, \quad B \equiv g_1^{x_1} g_2^{x_2}, \quad z \equiv (z')^s,$$

   $$a \equiv g_w^{\alpha_1} g^{\alpha_2} \quad \text{ja} \quad b \equiv \beta^{s\alpha_1} A^{\alpha_2} \pmod{p}.$$

   Kolikoita, joille $A = 1$ ei hyväksytä. Se voi tapahtua vain kahdella tavalla. Jos $s \equiv 0$ modulo q, joten vaaditaan että $s \not\equiv 0$ modulo q ja jos $Ig_2 \equiv 1$ modulo p, mikä tarkoittaisi, että käyttäjä olisi ratkaissut diskreetin logaritmin ongelman onnekkaalla valinnalla u. Alkuluku p tulisi valita niin suureksi, ettei tämä käytännössä ole mahdollista.

4. Käyttäjä suorittaa laskutoimituksen

$$c \equiv \alpha_1^{-1} H(A, B, z, a, b) \pmod{q}$$

ja lähettää luvun c pankille. Tässä H on aiemmin mainittu hajautusfunktio.

5. Pankki suorittaa laskutoimituksen

$$c_1 \equiv cx + w \pmod{q}$$

ja lähettää luvun c_1 käyttäjälle.

6. Viimeisenä käyttäjä suorittaa laskutoimituksen

$$r \equiv \alpha_1 c_1 + \alpha_2 \pmod{q}.$$

Kolikko $(A,\ B,\ z,\ a,\ b,\ r)$ on nyt valmis ja kolikkoa vastaava rahasumma on vähennetty käyttäjän pankkitililtä.

Tämä suhteellisen nopea prosessi toistetaan aina, kun käyttäjä haluaa kolikon. Pankin tulee valita jokaiselle siirrolle uusi w ja myös jokaisen käyttäjän tulee valita uusi viisialkioinen monikko $(s,\ x_1,\ x_2,\ \alpha_1,\ \alpha_2)$ jokaiselle uudelle kolikolle.

4.2 Digitaalisen kolikon käyttö

Käyttäjä antaa kolikon $(A,\ B,\ z,\ a,\ b,\ r)$ myyjälle, jolloin suoritetaan seuraavat toimenpiteet:

1. Myyjä tarkistaa pitääkö paikkansa, että

Lemma 4.1.

$$g^r \equiv a h^{H(A,B,z,a,b)} \quad ja \quad A^r \equiv z^{H(A,B,z,a,b)} b \quad (mod\ p).$$

Todistus.
Todistetaan ensin väite

$$g^r \equiv ah^{H(A,B,z,a,b)} \pmod{p}.$$

Vasen puoli:
Sijoituksilla $r \equiv \alpha_1 c_1 + \alpha_2$, $c_1 \equiv cx + w$ ja $c \equiv \alpha_1^{-1} H(A, B, z, a, b)$ saadaan

$$\begin{aligned} g^r &\equiv g^{\alpha_1 c_1 + \alpha_2} \equiv g^{\alpha_1 (cx+w) + \alpha_2} \equiv g^{\alpha_1 cx + \alpha_1 w + \alpha_2} \\ &\equiv g^{\alpha_1 \alpha_1^{-1} H(A,B,z,a,b)x + \alpha_1 w + \alpha_2} \equiv g^{H(A,B,z,a,b)x + \alpha_1 w + \alpha_2} \pmod{p}. \end{aligned}$$

Oikea puoli:
Sijoituksilla $a \equiv g_w^{\alpha_1}$ ja $g_w \equiv g^w, h \equiv g^x$ sekä potenssin laskusäännöillä saadaan

$$\begin{aligned} ah^{H(A,B,z,a,b)} &\equiv g_w^{\alpha_1} g^{\alpha_2} h^{H(A,B,z,a,b)} \equiv (g^w)^{\alpha_1} g^{\alpha_2} (g^x)^{H(A,B,z,a,b)} \\ &\equiv g^{w\alpha_1} g^{\alpha_2} g^{xH(A,B,z,a,b)} \equiv g^{w\alpha_1 + \alpha_2 + xH(A,B,z,a,b)} \pmod{p}. \end{aligned}$$

Kongruenssien kummankin puolen kantaluku ja potenssit ovat samat, joten myös kongruenssi pätee.
Todistetaan seuraavaksi väite

$$A^r \equiv z^{H(A,B,z,a,b)} b \pmod{p}.$$

Vasen puoli:
Sijoituksilla $r \equiv \alpha_1 c_1 + \alpha_2$ ja $A \equiv (Ig_2)^s$ saadaan

$$A^r \equiv A^{\alpha_1 c_1 + \alpha_2} \equiv ((Ig_2)^s)^{\alpha_1 c_1 + \alpha_2} \equiv (Ig_2)^{s\alpha_1 c_1 + s\alpha_2} \pmod{p}$$

ja edelleen sijoituksilla $c_1 \equiv cx + w$ ja $c \equiv \alpha_1^{-1} H(A, B, z, a, b)$ saadaan

$$\begin{aligned} (Ig_2)^{s\alpha_1 c_1 + s\alpha_2} &\equiv (Ig_2)^{s\alpha_1 (cx+w) + s\alpha_2} \equiv (Ig_2)^{s\alpha_1 cx + s\alpha_1 w + s\alpha_2} \\ &\equiv (Ig_2)^{s\alpha_1 \alpha_1^{-1} H(A,B,z,a,b)x + s\alpha_1 w + s\alpha_2} \\ &\equiv (Ig_2)^{sH(A,B,z,a,b)x + s\alpha_1 w + s\alpha_2} \pmod{p}. \end{aligned}$$

Oikea puoli:
Sijoituksilla $z \equiv (z')^s, b \equiv \beta^{s\alpha_1} A^{\alpha_2}, \beta \equiv (Ig_2)^w, A \equiv (Ig_2)^s$ ja $z' \equiv (Ig_2)^x$ sekä potenssin laskusäännöillä saadaan

$$\begin{aligned} z^{H(A,B,z,a,b)} b &\equiv ((z')^s)^{H(A,B,z,a,b)} \beta^{s\alpha_1} A^{\alpha_2} \\ &\equiv ((Ig_2)^x)^{sH(A,B,z,a,b)} ((Ig_2)^w)^{s\alpha_1} ((Ig_2)^s)^{\alpha_2} \\ &\equiv (Ig_2)^{xsH(A,B,z,a,b)} (Ig_2)^{ws\alpha_1} (Ig_2)^{s\alpha_2} \\ &\equiv (Ig_2)^{xsH(A,B,z,a,b)+ws\alpha_1+s\alpha_2} \pmod{p}. \end{aligned}$$

Kongruenssien kummankin puolen kantaluku ja potenssit ovat samat, joten myös kongruenssi pätee. □

Jos näin on, niin kauppias tietää, että kolikko on aito, mutta tarvitaan lisää vaiheita, jotta voidaan taata ettei jo kertaalleen käytettyä kolikkoa yritetä käyttää uudestaan.

2. Myyjä suorittaa laskutoimituksen

$$d = H_0(A,\ B,\ M,\ t),$$

missä H_0 on luvussa 3.2 valittu hajautusfunktio ja t on luku, joka vastaa kolikon käyttöaikaa ja -päivää. Luku t on valittu, jotta jokaisella siirtotapahtumalla on eri d. Kauppias lähettää luvun d käyttäjälle.

3. Käyttäjä suorittaa laskutoimitukset

$$r_1 \equiv dus + x_1 \quad \text{ja} \quad r_2 \equiv ds + x_2 \pmod{q},$$

missä u on käyttäjän salainen tunnisteluku, jonka hän valitsi luvussa 3.4, ja luvut $s,\ x_1$ ja x_2 ovat peräisin salaisesta ja satunnaisesta viiden alkion monikosta, joka valittiin luvussa 4.1 kohdassa 2. Käyttäjä lähettää luvut r_1 ja r_2 myyjälle.

4. Myyjä tarkistaa kongruenssin

$$g_1^{r_1} g_2^{r_2} \equiv A^d B \pmod{p}.$$

Jos kongruenssi pätee, niin myyjä hyväksyy kolikon. Muussa tapauksessa myyjä hylkää sen.

4.3 Myyjä tallettaa kolikon pankkiin

Muutamia päiviä myöhemmin myyjä haluaa tallettaa saamansa kolikon pankkiin, jotta hän saa rahat pankkitililleen. Myyjä lähettää pankille kolikon $(A,\ B,\ z,\ a,\ b,\ r)$ sekä kolmikon $(r_1,\ r_2,\ d)$. Pankki suorittaa seuraavat toimenpiteet:

1. Pankki tarkistaa, että kolikkoa $(A,\ B,\ z,\ a,\ b,\ r)$ ei ole talletettu aiemmin, jollei ole, niin pankki suorittaa toimenpiteen 2. Mikäli kolikko oli talletettu jo aiemmin, niin pankki siirtyy kohtaan väärinkäytösten estäminen, jota käsitellään seuraavassa alakohdassa.

2. Pankki suorittaa laskitoimitukset

$$g^r \equiv a h^{H(A,B,z,a,b)}, \quad A^r \equiv z^{H(A,B,z,a,b)} b \quad \text{ja} \quad g_1^{r_1} g_2^{r_2} \equiv A^d B \pmod{p}.$$

Mikäli jokainen näistä toteutuu, niin pankki tietää, että kolikko on aito ja ettei sitä ole käytetty aiemmin, joten se hyväksyy kolikon ja tallettaa rahat myyjän pankkitilille.

4.4 Väärinkäytösten estäminen

Edellä kuvaillun kaltaisessa järjestelmässä on useita kohtia, joissa joku voisi yrittää huijata. Seuraavaksi käsitellään keinoja huijauksien torjumiseen.

1. Käyttäjä yrittää käyttää samaa kolikkoa kahdesti. Ensimmäisen kerran myyjän luona ja toisen kerran kauppiaan luona. Myyjä tallettaa pankkiin kolikon ja sen lisäksi kolmikon $(r_1,\ r_2,\ d)$ kuten edellä kuvattiin.

Kauppias tallettaa saman kolikon ja sen lisäksi kolmikon $(r_1',\ r_2',\ d')$. Helppo laskutoimitus osoittaa, että kun

$$r_1 - r_1' \equiv us(d - d') \quad \text{ja} \quad r_2 - r_2' \equiv s(d - d') \pmod{q},$$

niin

$$r_1 - r_1' \equiv u(r_2 - r_2') \iff u \equiv (r_1 - r_1')(r_2 - r_2')^{-1} \pmod{q}.$$

Pankki ratkaisee kongruenssin $I \equiv g_1^u$ modulo p ja tunnistaa käyttäjän. Koska pankilla ei ole muuten mitään keinoa selvittää lukua u, niin sillä on todisteet että käyttäjä on käyttänyt samaa kolikkoa kahdesti ja käyttäjä saa tuomion, ainakin mikäli tuomioistuin uskoo, että diskreetin logaritmin ratkaisu on lähes mahdotonta.

2. Myyjä yrittää tallettaa saman kolikon kahdesti, ensin aidolla kolmikolla $(r_1,\ r_2,\ d)$ ja uudestaan keksityllä kolmikolla $(r_1',\ r_2',\ d')$. Tämän tekeminen on kuitenkin myyjälle käytännössä mahdotonta, sillä on erittäin vaikea keksiä sellaiset luvut $r_1',\ r_2'\ ja\ d'$ että

$$g_1^{r_1'} g_2^{r_2'} \equiv A^{d'} B \pmod{p}.$$

3. Joku yrittää luoda uuden kolikon tyhjästä ilman pankkia. Tätä varten tulisi löytää ratkaisut kongruensseille

$$g^r \equiv a h^{H(A,B,z,a,b)} \quad \text{ja} \quad A^r \equiv z^{H(A,B,z,a,b)} b \pmod{p}.$$

Näiden kongruenssien ratkaisu on erittäin vaikeaa, sillä jos aloittaa luvuilla $A,\ B,\ z,\ a\ ja\ b$ ja yrittää ratkaista luvun r, niin törmää diskreetin logaritmin ongelmaan, ennen kuin saisi edes ensimmäisen kongruenssin toimimaan. Ainoastaan pankki tuntee luvun x ja ilman sitä on erittäin vaikea selvittää lukua r.

4. Epärehellinen kaupustelija, joka ottaa vastaan kolikon käyttäjältä ja tallettaa sen pankkiin, yrittää samanaikaisesti myös käyttää kolikon

myyjän luona. Epärehellinen kaupustelija antaa kolikon myyjälle, joka ratkaisee luvun d'. On erittäin epätodennäköistä, että $d = d'$. Kaupustelija ei tiedä lukuja $u,\ x_1,\ x_2$ ja s, mutta hänen tulisi valita luvut r_1' ja r_2' siten, että

$$g_1^{r_1'} g_2^{r_2'} \equiv A^{d'} B \pmod{p}.$$

Tässäkin on jälleen kyseessä diskreetin logaritmin ongelma. Mutta mitä jos kaupustelija käyttäisi tuntemiaan lukuja r_1 ja r_2? Koska $d' \neq d$, niin myyjä huomaisi, että

$$g_1^{r_1} g_2^{r_2} \not\equiv A^{d'} B \pmod{p}.$$

5. Joku, joka työskentelee pankissa yrittää luoda väärennetyn kolikon. Hänellä on käytännössä käytössään samat luvut kuin edellisen kohdan kaupustelijalla ja sen lisäksi tilinumero I. Hänen on mahdollista luoda kolikko, joka toteuttaa kongruenssin $g^r \equiv ah^{H(A,B,z,a,b)}$ modulo p, mutta koska käyttäjä on pitänyt luvun u salassa niin pankin työntekijä ei voi keksiä sopivaa lukua r_1. Tietenkin, jos olisi niin, että $s = 0$ niin hänen olisi mahdollista ratkaista luku r_1, mutta koska vaadittiin, että $A \neq 1$, niin $s \neq 0$.

6. Joku varastaa kolikon käyttäjältä ja yrittää käyttää sen itse. Ensimmäinen varmistus kongruenssi menee vielä läpi, mutta koska varas ei tiedä lukua u niin hän ei voi ratkaista lukuja r_1 ja r_2 siten, että $g_1^{r_1} g_2^{r_2} \equiv A^{d'} B$ modulo p.

7. Epärehellinen kaupustelija varastaa kolikon ja kolmikon $(r_1,\ r_2,\ d)$ myyjältä ennen kuin myyjä on ehtinyt tallettaa kolikon pankkiin. Mikäli myyjällä ei ole tallessa jokaisen kolikonsiirron päivämäärä ja aika, joiden avulla hän voisi uudelleen laskea lähtöarvot hajautusfunktiolle H_0 ja todistaa sen tuottavan luvun d, niin kaupustelijan varkaus onnistuu. Toisaalta, vastaava varkausongelma on olemassa myös nykyisen käteisen kanssa.

4.5 Anonymiteetti

Kun käyttäjä siirtää kolikon myyjälle ei hänen missään vaiheessa siirtoa tarvitse luovuttaa myyjälle sellaista tietoa, jonka perusteella hänet voisi tunnistaa, kuten ei myöskään perinteisen käteisen kanssa. Pankki ei saa koskaan tietää lukuja $A,\ B,\ z,\ a,\ b$ tai r ennen kuin kauppias tallettaa kolikon takaisin pankkiin. Itseasiassa pankista saadaan ainoastaan luvut w ja c_1 ja pankki on nähnyt vain luvun c. Siitä huolimatta jokainen kolikko sisältää tiedon, jonka avulla pankin on mahdollista tunnistaa käyttäjä siinä tapauksessa, että käyttäjä yrittää käyttää samaa kolikkoa kahdesti. Onko siis myyjän tai pankin mahdollista tunnistaa käyttäjä kolikon tietojen $(A,\ B,\ z,\ a,\ b,\ r)$ ja kolmikon $(r_1,\ r_2,\ d)$ avulla? Koska näistä vaihtoehdoista pankilla on enemmän tietoa käyttäjästä, se kun tietää käyttäjän tilinumeron I, niin riittää että tutkitaan pankin mahdollisuutta tunnistaa käyttäjä. Koska luvut $s,\ x_1$ ja x_2 ovat salaisia ja satunnaisia lukuja, jotka vain käyttäjä tietää, niin luvut A ja B ovat satunnaisia lukuja. Tarkemmin tutkittuna, A on luvun g satunnainen potenssi, eikä sen avulla voida päätellä lukua I. Luku z on vain A^x modulo p, joten myöskään siitä ei saada mitään tietoa, jota ei olisi saatu luvusta A. Koska luvut a ja b tuovat mukanaan vain uudet salaiset ja satunnaiset luvut α_1 ja α_2, niin myöskin ne ovat vain satunnaisia lukuja kaikkien muiden, paitsi käyttäjän näkökulmasta.

Joten meillä on viisi lukua, $A,\ B,\ z,\ a$ ja b, jotka näyttävät olevan täysin satunnaisia luvun g potensseja kaikille muille, paitsi käyttäjälle. Kuitenkin, kun $c \equiv \alpha_1^{-1} H(A, B, z, a, b)$ modulo q lähetetään pankkiin, voi pankki yrittää laskea arvoa hajautusfunktiolle H ja sitä kautta ratkaista luvun α_1, mutta koska pankki ei ole nähnyt kolikkoa ei sen ole mahdollista laskea arvoa H. Pankki voisi yrittää pitää yllä listaa kaikista sen saamista luvuista c ja myöskin listaa kaikista hajautusfunktion H arvoista jokaiselle kolikolle, jotka on talletettu takaisin ja kokeilla näin kaikkia mahdollisia yhdistelmiä löytääkseen luvun α_1. Kuitenkin helposti nähdään, ettei tämä ole käytännössä mitenkään järkevästi mahdollista, jos järjestelmässä on miljoonia kolikoita. Tämän vuoksi on erittäin epätodennäköistä, että tieto luvusta c ja sitä

kautta luvusta b auttaisi pankkia tunnistamaan käyttäjän.

Luvut α_1 ja α_2 luovat kolikolle niin kutsutun rajoitetun sokean allekirjoituksen, jossa kolikon käyttäminen kerran ei mahdollista käyttäjän tunnistamista, mutta sen käyttäminen kahdesti mahdollistaa ja sitä kautta myös mahdollistaa huijausta yrittävän käyttäjän tunnistamisen ja tuomitsemisen kuten todettiin luvussa 4.4 kohdassa 1.

Rajoitetun sokean allekirjoituksen hyödyllisyyden havaitsemme parhaiten, jos poistamme luvun α_1 prosessista kokonaan valitsemalla $\alpha_1 = 1$. Siinä tapauksessa pankki voisi pitää kirjaa kaikista luvuista c ja niihin liitetyistä käyttäjistä. Kun kolikko talletetaan, niin hajautusfunktion H arvo laskettaisiin ja sitä verrattaisiin olemassa olevaan listaan. Todennäköisesti jokaiselle luvulle c olisi olemassa vain yksi käyttäjä, joten pankki voisi tunnistaa käyttäjän.

5 Esimerkkijärjestelmä

Luodaan esimerkkijärjestelmä ja lasketaan läpi kaikki käytettävät luvut. Yksinkertaisuuden vuoksi käytetään pientä alkulukua p. Käytetyt satunnaisesti valittavat luvut on saatu satunnaisgeneraattorista välillä $[10, 50]$.

5.1 Järjestelmän luonti

Järjestelmää hallinnoiva taho suorittaa seuraavat toimenpiteet. Valitaan alkuluku $p = 83$, jolloin $q = 41$ on myös alkuluku. Alkion g kertaluku on pienin sellainen positiivinen kokonaisluku d, jolle $g^d = 1$. Kertaluvulle käytetään merkintää $d = \text{ord } g$. Alkion kertaluku jakaa kunnan kertolaskuryhmän alkioiden lukumäärän. Jos alkion g kertaluku d on sama kuin kunnan kertolaskuryhmän alkioiden lukumäärä, niin g on kunnan primitiivijuuri. Kertolaskuryhmässä on $83 - 1 = 82$ alkiota ja luvun 82 tekijät ovat 2 ja 41, joten riittää, että tutkitaan vain nämä potenssit. $50^2 \equiv 2500 \equiv 10 \not\equiv 1$ modulo 83

ja 50^{41}. Nopealla potenssilla saadaan, että

$$\begin{aligned}
50^4 \equiv 50^{2^2} \equiv 10^2 \equiv 100 \equiv 17 \pmod{83},\\
50^8 \equiv 50^{4^2} \equiv 17^2 \equiv 289 \equiv 40 \pmod{83},\\
50^{16} \equiv 50^{8^2} \equiv 40^2 \equiv 1600 \equiv 23 \pmod{83},\\
50^{32} \equiv 50^{16^2} \equiv 23^2 \equiv 529 \equiv 31 \pmod{83},
\end{aligned}$$

joten $50^{41} \equiv 50^{32}50^8 50 \equiv 31 \cdot 40 \cdot 50 \equiv 62000 \equiv 82 \not\equiv 1$ modulo 83, eli 50 on primitiivijuuri modulo 83, joten valitaan $g = 50^2 \equiv 10$ modulo 83. Lisäksi valitaan eksponentit 28 ja 15. Lasketaan sekä julkaistaan luvut g_1 ja g_2. Jälleen nopealla potenssilla saadaan, että

$$\begin{aligned}
10^2 \equiv 17 \pmod{83},\\
10^4 \equiv 10^{2^2} \equiv 17^2 \equiv 40 \pmod{83},\\
10^8 \equiv 10^{4^2} \equiv 40^2 \equiv 23 \pmod{83},\\
10^{16} \equiv 10^{8^2} \equiv 23^2 \equiv 31 \pmod{83},
\end{aligned}$$

joten $g_1 = g^{28} = 10^{28} \equiv 10^{16}10^8 10^4 \equiv 31 \cdot 23 \cdot 40 \equiv 28520 \equiv 51$ modulo 83 ja $g_2 = g^{15} = 10^{15} \equiv 10^8 10^4 10^2 10 \equiv 23 \cdot 40 \cdot 17 \cdot 10 \equiv 156400 \equiv 28$ modulo 83. Lisäksi määritellään ja julkaistaan H ja H_0 siten, että ne ovat syötteidensä tulo modulo $q = 41$. Myös kaikki myöhemmät potenssit on laskettu vastaavalla tavalla nopean potenssin menetelmää ja potenssien laskusääntöjä käyttäen.

5.1.1 Pankki

Valitaan $x = 10$ ja lasketaan sekä julkaistaan luvut

$$\begin{aligned}
h \equiv g^x \equiv 10^{10} \equiv 59 \pmod{83},\\
h_1 \equiv g_1^x \equiv 51^{10} \equiv 69 \pmod{83},\\
h_2 \equiv g_2^x \equiv 28^{10} \equiv 30 \pmod{83}.
\end{aligned}$$

5.1.2 Käyttäjä

Valitaan $u = 16$ ja lasketaan

$$I \equiv g_1^u \equiv 51^{16} \equiv 21 \pmod{83}.$$

Käyttäjä lähettää tilinumeron I pankkiin. Pankki laskee ja lähettää käyttäjälle luvun

$$z' \equiv (Ig_2)^x \equiv (21 \cdot 28)^{10} \equiv 21 \pmod{83}.$$

5.1.3 Myyjä

Valitaan $M = 31$.

5.2 Digitaalisen käteisen käyttö

5.2.1 Digitaalisen kolikon luonti

Pankki valitsee luvun $w = 23$ ja laskee luvut

$$\begin{aligned} g_w &\equiv g^w \equiv 10^{23} \equiv 44 \pmod{83}, \\ \beta &\equiv (Ig_2)^w \equiv (21 \cdot 28)^{23} \equiv 37 \pmod{83} \end{aligned}$$

jotka se lähettää käyttäjälle. Käyttäjä valitsee luvut $s = 16$, $x_1 = 31$, $x_2 = 39$, $\alpha_1 = 22$ ja $\alpha_2 = 27$ ja laskee luvut

$$\begin{aligned} A &\equiv (Ig_2)^s \equiv (21 \cdot 28)^{16} \equiv 51 \pmod{83}, \\ B &\equiv g_1^{x_1} g_2^{x_2} \equiv 51^{31} 28^{39} \equiv 77 \cdot 9 \equiv 29 \pmod{83}, \\ z &\equiv (z')^s \equiv 21^{16} \equiv 69 \pmod{83}, \\ a &\equiv g_w^{\alpha_1} g^{\alpha_2} \equiv 44^{22} 10^{27} \equiv 21 \cdot 30 \equiv 49 \pmod{83}, \\ b &\equiv \beta^{s\alpha_1} A^{\alpha_2} \equiv 37^{16 \cdot 22} 51^{27} \equiv 63 \cdot 29 \equiv 1 \pmod{83}, \\ c &\equiv \alpha_1^{-1} H(A, B, z, a, b) \equiv 28 \cdot H(51 \cdot 29 \cdot 69 \cdot 49 \cdot 1) \equiv 28 \cdot 16 \equiv 38 \pmod{41}. \end{aligned}$$

Käyttäjä lähettää luvun c pankkiin. Pankki laskee luvun

$$c_1 \equiv cx + w \equiv 38 \cdot 10 + 23 \equiv 34 \pmod{41}$$

ja lähettää sen käyttäjälle, joka laskee vielä luvun

$$r \equiv \alpha_1 c_1 + \alpha_2 \equiv 22 \cdot 34 + 27 \equiv 37 \pmod{41}.$$

Kolikko $(A,\ B,\ z,\ a,\ b,\ r) = (51,\ 29,\ 69,\ 49,\ 1,\ 37)$ on näin luotu ja kolikon arvoa vastaava summa vähennetty käyttäjän pankkitililtä.

5.2.2 Digitaalisen kolikon käyttö

Käyttäjä haluaa käyttää kolikkoaan kaupankäynnissä ja antaa kolikon myyjälle. Myyjä suorittaa tarkistuslaskut $g^r \equiv ah^{H(A,B,z,a,b)}$ modulo p ja $A^r \equiv z^{H(A,B,z,a,b)}b$ modulo p.

$$\begin{aligned} H(A,B,z,a,b) \equiv H(51 \cdot 29 \cdot 69 \cdot 49 \cdot 1) &\equiv 16 \pmod{41}, \\ g^r \equiv 10^{37} &\equiv 27 \pmod{83}, \\ ah^{H(A,B,z,a,b)} \equiv 49 \cdot 59^{16} &\equiv 27 \pmod{83}, \\ A^r \equiv 51^{37} &\equiv 9 \pmod{83}, \\ z^{H(A,B,z,a,b)}b \equiv 69^{16} \cdot 1 &\equiv 9 \pmod{83}. \end{aligned}$$

Näin myyjä varmistaa, että kolikko on aito. Suoritetaan vielä järjestelmän huijaamista estävät vaiheet. Myyjä laskee luvun $d = H_0(A,B,M,t)$, valitaan $t = 30$ ja lasketaan luku

$$d = H_0(A,B,M,t) = H_0(51 \cdot 29 \cdot 31 \cdot 30) \equiv 2 \pmod{41}.$$

Kauppias lähettää luvun d käyttäjälle, joka laskee luvut

$$\begin{aligned} r_1 \equiv dus + x_1 &\equiv 2 \cdot 16 \cdot 16 + 31 \equiv 10 \pmod{41}, \\ r_2 \equiv ds + x_2 &\equiv 2 \cdot 16 + 39 \equiv 30 \pmod{41} \end{aligned}$$

ja lähettää ne myyjälle. Myyjä tarkistaa kongruenssin $g_1^{r_1} g_2^{r_2} \equiv A^d B$.

$$\begin{aligned} g_1^{r_1} g_2^{r_2} \equiv 51^{10} 28^{30} &\equiv 69 \cdot 25 \equiv 65 \pmod{83}, \\ A^d B \equiv 51^2 \cdot 29 &\equiv 28 \cdot 29 \equiv 65 \pmod{83} \end{aligned}$$

ja voi näin ollen hyväksyä kolikon maksuvälineenä.

5.2.3 Myyjä tallettaa kolikon pankkiin

Myyjä haluaa tallettaa käyttäjältä saamansa kolikon $(A,\ B,\ z,\ a,\ b,\ r) = (51,\ 29,\ 69,\ 49,\ 1,\ 37)$ pankkiin, jotta saa rahat pankkitililleen. Myyjä lähettää kolikon $(51,\ 29,\ 69,\ 49,\ 1,\ 37)$ ja kolmikon $(r_1,\ r_2,\ d) = (10,\ 30,\ 2)$ pankkiin. Pankki tarkistaa, ettei kolikkoa ole talletettu aiemmin ja jollei ole, niin pankki suorittaa laskut, jotka käsiteltiin jo edellisessä kohdassa myyjän kanssa asioidessa $g^r \equiv ah^{H(A,B,z,a,b)}$, $A^r \equiv z^{H(A,B,z,a,b)}b$ ja $g_1^{r_1}g_2^{r_2} \equiv A^dB$ modulo 83. Näin ollen pankki hyväksyy kolikon ja tallettaa rahat myyjän pankkitilille. Mikäli kolikko oli talletettu jo aiemmin, niin pankki siirtyy kohtaan väärinkäytösten estäminen.

5.2.4 Väärinkäytösten estäminen

Mikäli käyttäjä olisi käyttänyt samaa kolikkoa sekä myyjä että kauppiaan luona, niin myyjän luona suoritetut laskut olisivat tuottaneet aiemmin lasketun kolmikon $(r_1,\ r_2,\ d) = (10,\ 30,\ 2)$ ja kauppiaan luona olisi hänen valitsemillaan $M = 30$ ja $t = 40$ laskettu

$$\begin{aligned} d' &= H_0(51 \cdot 29 \cdot 30 \cdot 40) \equiv 33 \pmod{41}, \\ r_1' &\equiv d'us + x_1 \equiv 33 \cdot 16 \cdot 16 + 31 \equiv 33 \pmod{41}, \\ r_2' &\equiv d's + x_2 \equiv 33 \cdot 16 + 39 \equiv 34 \pmod{41} \end{aligned}$$

ja tarkistus

$$\begin{aligned} g_1^{r_1'}g_2^{r_2'} &\equiv 51^{33}28^{34} \equiv 29 \pmod{83} \\ A^{d'}B &\equiv 51^{33} \cdot 29 \equiv 29 \pmod{83} \end{aligned}$$

joiden avulla olisi saatu kolmikko $(r_1',\ r_2',\ d') = (33,\ 34,\ 33)$. Kun sekä myyjä, että kauppias ovat tallettaneet kolikon $(51,\ 29,\ 69,\ 49,\ 1,\ 37)$ voi pankki ratkaista kongruenssin

$$\begin{aligned} u \equiv (r_1 - r_1')(r_2 - r_2')^{-1} &\equiv (10 - 33)(30 - 34)^{-1} \equiv \\ 18 \cdot 37^{-1} &\equiv 18 \cdot 10 \equiv 16 \pmod{41}, \end{aligned}$$

jolloin se voi ratkaista myös kongruenssin

$$I \equiv g_1^u \equiv 51^{16} \equiv 21 \pmod{83}$$

ja tunnistaa huijanneen käyttäjän.

Lähdeluettelo

[1] W. Trappe, L. Washington: *Introduction to Cryptography with Coding Theory* . Pearson Education, Inc. New Jersey, 2006.