IDENTITEETTIIN PERUSTUVISTA JULKISEN AVAIMEN KRYPTOSYSTEEMEISTÄ

Heikki Pernaa

Pro gradu -tutkielma
Helmikuu 2011

MATEMATIIKAN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan laitos

PERNAA, HEIKKI: Identiteettiin perustuvista julkisen avaimen kryptosysteemeistä
Pro gradu -tutkielma, 37 s.
Matematiikka
Helmikuu 2011

Tutkielman tarkoitus on esitellä lukijalle mitä identiteettiin perustuva julkisen avaimen kryptografia tarkoittaa, minkälaisia kryptosysteemejä identiteettiin perustuen on kehitetty ja minkälaisia sovellusmahdollisuuksia sillä on. Lukijan olisi hyvä tuntea kryptografian perusteiden lisäksi myös algebraa, lukuteoriaa ja koodausteoriaa.

Tutkielma alussa esitellään autentikointia, identifiointia ja hieman niihin liittyviä määritelmiä. Tämän jälkeen esitellään julkisen avaimen kryptografiaa yleisesti ja pohditaan autentikoinnin tarvetta julkisen avaimen kryptosysteemeissä. Tutkielmassa esitellään neljä erilaista identiteettiin perustuvaa kryptosysteemiä, jotka ovat Shamirin allekirjoitussysteemi, Guilloun ja Quisquaterin identifiointisysteemi, Sakain, Ohgishin ja Kasaharan avaimenvaihtosysteemi ja Bonehin ja Franklinin kryptosysteemi. Kahteen jälkimmäiseen systeemiin liittyvät olennaisesti parikuvaukset, joita myös käsitellään lyhyesti niiden ominaisuuksien osalta. Tutkielman lopuksi esitellään identiteettiin perustuvan julkisen avaimen kryptografian sovellusmahdollisuuksia.

Shamirin allekirjoitussyteemi antaa oivallisen tavan digitaalisten dokumenttien allekirjoittamiseen. Guilloun ja Quisquaterin identifiointisysteemi on tarkoitettu nimensä mukaan asiakkaan henkilöllisyyden varmentamiseen. Sakain, Ohgishin ja Kasaharan avaimenvaihtosysteemiä käyttämällä asiakkaat kykenevät luomaan yhteisen salaisen avaimen, minkä vuoksi he voivat käyttää jotain symmetristä kryptosysteemiä turvallisesti. Bonehin ja Franklinin kryptosysteemi on viestien salaukseen tarkoitettu julkisen avaimen kryptosysteemi sillä erotuksella, että julkista avainta ei käyttäjien toimesta tarvitse identifioida erikseen, kuten ei kolmessa muussakaan tutkielman systeemissä. Kaikille tutkielmassa esiintyville systeemeille on lisäksi yhteistä se, että niissä tarvitaan asiakkaiden lisäksi kolmas luotettava osapuoli, joka luo asiakkaille julkisen ja salaisen avaimen henkilöllisyystodistusta vastaan. Asiakkaiden julkiset avaimet perustuvat heidän identiteetteihinsä, jolloin niiden kuuluminen tietyille henkilöille on kaikkien tunnistettavissa. Tästä syystä avainten autentikointia ei tarvitse asiakkaiden toimesta enää tehdä ja suurten avaimenhallintajärjestelmien resurssivaatimukset vähenevät.

Asiasanat: kryptografia, identiteettiin perustuva, julkinen avain, Shamir, Guillou-Quisquater, Sakai-Ohgishi-Kasahara, Boneh-Franklin.

Sisältö

1 Johdanto **1**

2 Autentikointi ja identifiointi **3**

2.1 Identifiointi 4

2.2 Viestin alkuperän autentikointi 4

3 Julkisen avaimen kryptografia **6**

3.1 Autentikoinnin tarve julkisen avaimen systeemeissä 7

3.2 Digitaaliset allekirjoitussysteemit 8

4 Diskreetin logaritmin ongelma **10**

5 Identiteettiin perustuva julkisen avaimen kryptografia **11**

5.1 Identiteettiin perustuva Shamirin allekirjoitussysteemi 12

5.1.1 Systeemiparametrien luominen 12

5.1.2 Käyttäjän avaimen luominen 13

5.1.3 Allekirjoituksen tekeminen 13

5.1.4 Allekirjoituksen varmentaminen 13

5.1.5 Esimerkki 14

5.2 Guilloun ja Quisquaterin identifiointisysteemi 16

5.2.1 Systeemiparametrien luominen 16

5.2.2 Käyttäjän avaimen luominen 17

5.2.3 Identifiointi 17

5.2.4 Esimerkkejä 18

5.3 Parikuvauksista 21

5.3.1 Perusteet 21

5.4 Identiteettiin perustuva epäinteraktiivinen Sakain, Ohgishin ja Kasaharan avaimenvaihtosysteemi 24

5.4.1 Systeemiparametrien luominen 24

5.4.2 Käyttäjän avaimen luominen 25

5.4.3 Avaimen vaihto 25

5.5 Identiteettiin perustuva Bonehin ja Franklinin kryptosysteemi 26

5.5.1 Systeemiparametrien luominen 27
5.5.2 Käyttäjän avaimen luominen 28
5.5.3 Viestin salaus 28
5.5.4 Salauksen purku 29
5.6 Bonehin ja Franklinin systeemin laajennus 29
5.6.1 Systeemiparametrien luominen 30
5.6.2 Käyttäjän avaimen luominen 30
5.6.3 Viestin salaus 30
5.6.4 Salauksen purku 31
5.6.5 Turvallisuudesta 31
5.7 Autentikointi ilman avaimenvaihtokanavaa 32

6 Identiteettiin perustuvan kryptografian sovelluksia 34
6.1 Julkisen avaimen kumoaminen 34
6.2 Dekryptausavainten jakaminen 35

Kirjallisuutta 37

1 Johdanto

Jokapäiväisessä elämässä on paljon tilanteita, joissa on välttämätöntä pystyä todistamaan jonkun tai joidenkin osapuolien identiteetti. Tällaisia tilanteita ovat esimerkiksi:

1. Rahan nostaminen pankkiautomaatista, jossa asiakas tunnistetaan pankkikortin ja siihen kuuluvan PIN-koodin avulla.

2. Puhelimen välityksellä tehtyjen ostosten maksaminen, johon tarvitaan ainoastaan luottokortin numero.

3. Tietokoneen etäkäyttö Internetin välityksellä, mihin tarvitaan käyttäjänimi ja salasana.

Käytännössä tämän tyyppiset menetelmät eivät ole kovin turvallisia. Puhelimen välityksellä toteutettavat protokollat ovat alttiita salakuuntelulle. Tällöin asiakkaan henkilötiedot päätyvät vääriin käsiin, ja salakuuntelija voi käyttää niitä omiin tarkoituksiinsa. Asiakkaan käyttäessä pankkikorttia rikollinen taho voi murtautua kommunikointikanavaan, josta hän voi kopioida kortin magneettinauhan tiedot ja PIN-koodin. Tällöin huijarilla on pääsy asiakkaan pankkitilille ja pankin palveluihin. Tietokoneen etäkäyttön ongelma on internetyhteys, jonka kautta tieto kulkee suojaamattomassa muodossa. Tietoliikennettä seuraava taho saattaa saada selville asiakkaan käyttäjänimen ja salasanan.

Modernissa kryptografiassa tai tarkemmin *julkisen avaimen kryptosysteemeissä* osapuolten identiteettien varmentaminen on myös tärkeässä roolissa tietoturvan säilymisen kannalta. Osapuolilla tulee olla varmuus siitä, kenen kanssa he kommunikoivat, eli kenen julkisella avaimella he kryptaavat. Suurissa organisaatioissa erilaiset avaimenhallintajärjestelmät saattavat olla hankalia toteuttaa ja ylläpitää käyttäjien paljouden vuoksi. Tämän tutkielman tarkoituksena on esittää edellä mainittuun ongelmaan ratkaisu toteuttamalla erilaisia julkisen avaimen kryptosysteemejä perustuen asiakkaiden identiteetteihin. Tutkielman luvut 2, 3 ja 4 perustuvat teoksiin [1], [2] ja [3]. Luvun 5 päälähteenä on käytetty kirjaa [6] ja osaltaan myös lähdettä [5]. Identiteettiin

perustuvan kryptografian sovelluksia käsittelevä luku perustuu Dan Bonehin ja Matthew K. Franklinin kirjoittamaan artikkeliin [4].

2 Autentikointi ja identifiointi

Autentikointi terminä on laajalti käytetty. Se tarkoittaa toimintaa, jolla taataan, että entiteetit todellakin ovat keitä he väittävät olevansa, tai että vastaanotettua ja lähetettyä informaatiota ei ole muutettu luvatta ulkopuolisten tahojen toimesta. Kuvitellaan tilanne, jossa kaksi osapuolta, Alice ja Bob, haluavat keskustella erittäin arkaluonteisista asioista. He ovat kuitenkin eri maissa, joista kumpikaan ei tarjoa turvallista kommunikointiyhteyttä. Maiden tiedetään myös seuraavan kaikkea viestiliikennettä. Jotta Alice ja Bob voivat olla varmoja, ettei kukaan ulkopuolinen pääse käsiksi heidän väliseen viestiliikenteeseensä, heidän tulee saada varmuus aluksi toistensa identiteeteistä. Tämän jälkeen Alicen ja Bobin tulee olla varovaisia, ettei ulkopuoliset muokkaa heidän lähettämiään viestejä.

Edellä esitettyssä tilanteessa Alicella ja Bobilla on ainakin kaksi kommunikointivaihtoehtoa, joiden vaatimat autentikointimenetelmät ovat erilaisia.

1. Alice ja Bob voivat kommunikoida aktiivisesti ilman huomattavaa viivettä reaaliajassa.

2. He voivat lähettää toisilleen viestejä jollain viiveellä. Tällöin viestit ohjataan tietoverkkojen kautta, varastoidaan ja toimitetaan eteenpäin vähän myöhemmin.

Ensimmäisessä tapauksessa Alicen ja Bobin täytyy saada varmuus toistensa identiteeteistä välittömästi. Tällöin Alice voi lähettää Bobille haasteen, johon vain Bob voi vastata oikein. Bob voi toistaa samanlaisen menettelytavan Alicelle. Tällaista autentikointitapaa kutsutaan *identifioinniksi*.

Jälkimmäisessä tapauksessa ei ole kätevää tehdä haastetta ja odottaa siihen vastausta, vaan viestin alkuperän autentikointi kannattaa suorittaa eri tavalla. Tässä tutkielmassa perehdytään enimmäkseen siihen, kuinka Alice ja Bob voivat toimia turvallisesti jälkimmäisen kommunikointivaihtoehdon puitteissa.

2.1 Identifiointi

Identifiointisysteemien tavoitteena on estää salakuuntelijoiden esittäytyminen väärällä henkilöllisyydellä. Identiteettivarkauksien lisäksi täytyy estää tilanteet, jossa Bob itse yrittää esittäytyä Alicena sen jälkeen, kun Bob on saanut todistuksen Alicen identiteetistä. Toisin sanoen Alicen täytyy pystyä todistamaan identiteettinsä Bobille tavalla, joka ei vaadi henkilötietojen luovuttamista.

Määritelmä 2.1. *Identifiointisysteemi* antaa osapuolelle todistuksen toisen osapuolen identiteetin oikeellisuudesta, ja samanaikaisesti varmistaa toisen osapuolen luoneen tämän todistuksen.

Seuraavaksi esitetään kaksi hyvin yksinkertaista esimerkkiä erilaisista arkipäiväisistä identifiointimenetelmistä.

Esimerkki 1. *Alice soittaa puhelimella Bobille. Jos osapuolet tuntevat toisensa, identifiointi tapahtuu äänen tunnistuksen perusteella. Menetelmä on yleisesti käytössä, vaikka se ei ole turvallinen.*

Esimerkki 2. *Alice haluaa asioida pankkiautomaatilla. Hän antaa pankkikorttin ja PIN-tunnuksen automaatille, joka lukee kortilla olevat tiedot magneettijuovalta ja todentaa PIN-tunnuksen kuuluvan juuri tämän kortin omistajalle. Jos PIN-tunnus on sama kuin kortin omistajan, Alice pääsee käsiksi pankkiautomaatin palveluihin.*

Esimerkki 1 on eräs tapaus *molemminpuolisesta autentikoinnista*, kun taas esimerkissä 2 on kyse *yksipuolisesta autentikoinnista*.

2.2 Viestin alkuperän autentikointi

Määritelmä 2.2. *Viestin alkuperän autentikointi* antaa viestin vastaanottajalle varmuuden viestin lähettäjän identiteetistä.

Yleensä vastaanottaja saa viestin mukana lisäinformaatiota, jonka avulla hän voi määrittää viestin lähettäjän identiteetin. Tämä autentikoinnin muoto on käyttökelpoinen tilanteissa, joissa kommunikointi ei tapahdu reaaliajassa.

Esimerkki 3. *Alice lähettää Bobille sähköpostiviestin, joka menee Internetin kautta Bobin sähköpostikansioon odottamaan avaamista. Alice ja Bob eivät ylläpidä tällöin suoraa kommunikointi yhteyttä, vaan Bob avaa viestin vasta kun hänelle sopii. Bob haluaa varmistua, että viestin luoja ja lähettäjä on Alice.*

Viestin alkuperän autentikointi antaa Bobille todistuksen siitä, että vastaanotettu viesti on täsmälleen sellaisessa muodossa, millaiseksi Alice on sen luonut. Jos viestiä muutetaan ulkopuolisen tahon toimesta, niin Alice ei ole enää viestin luoja.

3 Julkisen avaimen kryptografia

Klassisissa kryptosysteemeissä kryptaus- ja dekryptausfunktiot toimivat samalla avaimella K, jonka salassapitäminen on oleellista. Alicen ja Bobin täytyy keksiä ehdottoman turvallinen keino sopia käytettävästä avaimesta, mikä saattaa olla joissakin tilanteissa erittäin hankalaa. Tässä osiossa esitellään modernin kryptografian työkalu tämän ongelman ratkaisemiseen.

Julkisen avaimen kryptografiassa yhden avaimen sijaan käytetään kahta eri avainta, joista toinen on julkinen ja toinen salainen. Olennaista on, että salaisen avaimen laskeminen julkisen avaimen perusteella on *laskennallisesti vaikea ongelma*. Kuka tahansa voi julkisen avaimen avulla kryptata viestin, mutta dekryptaus onnistuu ainoastaan salaisen avaimen haltijalta. Matemaattisesti julkisen avaimen kryptosysteemit perustuvat *yksisuuntaisiin funktioihin*.

Määritelmä 3.1. *Yksisuuntainen funktio* on sellainen funktio f, jonka arvo $f(x)$ on helppo laskea arvolla x, mutta annetusta funktion arvosta $f(x)$ on vaikea laskea arvoa x.

Modernissa kryptografiassa käytetään paljon *hash-funktioita* yksisuuntaisina funktioina.

Määritelmä 3.2. *Hash-funktio* on laskennallisesti tehokas funktio, joka kuvaa satunnaista pituutta olevan binäärisen bittijonon joksikin halutun pituiseksi binääriseksi bittijonoksi.

Etuna hash-funktion käytössä on, että se kuvaa syötteeksi annetun satunnaista pituutta olevan bittijonon tiiviimmäksi hash-arvoksi. Yleensä kryptografiassa käytetään sellaisia yksisuuntaisia hash-funktioita, että on laskennallisesti vaikeaa löytää kaksi erilaista syötettä, joiden hash-arvot olisivat samat.

Lukittu postilaatikko on käytännön esimerkki siitä, kuinka julkisen avaimen kryptosysteemi toimii. Kuka tahansa voi laittaa laatikkoon kirjeen, mutta ainoastaan laatikon omistaja pystyy avaamaan lukitun laatikon ja avaamaan kirjeen.

Määritelmä 3.3. Olkoon $\{E_e : e \in K\}$ joukko kryptausfunktioita, $\{D_d : d \in K\}$ joukko dekryptausfunktioita ja K kaikkien mahdollisten avainten joukko. Kryptosysteemin sanotaan olevan *julkisen avaimen kryptosysteemi*, jos avainparista (e, d) e on kaikkien saatavilla ja d pidetään salassa.

Ilman salaista avainta d kryptausfunktio E_e käyttäytyy kuin yksisuuntainen funktio. Seuraavaksi esitetään yksinkertainen esimerkki julkisen avaimen kryptosysteemistä, jossa on kaksi osapuolta.

Esimerkki 4. *Alicen halutessa lähettää Bobille viestin m, he toimivat seuraavasti.*

1. *Bob valitsee avainparin (e, d). Hän lähettää julkisen dekryptausavaimen e Alicelle ja pitää salaisen dekryptausavaimen d itsellään.*

2. *Alice kryptaa viestin m käyttäen Bobin julkista avainta. Laskettuaan kryptotekstin $c = E_e(m)$ hän lähettää sen Bobille.*

3. *Bob purkaa salauksen salaisen avaimen avulla kryptotekstistä c laskemalla $D_d(c) = m$.*

Kryptausavain e voidaan julkistaa kaikille halukkaille, jolloin kuka tahansa voi lähettää salattuja viestejä Bobille. On myös huomattavaa, että jos Alice tuhoaa viestin m kryptauksen jälkeen, niin edes hän ei pysty palauttamaan kryptotekstiä c takaisin alkuperäiseksi viestiksi m.

3.1 Autentikoinnin tarve julkisen avaimen systeemeissä

Julkisen avaimen kryptografia vaikuttaa käytännölliseltä systeemiltä, koska se ei vaadi turvallista yhteyttä kryptausavaimen lähettämiseen. Tämä ominaisuus altistaa systeemit kuitenkin aktiivisen vihollisen, Even, juonille. Rikollinen taho saattaa tekeytyä Bobiksi lähettämällä Alicelle oman kryptausavaimensa e', jota Alice erehtyy luulemaan Bobin julkiseksi avaimeksi. Alice kryptaa Bobille kuuluvan viestin m käyttäen Even avainta, ja lähettää kryptotekstin c' salaamattoman yhteyden kautta eteen päin. Eve kaappaa viestin

ja purkaa salauksen omalla dekryptausavaimellaan d'. Saatuaan salaisuuden selville Eve kryptaa salaisuuden m Bobin julkisella avaimella ja lähettää sen Bobille. Nyt Alice ja Bob luulevat kaiken olevan kunnossa, vaikka Eve on saanut käsiinsä erittäin arkaluontoista tietoa. Edellä esitetty tilanne korostaa julkisten avainten autentikoinnin tarvetta. Alicen täytyy olla vakuuttunut, että hän kryptaa todella Bobin avaimella.

3.2 Digitaaliset allekirjoitussysteemit

Käsinkirjoitettuja allekirjoituksia on pidetty todistuksena asiakirjan alkuperästä tai ainakin merkkinä sen sisällön hyväksymisestä. Allekirjoitusta käytetään monissa arkipäiväisissä tilanteissa. Maksettaessa luottokortilla myyjän tulee tarkistaa, että asiakkaan allekirjoitus vastaa luottokortin takana olevaa allekirjoitusta. Tällainen todennus ei tietenkään ole kovin varma ja on selvää, että käsintehtyyn allekirjoitukseen liittyy riskejä. Se voidaan väärentää, tai siirtää toiseen asiakirjaan. Asiakirjaa saatetaan myös muuttaa allekirjoituksen jälkeen.

Julkisen avaimen kryptografia mahdollistaa asiakirjojen turvallisen allekirjoittamisen. Tavanomaiset *digitaaliset allekirjoitussysteemit* ovat kuitenkin usein liian tehottomia pitkien asiakirjojen allekirjoittamiseen. Sen vuoksi allekirjoitussysteemeissä käytetään apuna hash-funktioita. Asiakirjan sijaan Alice allekirjoitaa asiakirjasta lasketun hash-funktion arvon. Seuraavassa esimerkissä käytettävät yksisuuntainen hash-funktio ja digitaalinen allekirjoitussysteemi ovat sovitut etukäteen.

Esimerkki 5. *Alicen halutessa lähettää Bobille allekirjoitetun asiakirjan he toimivat seuraavasti.*

1. *Alice valitsee yksisuuntaisen hash-funktion ja laskee sen avulla asiakirjasta hash-arvon.*

2. *Alice allekirjoittaa hash-arvon salaisella avaimellaan.*

3. *Alice lähettää asiakirjan ja allekirjoitetun hash-arvon Bobille.*

4. *Aluksi Bob laskee hash-arvon Alicen lähettämästä asiakirjasta ja tarkistaa hash-arvon allekirjoituksen Alicen julkisella avaimella. Lopuksi Bob vertaa näitä keskenään ja hyväksyy allekirjoituksen, jos ne ovat samat.*

Hash-funktioita käytettäessä allekirjoitussysteemeissä tilaa ja aikaa säästyy huomattavasti. Sen todennäköisyys, että kaksi eri asiakirjaa saisivat saman n-bittisen hash-arvon, on vain 2^{-n}.

4 Diskreetin logaritmin ongelma

Monet modernit julkisen avaimen kryptosysteemit perustavat turvallisuutensa diskreetin logaritmin laskemisen vaikeuteen, minkä vuoksi se on ollut monien tutkimuksien kohteena. Esimerkiksi tässä tutkielmassa esiintyvistä systeemeistä Sakain, Ohgishin ja Kasaharan avaimenvaihtojärjestelmässä on oleellista, että edellä mainitun ongelman ratkaiseminen tehdään viholliselle tarpeeksi raskaaksi. Seuraavassa määritelmässä kuvataan diskreetin logaritmin ongelma äärellisessä kunnassa Z_p, jossa p on alkuluku. Multiplikatiivinen ryhmä Z_p^* on syklinen, ja sen generaattoria kutsutaan primitiiviseksi alkioksi.

Määritelmä 4.1. Olkoon p alkuluku, $\alpha \in Z_p$ primitiivinen alkio ja $\beta \in Z_p^*$. *Diskreetin logaritmin ongelma* on seuraava: täytyy löytää sellainen yksikäsitteinen kokonaisluku a, että $0 \leq a \leq p-2$ ja

$$\alpha^a \equiv \beta \pmod{p}.$$

Tällaista kokonaislukua a merkitään $\log_\alpha \beta$.

Nykytietämyksen mukaan diskreetin logaritmin ongelmaa pidetään yleisesti vaikeana, kun p on valittu huolellisesti. Toisin sanoen sellaista algoritmia ei ole keksitty, jolla olisi mahdollista ratkaista diskreettejä logaritmeja polynomisessa ajassa. Vaikka diskreetin logaritmin modulo p laskeminen on vaikeaa, niin sille käänteinen operaatio, modulaarinen potenssiin korottaminen, voidaan toteuttaa tehokkaasti esimerkiksi *neliöi ja kerro*-algoritmin avulla. Tällöin potenssiin korottaminen modulo p on yksisuuntainen funktio sopivilla alkuluvuilla p, mikä tekee diskreetin logaritmin ongelmasta tehokkaan apuvälineen kryptografiaan. Hyökkäyksien välttämiseksi p tulee valita ainakin 150 bitin mittaiseksi ja luvun $p-1$ tekijänä täytyy olla ainakin yksi suuri alkuluku.

5 Identiteettiin perustuva julkisen avaimen kryptografia

Julkisen avaimen kryptografiassa tavalliseen tapaan tehtävä avaimen luominen tuottaa satunnaisessa muodossa olevia avaimia. Tämän vuoksi on välttämätöntä voida todentaa julkisen avaimen kuuluminen tietylle asiakkaalle. Satunnaisen julkisen avaimen todennusjärjestelmän luominen ja ylläpitäminen vaatii kuitenkin paljon resursseja. Tässä osiossa perehdytään sellaisiin julkisen avaimen kryptosysteemeihin, jotka pienentävät olennaisesti edellä mainittuja resurssivaatimuksia.

Kuvitellaan tilanne, jossa asiakkaan julkinen avain voidaan suoraan yhdistää johonkin hänen henkilökohtaiseen ominaisuuteensa, kuten nimeen, henkilötunnukseen, sähköposti- tai postiosoitteeseen. Tällöin julkisen avaimen todennusta ei tarvitse enää tehdä erikseen ja järjestelmän resurssivaatimukset vähenevät.

Shamir loi julkisen avaimen kryptosysteemin, joka on edellä kuvaillun kaltainen. Tässä julkisen avaimen kryptosysteemissä avaimen luominen tapahtuu jonkin luotettavan tahon (merkitään jatkossa TA tai Trent) toimesta. TA laskee jonkin yksisuuntaisen funktion avulla omasta salaisesta yleisavaimesta ja asiakkaan julkisesta avaimesta asiakkaalle salaisen avaimen. Asiakkaan julkisena avaimena käytetään jotain bittijonoa ID, joka voidaan yksikäsitteisesti yhdistää asiakkaan identiteettiin tunnuksena. Shamir nimesi järjestelmän *identiteettiin perustuvaksi julkisen avaimen kryptosysteemiksi*.

Luotettavan osapuolen TA tarjoama avainpalvelu kuuluu kaikille järjestelmän asiakkaille. Palvelu on luonteeltaan todentava. TA luo asiakkaalle salaisen avaimen asiakkaan tunnuksen ID perusteella, jota myös järjestelmän toiset osapuolet voivat käyttää asiakkaan identiteetin tunnistamisessa. Ennen kuin TA tarjoaa avainpalvelun asiakkaalle, hänen täytyy olla varma, että asiakkaan esittämä tunnus ID kuuluu kyseiselle asiakkaalle. TA varmistaa myös, että ID paikantaa asiakkaan yksikäsitteisesti, eikä samaa tunnusta voi olla kellään toisella. Kun edellä esitetyt todennukset on tehty, asiakkaan julkisena avaimena voidaan käyttää tunnusta ID, jonka avulla TA voi luoda asiakkaalle salaisen avaimen.

Asiakkaiden on voitava luottaa täysin avainpalvelun tarjoajaan, koska TA voi halutessaan lukea kaikki salatut viestit tai väärentää asiakkaiden allekirjoitukset. Identiteettiin perustuva kryptografia ei näin ollen sellaisenaan sovellu avoimiin ympäristöihin, joissa ehdotonta luottamusta osapuolien välillä ei ole. Tämän osion lopussa on esimerkki kryptosysteemistä, jossa avainpalvelu on jaettu useammalle taholle TA_i. Tällöin asiakkaan salainen avain paljastuu vain sellaisessa tapauksessa, jossa kaikki osapuolet TA_i tekevät yhteistyötä.

5.1 Identiteettiin perustuva Shamirin allekirjoitussysteemi

Identiteettiin perustuvassa Shamirin allekirjoitussysteemissä on neljä algoritmia. Esitetään aluksi määritelmä ja lause, joita tarvitaan ensimmäisessä algoritmissa.

Määritelmä 5.1. *Eulerin phi*-funktio $\phi(n)$ antaa multiplikatiivisessa ryhmässä Z_n^* olevien alkioiden lukumäärän.

Lause 5.2. *Olkoon n kahden alkuluvun p ja q tulo. Tällöin*

$$\phi(n) = (p-1)(q-1).$$

Todistus. Joukosta $\{1, 2, ..., pq-1\}$ jätetään pois kaikki sellaiset alkiot, joilla on yhteisiä tekijöitä luvun pq kanssa eli $\{p, 2p, ..., (q-1)p\}$ ja $\{q, 2q, ..., (p-1)q\}$. Lukumääräisesti jäljelle jää

$$pq - 1 - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1)$$

alkiota. □

5.1.1 Systeemiparametrien luominen

1. Luotettava osapuoli Trent valitsee luvun n, joka on kahden suuren alkuluvun p ja q tulo.

2. Hän valitsee luvun e, joka toteuttaa yhtälön $\text{syt}(e, \phi(n)) = 1$.

3. Hän valitsee luvun d, joka toteuttaa kongruenssin $ed \equiv 1 \pmod{\phi(n)}$. Luku d on Trentin salainen yleisavain.

4. Hän valitsee vahvan yksisuuntaisen hash-funktion $h : \{0,1\}^* \mapsto Z_{\phi(n)}$.

Trent pitää parametrin d systeemin salaisena avaimena ja julkaisee systeemiparametrit (n, e, h).

5.1.2 Käyttäjän avaimen luominen

Olkoon ID_A Alicen identiteettiin yhdistettävä tunnus. Trentin tunnistettua Alicen ja tunnuksen autenttisuuden tarkistamisen jälkeen hän laskee Alicelle salaisen avaimen

$$g \leftarrow (ID_A)^d \pmod{n}$$

5.1.3 Allekirjoituksen tekeminen

Allekirjoittaakseen viestin $M \in \{0,1\}^*$ Alice valitsee luvun $r \in Z_n^*$, ja laskee

$$t \leftarrow r^e \pmod{n}.$$

Hän muuttaa luvun t modulo n binääriluvuksi t_2 ja laskee

$$s \leftarrow g \cdot r^{h(t_2||M)} \pmod{n}.$$

Allekirjoitus on pari (s, t).

Merkintä $||$ tarkoittaa *katenaatio*-operaatiota, jossa kaksi binääristä merkkijonoa liitetään yhteen peräkkäin.

Esimerkki 6. *Oletetaan, että* $t_2 = 1101$ *ja* $M = 1001101$. *Tällöin*

$$(t_2 \,||\, M) = 11011001101.$$

5.1.4 Allekirjoituksen varmentaminen

Bob hyväksyy Alicen allekirjoituksen (s, t) viestiin M, jos

$$s^e \equiv ID_A \cdot t^{h(t_2||M)} \pmod{n}.$$

Näytetään kohta, että identiteettiin perustuva Shamirin allekirjoitussysteemi toimii. Esitetään kuitenkin ensin siinä tarvittava määritelmä, joka on tarpeen myös seuraavassa kryptosysteemissä.

Määritelmä 5.3. Todistamisprotokollan sanotaan olevan *täydellinen*, jos todistaja (Alice) onnistuu vakuuttamaan varmentajan (Bobin) todesta teoreemasta.

Lause 5.4. *Identiteettiin perustuva Shamirin allekirjoitussysteemi on täydellinen.*

Todistus. Bob hyväksyy Alicen allekirjoituksen (s, t) viestiin M, koska

$$\begin{aligned} s^e &\equiv g^e \cdot r^{e \cdot h(t_2 || M)} \pmod{n} \\ &\equiv (ID_A)^{ed} \cdot t^{h(t_2 || M)} \pmod{n} \\ &\equiv ID_A \cdot t^{h(t_2 || M)} \pmod{n}. \end{aligned}$$

□

Jos Bob hyväksyy Alicen allekirjoituksen, niin Alicella on hallussaan arvo $ID_A \cdot t^{h(t_2 || M)}$ ja sen yksikäsitteinen e:s juuri modulo n, joka on arvoltaan s. Yksikäsitteisyys johtuu siitä, että $syt\left(e, \phi\left(n\right)\right) = 1$.

Ulkopuoliselle taholle arvon $ID_A \cdot t^{h(t_2 || M)}$ konstruointi ei ole kuitenkaan vaikeaa. Aluksi voidaan valita satunnainen t, minkä jälkeen lasketaan hash-funktiolla arvo $h\left(t_2 \mid\mid M\right)$. Seuraavaksi lasketaan $t^{h(t_2 || M)} \pmod{n}$ ja lopuksi kerrotaan se luvulla ID_A. Koska tällä tavoin konstruoitu arvo on suuri johtuen hash-funktion käytöstä, e:nnen juuren ottaminen pitäisi olla matemaattisesti vaikeaa. Siksi on oletettavaa, että Alicella on hallussaan e:s juuri tunnuksestaan ID_A, mikä on Trentin luoma salainen avain g, ja jota hänen on pitänyt käyttää allekirjoituksen konstruoimisessa.

5.1.5 Esimerkki

Esitetään seuraavaksi esimerkki siitä, kuinka identiteettiin perustuvaa Shamirin allekirjoitussysteemiä voi käyttää digitaalisten asiakirjojen, esimerkiksi sopimuksien, allekirjoittamiseen. Esimerkissä käytettävät luvut ovat

kuitenkin niin pieniä, että oikeassa elämässä niiden käyttäminen olisi selkeä turvallisuusriski.

Esimerkki 7. *Oletetaan, Trent aloittaa systeemiparametrien luomisen valitsemalla alkuluvut* $p = 683$ *ja* $q = 367$*, joiden avulla hän laskee* $n = 250661$ *ja* $\phi(n) = 249612$*. Trent valitsee vielä julkisen kryptauseksponentin* $e = 503$ *ja laskee sille käänteisluvun* $d = 142919 \pmod{249612}$*, joka on salainen. Trent julkaisee systeemiparametreista kolmikon* (n, e, h)*, jossa* h *on jokin yksisuuntainen hash-funktio.*

Olkoon Alicen identiteettiin yhdistettävä tunnus $ID_A = 140983$*. Trent laskee sen avulla salaisen avaimen*

$$\begin{aligned} g &= (ID_A)^d \pmod{n} \\ &= 140983^{142919} \pmod{250661} \\ &= 188993 \pmod{250661}, \end{aligned}$$

ja luovuttaa sen Alicelle.

Allekirjoittaakseen dokumentin M *Alice valitsee ensin satunnaisen kokonaisluvun* $r = 34579$*, ja laskee sen avulla parametrin*

$$\begin{aligned} t &= r^e \pmod{n} \\ &= 34579^{503} \pmod{250661} \\ &= 134444 \pmod{250661}. \end{aligned}$$

Tämän jälkeen Alice laskee parametrin

$$s = g \cdot r^{h(t_2||M)} \pmod{n},$$

jossa t_2 *on luvun* t *binäärimuoto.*

Vielä ennen parametrin s *laskemista tehdään sellainen oletus, että eksponentti* $h(t \,||\, M)$ *saa arvon* 148997*. Tämän esimerkin kannalta ei ole olennaista paneutua hash-funktion olemukseen syvemmin. Nyt*

$$\begin{aligned} s &= 188993 \cdot 34579^{148997} \pmod{250661} \\ &= 188993 \cdot 246866 \pmod{250661} \\ &= 163347 \pmod{250661}. \end{aligned}$$

Alicen allekirjoitus on pari $(163347, 134444)$.

Bob hyväksyy Alicen allekirjoituksen dokumenttiin M*, jos kongruenssi*

$$s^e \equiv ID_A \cdot t^{h(t||M)} \pmod{n} \tag{1}$$

on tosi. Vasemman puolen arvoksi saadaan

$$s^e = 1633347^{503} = 13940 \pmod{250661}$$

ja oikean puolen arvoksi

$$\begin{aligned} ID_A \cdot t^{h(t||M)} &= 140983 \cdot 134444 \pmod{250661} \\ &= 140983 \cdot 37554 \pmod{250661} \\ &= 13940 \pmod{250661}. \end{aligned}$$

Näin ollen kongruenssi (1) on tosi, ja Alicen allekirjoitus tulee hyväksytyksi.

5.2 Guilloun ja Quisquaterin identifiointisysteemi

Guilloun ja Quisquaterin identifiointisysteemi (merkitään jatkossa GQ-systeemi) pohjautuu RSA-systeemiin ja siihen tarvitaan kolme osapuolta; todistaja Alice, varmentaja Bob ja luotettava osapuoli Trent.

5.2.1 Systeemiparametrien luominen

Luotettava osapuoli Trent asettaa systeemiparametrit seuraavasti:

1. Hän valitsee kaksi suurta salassa pidettävää alkulukua p ja q, ja laskee näiden avulla julkisen parametrin $n = pq$. Käytännössä alkulukujen p ja q tulee olla niin suuria, että luvun n tekijöihin jako on matemaattisesti vaikea tehtävä.

2. Hän valitsee turvallisuusparametriksi alkuluvun b, joka on samalla julkinen RSA-kryptauseksponentti. Alkuluvun b tulee olla ainakin 40 bittiä pitkä, jotta systeemin turvallisuuteen voidaan luottaa. Hän laskee alkuluvulle b käänteisluvun a modulo $\phi(n)$, joka on vastaavasti salainen RSA:n dekryptauseksponentti.

3. Hän valitsee vielä hash-funktion $h : \{0,1\}^* \longmapsto Z_n$.

4. Hän julkistaa parametrit (n, b, h).

5.2.2 Käyttäjän avaimen luominen

1. Trent varmistaa Alicen henkilöllisyyden ja tunnuksen ID_A autenttisuuden.

2. Hän laskee Alicen salaisen avaimen

$$u = \left(h\left(ID_A\right)^{-1}\right)^a \pmod{n}$$

ja luovuttaa sen Alicelle.

Nyt Alicella on valmius todentaa itsensä Bobille.

5.2.3 Identifiointi

1. Alice valitsee sellaisen satunaisen kokonaisluvun k, että $0 \leq k \leq n-1$, ja laskee

$$\gamma = k^b \pmod{n}.$$

2. Alice lähettää tunnuksensa ID_A ja luvun γ Bobille.

3. Bob laskee julkisen hash-funktion avulla arvon

$$v = h\left(ID_A\right).$$

4. Bob valitsee haasteeksi sellaisen satunnaisen kokonaisluvun r, että $0 \leq r \leq b-1$, ja lähettää sen Alicelle.

5. Alice laskee

$$y = ku^r \pmod{n}$$

ja lähettää luvun y Bobille.

6. Bob todentaa, että

$$\gamma \equiv v^r y^b \pmod{n}.$$

Selvitäkseen identifiointiprotokollasta Alicella tulee olla hallussaan arvo u, jonka ainoastaan Trent pystyy laskemaan. Jos rikollinen taho pystyisi murtamaan RSA-salauksen, niin se pystyisi myös laskemaan arvon u ja täten esiintymään Alicen identiteetillä. Jos Trent kuitenkin valitsee salaiset parametrit huolellisesti, voidaan olettaa, että RSA on turvallinen.

Lause 5.5. *GQ-protokolla on täydellinen.*

Todistus. Bob hyväksyy Alicen todistuksen hänen identiteetistään, koska

$$\begin{aligned} v^r y^b &\equiv h(ID_A)^r (ku^r)^b \pmod{n} \\ &\equiv h(ID_A)^r k^b (h(ID_A)^{-1})^{abr} \pmod{n} \\ &\equiv k^b \pmod{n} \\ &\equiv \gamma \pmod{n}. \end{aligned}$$

□

5.2.4 Esimerkkejä

Seuraavaksi esitetään kaksi numeerista esimerkkilaskua, jotka demonstroivat GQ-protokollan toimintaa.

Esimerkki 8. *Oletetaan, että Trent valitsee systeemiparametreiksi alkuluvut* $p = 61$ *ja* $q = 53$*, jolloin* $n = 61 \times 53 = 3233$ *ja* $\phi(n) = 3120$*. Trent valitsee julkiseksi kryptauseksponentiksi alkuluvun* $b = 17$*, ja ratkaisee kongruenssin*

$$ab \equiv 1 \pmod{\phi(n)},$$

josta saadaan luvun b *käänteisluku*

$$a = 2753 \pmod{3120}.$$

Alicen todistettua Trentille henkilöllisyytensä ja tunnuksensa autenttisuuden ID_A*, Trent laskee hash-arvon* v *Alicen tunnuksesta. Olkoon*

$$v = h(ID_A) = 2312 \pmod{3233},$$

jolloin

$$v^{-1} = h(ID_A)^{-1} = 681 \pmod{3233}.$$

Trent laskee salaisen kokonaisluvun

$$\begin{aligned} u &= \left(v^{-1}\right)^a \pmod{n} \\ &= 681^{2753} \pmod{3233} \\ &= 2494 \pmod{3233}, \end{aligned}$$

ja lähettää sen Alicelle.

Alicella on nyt valmius aloittaa identifiointiprotokolla ja hän haluaa todistaa identiteettinsä Bobille. Aluksi hän valitsee salaisesti kokonaisluvun $k = 1561$ *ja laskee sen avulla arvon*

$$\begin{aligned} \gamma &= k^b \pmod{n} \\ &= 1561^{17} \pmod{3233} \\ &= 473 \pmod{3233}, \end{aligned}$$

ja lähettää sen ja oman tunnuksensa ID_A *Bobille.*

Bob valitsee satunnaisesti arvon $r = 13$ *ja toimittaa sen haasteena Alicelle.*

Alice vastaa Bobin haasteeseen ja laskee arvon

$$\begin{aligned} y &= ku^r \pmod{n} \\ &= 1561 \cdot 2494^{13} \pmod{3233} \\ &= 1561 \cdot 189 \pmod{3233} \\ &= 826 \pmod{3233}, \end{aligned}$$

ja lähettää sen Bobille.

Bobin saatua arvon y *hän todentaa Alicen identiteetin laskemalla*

$$\begin{aligned} v^r y^b &= 2312^{13} \cdot 826^{17} \pmod{3233} \\ &= 2991 \cdot 145 \pmod{3233} \\ &= 473 \pmod{3233}. \end{aligned}$$

Esimerkissä 8 käytettävät luvut ovat todella pieniä ja käytännön tilanteissa GQ-systeemi tulisi toteuttaa paljon suuremmilla luvuilla. Seuraavassa esimerkissä laskutoimitukset vaativat laskijalta hieman enemmän aikaa ja vaivaa.

Esimerkki 9. *Aluksi Trent valitsee alkuluvut* $p = 503$ *ja* $q = 379$*, jolloin parametri* $n = 190637$ *ja* $\phi(n) = 189756$*. Julkiseksi kryptauseksponentiksi hän valitsee luvun* $b = 509$*, ja laskee sille salassa pidettävän käänteisluvun*

$$a = 46973 \pmod{189756}.$$

Seuraavaksi Trent laskee hash-arvon v *ja sen käänteisluvun* $v^{-1} \pmod{n}$ *Alicen tunnuksesta* ID_A*. Olkoon* $v = h(ID_A) = 155863$*, jolloin sen käänteisluku* $v^{-1} = 3536 \pmod{190637}$*. Nyt Trent voi laskea Alicen salaisen avaimen*

$$\begin{aligned} u &= \left(v^{-1}\right)^a \pmod{n} \\ &= 3536^{46973} \pmod{190637} \\ &= 152496 \pmod{190637}, \end{aligned}$$

jonka hän luovuttaa Alicelle henkilöllisyyden ja tunnuksen autenttisuuden varmentamisen jälkeen.

Alicen halutessa todistaa identiteettinsä Bobille hän valitsee ensin kokonaisluvun $k = 123845$*, jonka jälkeen hän laskee luvun*

$$\begin{aligned} \gamma &= k^b \pmod{n} \\ &= 123845^{509} \pmod{190637} \\ &= 162227 \pmod{190637}, \end{aligned}$$

ja lähettää sen ja tunnuksen ID_A *Bobille.*

Bob lähettää Alicelle haasteen $r = 487$*, johon Alice vastaa laskemalla luvun*

$$\begin{aligned} y &= ku^r \pmod{n} \\ &= 123845 \cdot 152496^{487} \pmod{190637} \\ &= 123845 \cdot 189619 \pmod{190637} \\ &= 127484 \pmod{190637}, \end{aligned}$$

ja lähettämällä sen Bobille.

Bob todentaa, että Alice on kuka hän väittää olevansa laskemalla

$$\begin{aligned} v^r y^b &= 155863^{487} \cdot 127484^{509} \pmod{190637} \\ &= 179405 \cdot 62428 \pmod{190637} \\ &= 127484 \pmod{190637} \\ &= \gamma \pmod{n}. \end{aligned}$$

5.3 Parikuvauksista

Tutkielman kolmeen viimeiseen kryptosysteemiin liittyvät olennaisena osana *parikuvaukset*, joiden ominaisuuksiin perehdytään nyt hieman tarkemmin. Elliptisiä käyriä käyttäen voidaan nimittäin määritellä kaksi bilineaarista kuvausta: Weil-parikuvaus ja Tate-parikuvaus. Teoria näiden kuvausten takana on kuitenkin todella monimutkaista, joten se sivuutetaan. Jatkossa tyydymme ainoastaan olettamaan, että on olemassa parikuvauksia, joilla on tietyt ominaisuudet. Seuraavaksi esitetään joitakin määritelmiä ja lauseita parikuvauksiin liittyen. Tämä alaosio perustuu kirjaan [5].

5.3.1 Perusteet

Olkoon G_1, G_2, G_T kertalukua p olevia ryhmiä. Olkoon p alkuluku, minkä vuoksi ryhmät ovat syklisiä.

Määritelmä 5.6. *Parikuvaus* on tehokkaasti laskettava kuvaus $e : G_1 \times G_2 \to G_T$, joka toteuttaa seuraavat ehdot:

1. Bilineaarisuus: $e(A_1 + B_1, A_2) = e(A_1, A_2)\, e(B_1, A_2)$ kaikille $A_1, B_1 \in G_1$ ja kaikille $A_2 \in G_2$.
   Vastaavasti $e(A_1, A_2 + B_2) = e(A_1, A_2)\, e(A_1, B_2)$ kaikille $A_1 \in G_1$ ja kaikille $A_2, B_2 \in G_2$.

2. Epä-degeneroituvuus: On olemassa sellainen $(A_1, A_2) \in G_1 \times G_2$, että $e(A_1, A_2) \neq 1$.

Ryhmät G_1 ja G_2 ovat additiivisia ja G_T on multiplikatiivinen. Merkitään luvulla $a = \log_g A$ diskreettiä g-kantaista logaritmia luvusta A, eli sellaista

kokonaislukua a, että $ag = A$. Olkoon G^* joukko epäidenttisiä ryhmän G alkioita, jotka muodostavat tässä generaattoreiden joukon ryhmän G kertaluvun ollessa alkuluku. On mahdollista, että $G_1 = G_2$, jolloin on kysessä symmetrinen tapaus. Epäsymmetrinen tapaus, jossa $G_1 \neq G_2$, on yleisempi.

On mahdollista rakentaa isomorfismi $\psi : G_2 \to G_1$. Symmetrisessä tapauksessa tämä on identiteettikuvaus. Jos g_2 on ryhmän G_2 generaattori, niin $\psi(g_2)$ on ryhmän G_1 generaattori.

Seuraava tulos on parikuvausten keskeinen algebrallinen ominaisuus, josta on peräisin suuri osa niiden tehosta.

Lause 5.7. *$e(a_1A_1, a_2A_2) = e(A_1, A_2)^{a_1a_2}$ kaikille $(A_1, A_2) \in G_1 \times G_2$ ja kaikille $a_1, a_2 \in Z$.*

Todistus. Lause seuraa parikuvauksen bilineaarisuusominaisuudesta;

$$\begin{aligned} e(a_1A_1, a_2A_2) &= e(\underbrace{A_1 + \cdots + A_1}_{a_1}, a_2A_2) = e(A_1, a_2A_2)^{a_1} \\ &= e(A_1, \underbrace{A_2 + \cdots + A_2}_{a_2})^{a_1} = e(A_1, A_2)^{a_1a_2}. \end{aligned}$$

□

Lause 5.8. *Samaan kertalukua p olevaan ryhmään G_1 kuuluvien alkioiden P ja G parikuvaukset $e(P, G)$ ja $e(G, P)$ ovat yhtä suuret alkion P ollessa ryhmän G_1 generaattori.*

Todistus.

$$e(P, G) = e(P, nP) = e(P, P)^n = e(nP, P) = e(G, P).$$

□

Lause 5.9. *Jos g_1 on ryhmän G_1 generaattori ja g_2 on ryhmän G_2 generaattori, niin alkio $e(g_1, g_2)$ on ryhmän G_T generaattori.*

Todistus. Koska ryhmän G_T kertaluku p on alkuluku, riittää todistaa pelkästään, että parikuvaus $e(g_1, g_2) \neq 1$. Tehdään vastaoletus, että $e(g_1, g_2) = 1$. Lauseen 5.7 mukaan kaikille $(A_1, A_2) \in G_1 \times G_2$ parikuvaus $e(A_1, A_2) = e(a_1g_1, a_2g_2) = e(g_1, g_2)^{a_1a_2} = 1^{a_1a_2} = 1$, missä $a_i = \log_{g_1} A_i$, kun $i = 1, 2$. Tämä on ristiriidassa parikuvauksen epä-degeneroituvuuden kanssa. □

Merkitään, että (g_2, xg_2, h, W) on *dh-tupla*, jos $W = xh$, missä $g_2 \in G_2^*$, $x \in Z$ ja $h, W \in G_1$. Seuraavan lauseen mukaan tällaiset tuplat voidaan tunnistaa helposti käyttäen parikuvausta.

Lause 5.10. *On olemassa sellainen tehokas funktio V, että kaikilla arvoilla $g_2 \in G_2^*$, kaikilla $h, W \in G_1$ ja kaikille $x \in Z$ funktion $V(g_2, xg_2, h, W)$ arvo on 1, jos $W = xh$. Muissa tapauksissa funktion arvo on 0.*

Todistus. Oletetaan, että g_1 on ryhmän G_1 generaattori. Olkoon $w = \log_{g_1} W$, $\alpha = \log_{g_1} h$ ja $g_T = e(g_1, g_2)$. Oletuksista ja lauseesta 5.7 seuraa, että

$$\begin{aligned} e(W, g_2) &= e(wg_1, g_2) = e(g_1, g_2)^w = g_T^w, \\ e(h, xg_2) &= e(\alpha g_1, xg_2) = e(g_1, g_2)^{\alpha x} = g_T^{\alpha x}. \end{aligned}$$

Lauseen 5.9 mukaan g_T on ryhmän G_T generaattori. Tästä seuraa, että

$$g_T^w = g_T^{\alpha x} \Leftrightarrow w \equiv \alpha x \pmod{p} \Leftrightarrow W = xh.$$

Funktion V arvoksi valitaan 1, jos $e(W, g_2) = e(h, xg_2)$ ja 0 muuten. □

Käyttämällä edellisen lauseen funktiota V voidaan siis saada selville, että onko kyseinen (g_2, xg_2, h, W) dh-tupla.

Määritelmä 5.11. *Diffien ja Hellmanin päätösongelma* (DDH-ongelma) ryhmässä $G_1 (= G_2)$ on erottaa toisistaan distribuutiot (P, aP, bP, abP) ja (P, aP, bP, cP), missä a, b, c ovat satunnaisia alkioita joukossa Z_p^* ja P on satunnainen ryhmän G_1^* alkio.

Lauseen 5.10 avulla DDH-ongelma on helppo ratkaista.

Määritelmä 5.12. Olkoon G_1, G_T kaksi, kertalukua p olevaa ryhmää, kun p on alkuluku. Olkoon $e : G_1 \times G_1 \to G_T$ parikuvaus ja alkio P ryhmän G_1 generaattori. *Bilineaarinen Diffien ja Hellmanin ongelma* (BDH-ongelma) on seuraava: täytyy laskea arvo $W = e(P, P)^{abc} \in G_T$, kun on annettu P, aP, bP, cP joillakin arvoilla $a, b, c \in Z$.

BDH-ongelma on vaikea, mutta ei yhtä vaikea kuin tavallinen Diffien ja Hellmanin ongelma (DH-ongelma), jossa täytyy laskea abP annetuista

luvuista P, aP ja bP. Jos DH-ongelman voidaan ratkaista, parikuvauksen $e\left(abP, cP\right) = e\left(P, P\right)^{abc}$ laskeminen annetuista $P, aP, bP, cP \in G_1^*$ on myös mahdollista. BDH-ongelmaa pidetään kuitenkin tarpeeksi vaikeana ongelmana käytettäväksi kryptosysteemeissä.

5.4 Identiteettiin perustuva epäinteraktiivinen Sakain, Ohgishin ja Kasaharan avaimenvaihtosysteemi

Shakain, Ohgishin ja Kasaharan avaimenvaihtosysteemi (merkitään jatkossa SOK-systeemi) vaatii asiakkaiden lisäksi myös kolmannen osapuolen, luotettavan Trentin, osallistumista. Hän toimii järjestäjänä systeemissä luoden avainpalvelun, joka tarjoaa asiakkaalle salaisen avaimen henkilöllisyystodistusta vastaan. SOK-systeemissä on kaikkiaan kolme osaa.

5.4.1 Systeemiparametrien luominen

Trent asettaa systeemiparametrit seuraavaasti:

1. Trent luo kaksi ryhmää $(G_1, +)$, $(G_T, \cdot)$, joiden kertaluku on alkuluku p. Lisäksi hän valitsee parikuvauksen $e : (G_1, +)^2 \mapsto (G_T, \cdot)$ ja satunnaisen generaattorin $P \in G_1$.

2. Hän valitsee salaisen avaimen $l \in Z_p$ ja asettaa sen avulla parametrin $P_{pub} \leftarrow lP$.

3. Hän valitsee kryptografisesti vahvan hash-funktion $f : \{0,1\}^* \mapsto G_1$, joka kuvaa asiakkaan identiteettiin yhdistettävän tunnuksen ID ryhmän G_1 alkioksi.

Trent julkaisee systeemiparametrit

$$\left(G_1, G_T, e, P, P_{pub}, f\right),$$

ja pitää luvun l itsellään systeemin salaisena avaimena. Trentiä pidetään tunnettuna osapuolena järjestelmässä, joten myös hänen julkaisemia systeemiparametrejä voidaan pitää tunnettuina järjestelmässä. Systeemin salaisen avaimen l salassa pysyminen turvaa diskreetin logaritmin laskemisen vaikeuteen ryhmässä G_1. Seuraavaksi Trent voi aukaista avainpalvelun asiakkaille.

5.4.2 Käyttäjän avaimen luominen

Olkoon merkkijono ID_A Alicen identiteettiin liitettävä tunnus. Oletetaan, että ID_A sisältää riittävästi redundanssia, ettei kenelläkään toisella asiakkaalla voi olla tunnuksenaan samaa merkkijonoa ID_A. Trentin tunnistettua Alicen ja tarkistettua tunnuksen ID_A ainutlaatuisuuden, hän voi aloittaa avaimen luomisen:

1. Trent laskee Alicen tunnukseen ID_A perustuvan julkisen avaimen $P_{ID_A} \leftarrow f(ID_A)$, joka on rymän G_1 alkio.

2. Hän laskee Alicen salaisen avaimen $S_{ID_A} \leftarrow lP_{ID_A}$.

Hash-funktion arvon P_{ID_A} pitää näyttää satunnaiselta. Tunnuksen ID_A sisältäessä kuitenkin riittävän määrän tunnistettavaa informaatiota, hash-funktion arvo $f(ID_A) = P_{ID_A}$ säilyy myös tunnistettavana. Tällöin Alicen julkisena avaimena voidaan pitää joko bittijonoa ID_A tai parametria P_{ID_A}, koska molemmat voidaan liittää yksikäsitteisesti asiakkaaseen Alice.

Näytetään seuraavaksi, että Alicen salaisen avaimen turvallisuus nojaa DH-ongelman vaikeuteen ryhmässä G_1. Parametri $P_{ID_A} \in G_1$, joten P generoi sen. Merkitään $P_{ID_A} = aP$, jossa luku $a < p$. Alicen salaisen avaimen

$$S_{ID_A} = lP_{ID_A} = laP$$

selvittäminen julkisten parametrien $P, P_{pub} = lP, P_{ID_A} = aP$ perusteella on DH-ongelma ryhmässä G_1.

5.4.3 Avaimen vaihto

Alicen ja Bobin tunnukset ID_A ja ID_B ovat julkista tietoa, joten he tietävät toistensa julkiset avaimet $P_{ID_A} = f(ID_A)$ ja $P_{ID_B} = f(ID_B)$. Seuraavaksi Alice generoi avaimen $K_{AB} \in (G_T, \cdot)$ laskemalla

$$K_{AB} \leftarrow e(S_{ID_A}, P_{ID_B}).$$

Bob generoi vastaavasti avaimen $K_{BA} \in (G_T, \cdot)$ laskemalla

$$K_{BA} \leftarrow e(S_{ID_B}, P_{ID_A}).$$

Todistetaan vielä, että SOK-systeemi todella toimii.

Lause 5.13. *SOK-systeemin asiakkaiden generoimat avaimet K_{AB} ja K_{BA} ovat samat.*

Todistus. Parikuvauksen bilineaarisuudesta seuraa, että

$$K_{AB} = e\left(S_{ID_A}, P_{ID_B}\right) = e\left(lP_{ID_A}, P_{ID_B}\right) = e\left(P_{ID_A}, P_{ID_B}\right)^l.$$

Vastaavasti

$$K_{BA} = e\left(P_{ID_B}, P_{ID_A}\right)^l.$$

Lauseen 5.8 mukaan

$$K_{AB} = K_{BA}.$$

□

Alice ja Bob voivat täten jakaa salaisuuden ilman interaktiivista kanssakäymistä toistensa kanssa. Selvittääkseen salaisen avaimen K_{AB} julkisista tiedoista $(P, P_{ID_A}, P_{ID_B}, P_{pub})$ vihollisen täytyisi pystyä ratkaisemaan BDH-ongelma, joka tiedetään matemaattisesti vaikeaksi ongelmaksi. Alice ja Bob voivat nyt turvallisesti lähettää toisilleen salattuja viestejä käyttäen jotain symmetristä kryptosysteemiä, jonka avaimena on K_{AB}.

Bobin saadessa salaisella avaimella K_{AB} kryptatun viestin hän voi olla varma, että Alice on luonut viestin, koska hän itse ei ole luonut sitä. Alice voi kuitenkin kieltää kolmannelle osapuolelle osallisuutensa viestiin, koska Bobilla on samat valmiudet konstruoida salattu viesti. Oletetaan, että Alice ja Bob ovat vakoojia. Ollakseen yhteydessä heidän täytyy varmentaa itsensä toisilleen. Kaksoisagenttina Alice epäilee Bobinkin olevan kaksoisagentti. Vakoojien varmennusjärjestelmällä on oltava sellainen ominaisuus, että varmennus on pystyttävä kiistää. SOK-systeemi on juuri tällainen, koska varmennukseen ei tarvita kolmatta luotettavaa osapuolta.

5.5 Identiteettiin perustuva Bonehin ja Franklinin kryptosysteemi

Kahden osapuolen välille voidaan luoda jaettu avain käyttäen heidän identiteettejään, mikä mahdollistaa myös identiteettiin perustuvan kryptauksen.

Boneh ja Franklin käyttivät parikuvausmenetelmää, ja saivat aikaan ensimmäisen käytännöllisen identiteettiin perustuvan julkisen avaimen kryptosysteemin.

Bonehin ja Franklinin identiteettiin perustuva kryptosysteemi (merkitään jatkossa BF-systeemi) koostuu neljästä algoritmista.

- **Systeemiparametrien luominen** Trent (luotettava osapuoli) luo julkiset systeemiparametrit ja oman salaisen avaimen.
- **Käyttäjän avaimen luominen** Trent luo Alicelle salaisen avaimen, joka riippuu Alicen identiteetin yksikäsitteisesti yksilöivästä tunnuksesta $ID \in \{0,1\}^*$.
- **Viestin salaus** Tämä probabilistinen algoritmi salaa viestin käyttäjän julkisen avaimen, eli hänen tunnuksensa ID, avulla.
- **Salauksen purku** Salattu viesti puretaan käyttäjän salaisella avaimella selvätekstiksi.

Oletetaan, että Bob haluaa lähettää Alicelle salaisen viestin. He tarvitsevat kolmanneksi osapuoleksi jonkun luotettavan tahon, olkoon hän Trent.

5.5.1 Systeemiparametrien luominen

1. Trent valitsee satunnaisen alkuluvun p. Hän generoi kaksi astetta p olevaa ryhmää $(G_1, +)$, $(G_T, \cdot)$, joille on olemassa parikuvaus $e : (G_1, +)^2 \mapsto (G_T, \cdot)$. Hän valitsee satunnaisesti generaattorin $P \in G_1$.
2. Trent valitsee salaisen avaimen $s \in Z_p$ ja laskee julkisen parametrin $P_{pub} \leftarrow sP$.
3. Trent valitsee hash-funktion $F : \{0,1\}^* \mapsto G_1$, joka kuvaa käyttäjän tunnuksen ID ryhmän G_1 alkioksi.
4. Trent valitsee hash-funktion $H : G_T \mapsto \{0,1\}^n$, jossa luku n on samaa suuruusluokkaa alkuluvun p pituuden kanssa. Hash-funktio H määrittää selvätekstiavaruudeksi $\{0,1\}^n$.

Trent julkaisee systeemiparametrit

$$(G_1, G_T, e, n, P, P_{pub}, F, H),$$

ja parametrin s hän pitää systeemin salaisena avaimena.

5.5.2 Käyttäjän avaimen luominen

Olkoon ID Alicen identiteettiin yksikäsitteisesti liitettävä tunnus, jonka hän käy esittämässä Trentille henkilökohtaisesti. Trent varmistaa, että ID on todellakin ainutlaatuinen, jonka jälkeen hän toimii seuraavasti:

1. Trent laskee Alicen tunnukseen ID perustuvan julkisen avaimen $Q_{ID} \leftarrow F(ID)$, joka on ryhmän G_1 alkio.

2. Trent laskee oman salaisen avaimen s avulla Alicen salaisen avaimen $d_{ID} \leftarrow sQ_{ID}$.

5.5.3 Viestin salaus

Lähettääkseen luottamuksellisia viestejä Alicelle, Bobin täytyy ensin saada systeemiparametrit $(G_1, G_T, e, n, P, P_{pub}, F, H)$. Bob laskee näiden parametrien avulla

$$Q_{ID} = F(ID).$$

Olkoon viesti jaettu lohkoihin, joiden pituudet ovat n bittiä. Salatessa lohkoa $M \in \{0,1\}^n$, Bob valitsee parametrin $r \in Z_p$ ja laskee

$$\begin{aligned} g_{ID} &\leftarrow e(Q_{ID}, rP_{pub}) \in G_T, \\ C &\leftarrow (rP, M \oplus H(g_{ID})). \end{aligned} \tag{2}$$

Salattu viesti eli kryptoteksti on $C = (rP, M \oplus H(g_{ID}))$. Merkintä $\oplus$ tarkoittaa XOR-operaatiota, jossa kaksi saman mittaista binääristä bittijonoa lasketaan yhteen biteittäin modulo 2.

5.5.4 Salauksen purku

Olkoon $C = (U, V)$ kryptoteksti, joka on salattu käyttäen Alicen julkista avainta ID. Purkaakseen salauksen kryptotekstistä C salaisella avaimellaan $d_{ID} \in G_1$, Alice laskee

$$V \oplus H\left(e\left(d_{ID}, U\right)\right). \tag{3}$$

Näytetään seuraavaksi, että BF-systeemi on toimiva kryptosysteemi.

Lause 5.14. *Salausta purettaessa laskettu $V \oplus H\left(e\left(d_{ID}, U\right)\right) = M$, joka on alkuperäinen salaamaton viesti.*

Todistus. Aloitetaan parikuvauksesta

$$e\left(d_{ID}, U\right) = e\left(sQ_{ID}, rP\right) = e\left(Q_{ID}, rP\right)^s = e\left(Q_{ID}, rP_{pub}\right) = g_{ID}.$$

Tällöin parikuvauksen arvo, jonka Alice sijoittaa kaavaan (3) purkaessaan salausta, on g_{ID}. Tämä on sama arvo, jonka Bob on sijoittanut kaavaan (2) salatessaan viestiä. Voidaan todeta, että

$$V \oplus H\left(e\left(d_{ID}, U\right)\right) = M \oplus H\left(g_{ID}\right) \oplus H\left(g_{ID}\right) = M,$$

koska kahdelle samanlaiselle binääriselle bittijonolle suoritettava XOR-operaatio tuottaa bittijonon, jonka kaikki bitit ovat nollia modulo 2. □

5.6 Bonehin ja Franklinin systeemin laajennus

Huomion arvoista Bonehin ja Franklinin kryptosysteemissä on se, että Trentillä on mahdollisuus purkaa jokainen systeemissä lähetetty salattu viesti. Siksi osion 5.5 mukainen kryptosysteemi ei sellaisenaan sovellu käytettäväksi avoimissa ympäristöissä. Seuraavaksi esitetään BF-systeemin laajennus, joka on yksinkertainen variaatio alkuperäisestä versiosta.

Laajennus pohjautuu ideaan käyttää useampia luotettavia osapuolia. Tällöin kukaan heistä ei pysty yksin selvittämään selvätekstiä, vaan siihen vaadittaisiin heidän kaikkien yhteistyötä. Nyt esitettävässä systeemissä luotettavia osapuolia on kaksi (merkitään heitä TA_1 ja TA_2), mutta siihen verrattuna useamman luotettavan osapuolen käyttö on lähes yhtä helppoa.

5.6.1 Systeemiparametrien luominen

Olkoon parametrit $(G_1, G_T, e, n, P, F, H)$ samat kuin osiossa 5.5. Luotettavat osapuolet TA_1 ja TA_2 laskevat kumpikin oman osansa Alicen julkisesta avaimesta, jolloin

$$\begin{aligned} P_1 &\leftarrow s_1 P \\ P_2 &\leftarrow s_2 P. \end{aligned}$$

Systeemin julkiset parametrit ovat täten $(G_1, G_T, e, n, P, P_1, P_2, F, H)$. Parametrit s_1 ja s_2 ovat osapuolien TA_1 ja TA_2 salaiset avaimet.

5.6.2 Käyttäjän avaimen luominen

Olkoon ID Alicen identiteettiin liittyvä tunnus. Luotettavat osapuolet TA_1 ja TA_2 suorittavat seuraavat operaatiot:

1. Lasketaan Alicen tunnukseen ID perustuva julkinen avain $Q_{ID} \leftarrow F(ID)$, joka on ryhmän G_1 alkio.

2. Luodaan Alicen salainen avain laskemalla $d_{ID}^i \leftarrow s_i Q_{ID}$. Koska luotettavia osapuolia on kaksi, indeksi i saa arvot 1 ja 2.

Alicen salainen avain on summa

$$d_{ID} \leftarrow d_{ID}^1 + d_{ID}^2.$$

Tämä avain pysyy salassa, jos TA_1 ja TA_2 eivät liittoudu.

5.6.3 Viestin salaus

Lähettääkseen luottamuksellisia viestejä Alicelle, Bobin täytyy ensin hankkia julkiset systeemiparametrit $(G_1, G_T, e, n, P, P_1, P_2, F, H)$. Bob laskee näiden parametrien avulla

$$Q_{ID} = F(ID).$$

Olkoon viesti jaettu lohkoihin, joiden pituudet ovat n bittiä. Salatessa lohkoa $M \in \{0,1\}^n$, Bob valitsee parametrin $r \in Z_p$ ja laskee

$$\begin{aligned} g_{ID} &\leftarrow e\left(Q_{ID}, r\left(P_1 + P_2\right)\right), \\ C &\leftarrow \left(rP, M \oplus H\left(g_{ID}\right)\right). \end{aligned}$$

Kryptoteksti C on pari, jonka muodostavat piste ryhmästä G_1 ja avaruuden $\{0,1\}^n$ alkio. Kryptotekstiavaruus on $G_1 \times \{0,1\}^n$.

5.6.4 Salauksen purku

Olkoon $C = (U, V)$ kryptoteksti, joka on salattu käyttäen Alicen julkista avainta ID. Purkaakseen salauksen kryptotekstistä C salaisella avaimellaan $d_{ID} \in G_1$, Alice laskee

$$V \oplus H\left(e\left(d_{ID}, U\right)\right).$$

Todistetaan seuraavaksi, että BF-systeemin laajennus toimii.

Lause 5.15. *Salausta purettaessa laskettu $V \oplus H\left(e\left(d_{id}, U\right)\right) = M$, joka on alkuperäinen selväteksti.*

Todistus. Todetaan, että parikuvaus

$$\begin{aligned} e\left(d_{ID}, U\right) &= e\left(s_1 Q_{ID} + s_2 Q_{ID}, rP\right) \\ &= e\left(s_1 Q_{ID}, rP\right) e\left(s_2 Q_{ID}, rP\right) \\ &= e\left(Q_{ID}, rs_1 P\right) e\left(Q_{ID}, rs_2 P\right) \\ &= e\left(Q_{ID}, r\left(P_1 + P_2\right)\right) \\ &= g_{ID}. \end{aligned}$$

Joten Alicen laskiessa

$$V \oplus H\left(e\left(d_{ID}, U\right)\right) = M \oplus H\left(g_{ID}\right) \oplus H\left(g_{ID}\right) = M$$

hän tulee purkaneeksi salauksen. □

5.6.5 Turvallisuudesta

Yhden luotettavan osapuolen TA käyttöön verrattuna salauksen ja salauksen purkamiseen liittyvät laskut kaksinkertaistuvat, mutta Alicen identiteettiin liittyvän tunnuksen ID ja salatun viestin koko säilyy tässä laajennetussa versiossa ennallaan.

Luotettavat osapuolet voivat purkaa salauksen yhdessä, mutta itsenäisesti he eivät tähän pysty. Joten mitä enemmän luotettavia osapuolia käytetään,

sitä turvallisemmaksi systeemi tulee. Luotettavien osapuolten määrä ei vaikuta Alicen tunnukseen ID eikä salatun viestin kokoon, mutta salauksessa ja salauksen purkamissa tarvittavien laskujen määrät kasvavat lineaarisesti suhteessa luotettavien osapuolten määrään.

Käytettäessä useita luotettavia osapuolia salauksen murtaminen vaatisi näiden kaikkien yhteistyötä. Jos pystytään luottamaan täydellisesti ainakin yhteen osapuolista TA_i, niin vakoilu tulee estetyksi, ja laajennettua versiota Bonehin ja Franklinin systeemistä voidaan käyttää avoimissa ympäristöissä.

5.7 Autentikointi ilman avaimenvaihtokanavaa

Lähettääkseen Alicelle luottamuksellisen viestin käyttäen jotain tavanomaista kryptosysteemiä Bobin täytyy aluksi luoda avaimenvaihtokanava heidän välilleen. Kanava voi olla tiedostopohjainen, jolloin se perustuu lähettäjän tekemään varmennukseen vastaanottajan julkisen avaimen sertifikaatista. Lähettäjän täytyy ensin pyytää vastaanottajalta hänen julkisen avaimen sertifikaattinsa. Avoimissa järjestelmissä, joissa osapuolet eivät pysty muistamaan mikä avain kuuluu kenellekin asiakkaalle, lähettäjän ja vastaanottajan on välttämättä oltava yhteydessä luodakseen avaimenvaihtokanavan ennen salattujen viestien lähetystä.

Identiteettiin perustuvassa julkisen avaimen kryptosysteemissä ei ole pelkästään tarpeetonta, vaan myös mahdotonta luoda avaimenvaihtokanava. Vaikka Bob pyytäisikin Alicelta tämän identiteettiin perustuvaa julkista avainta, Bobin on mahdotonta varmistaa, että avain todella on Alicen. Lähettääkseen luottamuksellisen viestin Alicelle Bobin täytyy vaan salata viesti Alicen julkisella avaimella ja toivoa, että avain on aito. Jos Alice pystyy purkamaan Bobin lähettämän viestin, niin Alicen ID todellakin on hänen julkinen avaimensa. Niin pitkään kuin luotettava taho varmentaa kaikkien asiakkaiden tunnuksien yksikäsitteisyyden, lähettäjän ei tarvitse olla yhteydessä vastaanottajan ennen salatun viestin lähetystä. Tämän takia identiteettiin perustuvaa julkisen avaimen kryptosysteemiä kutsutaan myös epäinteraktiiviseksi julkisen avaimen kryptosysteemiksi. Epäinteraktiivisuus on kaikista selvin SOK-systeemissä. Siinä Alicen ja Bobin rekisteröityä identiteetteihin-

sä perustuvat julkiset avaimet jakavat he jo turvallisen avainkanavan, jonka perustana ovat heidän salaiset avaimensa. Alicen ja Bobin ei tarvitse käyttää muuta protokollaa, koska yhteinen turvallinen yhteys on jo saavutettu.

6 Identiteettiin perustuvan kryptografian sovelluksia

Lopuksi esitetään muutamia sovelluksia, jotka ovat käyttökelpoisia erityisesti käytettäessä Bonehin ja Franklinin kryptosysteemiä. Sovellukset ovat peräisin artikkelista [4].

6.1 Julkisen avaimen kumoaminen

Julkisen avaimen sertifikaatit voidaan asettaa olemaan voimassa vain tietyn ajan. Identiteettiin perustuvan kryptosysteemin avaimeen lisätään erääntymispäivä (, jota merkitään jatkossa *date*), jolloin viestiä kryptattaessa käytetty vastaanottajan julkinen avain on muotoa $ID \,||\, date$. Tämän seurauksena vastaanottajan täytyy uusia salainen avain sen jälkeen, kun entinen avain on vanhentunut.

Oletetaan, että Alice ja Bob ovat töissä samassa yrityksessä. Heidän käytössään on identiteettiin perustuva julkisen avaimen kryptosysteemi, jossa Bobin julkinen avain on voimassa yhden päivän ajan kerrallaan. Jotta Bob voisi lukea Alicelta tulleita kryptattuja sähköposteja, hänen täytyy pyytää päivittäin yrityksen ylläpitämältä avainpalvelulta uusi salainen avain. Alicen ei kuitenkaan tarvitse olla yhteydessä kolmanteen osapuoleen saadakseen Bobin päivättäisen julkisen avaimen, vaan hän pystyy määrittämään sen itse, mikä helpottaa Alicen työskentelyä. Tämänkaltaisessa tilanteessa julkisen avaimen kumoaminen on helppoa. Bobin jäädessä pois yrityksen palveluksesta avainpalvelu lakkaa toimittamasta Bobille päivittäisiä salaisia avaimia, jolloin hän ei enää pysty avaamaan kryptattuja viestejä. Tällöin Alicen on mahdollista lähettää salattuja viestejä, jotka Bob saa luettua vasta tulevaisuudessa Alicen määrittämänä päivänä.

Edellä olleen tilanteen yksinkertainen laajennus on nimeltään *käyttäjän valtuuksien hallinta*. Alicen salatessa sähköpostin käyttäen Bobin julkisena avaimena bittijonoa $ID \,||\, date \,||\, secret$. Tällöin Bob pystyy lukemaan viestin, jos hänellä on avainpalvelun suomat valtuudet siihen. Avainpalvelun avulla pystytään täten helposti myöntämään ja kumoamaan valtuuksia.

6.2 Dekryptausavainten jakaminen

Eräs identiteettiin perustuvan kryptografian sovellus on dekryptauskyvyn jakaminen. Seuraavaksi esitettävissä esimerkeissä viestin vastaanottaja Bob on myös avainpalvelun ylläpitäjä. Hän luo järjestelmäparametrit ja oman salaisen yleisavaimen, jonka jälkeen hän hankkii julkisen avaimelleen sertifikaatin ylemmältä, luotetulta taholta. Täten Bob on ainoa, joka tietää salaisen yleisavaimen.

1. **Jakaminen kannettavalle tietokoneelle.** Oletetaan, että Alice kryptaa viestinsä käyttäen identiteetiin perustuvaa kryptosysteemiä ja Bobin päivättyä julkista avainta $ID \,||\, date$. Bobilla on halussaan salainen yleisavain, jonka avulla hän voi luoda itselleen dekryptaukseen tarvittavan salaisen avaimen. Bobin lähtiessä seitsemän päivän matkalle hän normaalisti asentaisi kannettavalle tietokoneelle salaisen avaimensa, jonka turvallisuus vaarantuisi, jos tietokone varastettaisiin. Käytössä oleva identiteettiin perustuva julkisen avaimen kryptosysteemi kuitenkin mahdollistaa sen, että Bob asentaa tietokoneelleen ainoastaan seitsemän salaista avainta, yhden jokaista matkan päivää kohden. Tietokoneen hävitessä ainoastaan nämä salasanat joutuvat vääriin käsiin, mutta systeemin yleisavain säilyy salaisena.

2. **Tehtävien jakaminen.** Oletetaan, että Alice kryptaa viestin Bobille käyttäen identiteettiin perustuvaa kryptosysteemiä, jossa julkiseen avaimeen on liitetty viestin aihealue. Tällöin julkinen avain on muotoa $ID \,||\, subject$ Bob pystyy purkamaan viestin käyttäen yleisavaintaan. Oletetaan myös, että Bobilla on muutama avustaja, joilla kaikilla on vastuullaan omat aihealueensa. Bob antaa jokaiselle avustajalleen yhden salaisen avaimen, joka riippuu kyseisen avustajan vastuualueesta. Nyt avustajat pystyvät lukemaan ainoastaan omaa vastuualuetta koskevat viestit.

Yleisesti identiteettiin perustuvan kryptografian avulla pystytään yksinkertaistamaan järjestelmiä, jotka sisältävät monia julkisia avaimia. Julkisten avainten varastoiminen suureen hakemistoon ja sen ylläpitäminen voidaan

korvata johtamalla ne suoraan käyttäjänimestä.

Kirjallisuutta

[1] Bruce Schneier: *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley and Sons, Inc., 1994.

[2] Douglas R. Stinson: *Cryptography - Theory and Practice*. CRC Press, 1995.

[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: *Handbook of Applied Cryptography*. CRC Press, 1997.

[4] Dan Boneh, Matthew K. Franklin: *Identity-Based Encryption from the Weil Pairing*. Proceedings of CRYPTO 2001, 2001.

[5] Ari Renvall, Tommi Meskanen: *Kryptografia II*. Matematiikan laitos, Turun Yliopisto, 2008.

[6] Wenbo Mao: *Modern Cryptography: Theory and Practice*. Pearson Education, 2003.