Adi Syväntö

NOLLATIETOTODISTUKSET KÄYTTÄJÄTIETOJEN TODENTAMISESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Syväntö, Adi
Nollatietotodistukset käyttäjätietojen todentamisessa
Jyväskylä: Jyväskylän yliopisto, 2023, 28 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Marttiin, Pentti

Nollatietotodistusten hyödyntäminen käyttäjätietojen todentamisessa on kehittyvän digitalisaation, ja tietoturvauhkien vuoksi saanut kasvavassa määrin huomiota potentiaalisena ratkaisuna perinteisen salasanaan perustuvan todentamismenetelmän riskeihin ja haavoittuvuuksiin. Perinteinen salasanaan perustuva todentamismenetelmä on altis vahinkoa aiheuttaville hyökkäyksille muiden tietoturvahaasteiden lisäksi. Nollatietotodistukset sen sijaan mahdollistavat identiteetin todistamisen ilman tarvetta sensitiivisen informaation säilyttämiseen ja lähettämiseen verkon välityksellä. Kirjallisuuskatsauksen tavoitteena oli selvittää, kuinka nollatietotodistuksia hyödynnetään verkkoympäristössä tapahtuvassa käyttäjätietojen todentamisessa, sekä kahden implementaatioesimerkin avulla tunnistaa nollatietotodistusten tarjoamia hyötyjä ja potentiaalisia haittoja. SRP-protokollassa nollatietoisuus saavutetaan käyttäjän salasanasta generoidun – palvelimen kanssa jaetun arvon avulla, joka ei itsessään vaaranna käyttäjän sensitiivistä informaatiota. M-Pin on puolestaan useaan tekijään pohjautuva todentamismenetelmä, jossa hyödynnetään niin sanotun luotetun osapuolen olemassaoloa. Luotettu osapuoli vastaa käyttäjän identiteettisidonnaisen salaisuuden myöntämisestä, josta käyttäjän valitseman PIN-koodin lisäksi generoidaan varmiste, jota käytetään käyttäjän todentamiseen palvelimelle. Nollatietotodistuksia hyödyntävät käyttäjän todentamisen menetelmät osoittautuivat hyvin vastustuskykyisiksi haavoittuvuuksia, kuten väliintulo- ja sanakirjahyökkäyksiä vastaan. Menetelmät koostuvat kuitenkin turvallisuuden takaamiseksi haastavista laskennallisista toimenpiteistä ja menetelmistä, joilla voi olla negatiivinen vaikutus implementaatiomahdollisuuksiin ja skaalautuvuuteen.

Asiasanat: nollatietotodistus, todentaminen, todistusmenetelmä, Secure Remote Password, M-Pin

ABSTRACT

Syväntö, Adi
Zero-Knowledge proofs in user authentication
Jyväskylä: University of Jyväskylä, 2023, 28 pp.
Information Systems Science, Bachelor's Thesis
Supervisor(s): Marttiin, Pentti

The use of zero-knowledge proofs to authenticate user has received increasing attention due to evolving digitalization and security threats as a potential solution to the risks and vulnerabilities of the traditional password-based authentication method. The traditional password-based authentication method is vulnerable to damaging attacks in addition to other security challenges. In contrast, zero-knowledge proofs allow proving identity without the need to store and transmit sensitive information over internet. The aim of this literature review was to investigate how zero-knowledge proofs are used in authenticating user credentials in an online environment, and to identify the benefits and potential drawbacks of zero-knowledge proofs through two implementation examples. In the SRP protocol, zero-knowledge is achieved through a shared value between user and server, generated from the user's password, which itself does not compromise the user's sensitive information. M-Pin, on the other hand, is a multi-factor authentication method that includes the existence of a so-called Trusted Party. The Trusted Party is responsible for granting a user an identity-related secret, which, in addition to the PIN chosen by the user, is used to generate a token required when authenticating user to the server. User authentication methods using zero-knowledge proofs proved to be highly resistant to vulnerabilities such as man-in-the-middle and dictionary attacks. However, they consist of challenging computational operations and methods to ensure security, thus can have a negative impact on implementation capabilities in addition to scalability.

Keywords: zero-knowledge proof, authentication, proof system, Secure Remote Password, M-Pin

KUVIOT

SISÄLLYS

1 JOHDANTO

Digitalisaation myötä useat käyttämämme palvelut ovat siirtyneet fyysisistä palveluista verkkopalveluiksi. Esimerkiksi pankkien ja asiakkaiden välinen toiminta painottuu yhä enemmän verkkoon rakennetuille palveluille. Teknologisen kehityksen myötä riskit tietoturvauhkiin kasvavat samalla. Käyttäjän identiteetin todentaminen nähdään tietojärjestelmien turvallisuuden perustana (Zhu ym., 2015). Todentamistapoja eri käyttötarkoituksiin on useita; yleisimpänä verkkoympäristössä esiintyy kuitenkin perinteinen käyttäjänimi/salasana -todennus, joka laajalti katsottuna nähdään käytännössä rikkoutuneena. Grzonkowski & Corcoran (2014) mukaan käytännössä kaikki salasanaan perustuvat HTTPS-protokollaa käyttävät web-applikaatiot olettavat sen tarjoavat suojatun yhteyden todentavaan palvelimeen, jolloin käyttäjätiedot ovat salattuja vain palvelimen julkisella avaimella, joka toimitetaan istunnon alkaessa. Lisäksi Pathak ym. (2021) mukaan käyttäjän tunnistetietoja ei yleensä tallenneta tavallisessa tekstimuodossa, mutta tunnistautumisprosessin aikana tunnistetiedot lähetetään tekstimuodossa. Tämä nähdään ongelmana, mutta monet kehittäjät laiminlyövät sen. Kasvava määrä verkkopalveluita on johtanut myös uusien digitaalisen identiteetin hallintajärjestelmien (DIMS) syntyyn (Yang & Li, 2020). Suurin osa näistä on kuitenkin keskitettyjä, jonka vuoksi ne ovat alttiita kyberhyökkäyksille (Dunphy & Petitcolas, 2018). Keskitettyjen digitaalisen identiteetin hallintajärjestelmien tietovuodot, kuten Facebookin kymmenien miljoonien käyttäjätietojen vuoto, aiheuttavat suuria menetyksiä käyttäjille. Tämän vuoksi keskitetyt DIMS:it eivät voi taata henkilötietojen luotettavuutta ja saatavuutta. (Ingram, 2018.) Identiteetin todentamisessa ja todentamisen tietoturvassa on siis vielä nykypäivänäkin puutteita verkkopalveluiden tallentaessa kirjautumistiedot hallintajärjestelmiin, ja siten mahdollistaen kyberhyökkäykset, kuten esimerkiksi tietojen kalastelu-hyökkäykset. Tässä tutkielmassa tarkastellaan nollatietotodistusten (eng. Zero-Knowledge Proofs tai ZKP) käyttöä todentamisessa erinäisissä palveluissa. Nollatietotodistuksia käyttäviä todennusprotokollia on muodostettu teoreettisella tasolla tieteen alan teksteissä useita, mutta tutkielmassani keskityn kahteen perinteisen käyttäjänimi/salasana -todennusmenetelmän korvaavaan – nollatietotodistuksia hyödyntäviin protokolliin. Tutkimuksessa käyn läpi myös

protokollien tarjoamia hyötyjä sekä mahdollisia haittoja perinteisiin menetelmiin verrattuna. Tutkimuskysymykset tutkielmassani ovat:

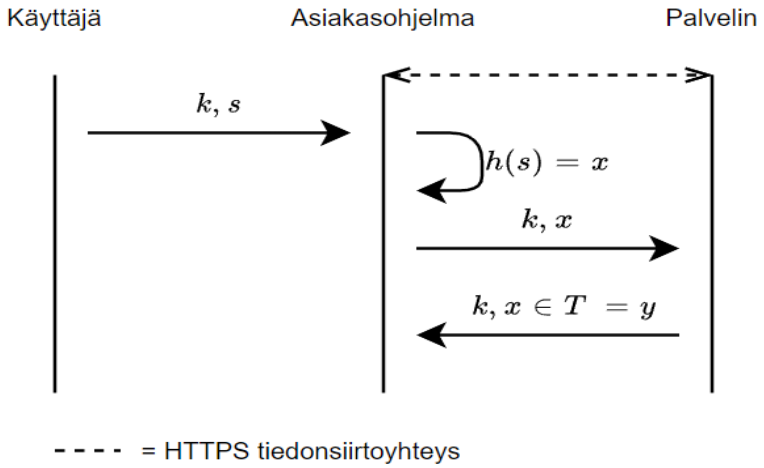
1) *Miten nollatietotodistuksia hyödynnetään käyttäjätietojen todentamisessa?*
2) *Mitä hyötyjä ja haittoja nollatietotodistus protokollilla on käyttäjätietojen todentamisessa?*

Tutkimus toteutetaan Salmisen (2011) esittelemän kuvailevan kirjallisuuskatsauksen menetelmien mukaisesti. Tutkimuksen kirjallisuus haettiin käyttäen kirjallisuuden tietokantoja, kuten Google Scholaria, Science Directiä ja ACM Digital Librarya. Keskeisimpiä hakutermejä tai tarkennettuja hakuja ovat: ”Zero-Knowledge Proof”AND ”Authentication” OR ”Protocol”, “Cryptography” AND “Zero-Knowledge Proof” ja ”Web-application” OR ”Web” AND ”Authentication” OR ”Identification”. Tutkimuksessa esittelen ensin perinteisen käyttäjätunnus/salasana -tunnistautumismenetelmän toiminnan, sen hyötyjä ja haittoja, minkä jälkeen käsittelen nollatietotodistuksen konseptin kryptografian osa-alueena. Tämän jälkeen käsittely kohdistuu nollatietotodistusten hyödyntämiseen todentamisen protokollissa kahden esimerkin avulla, sekä näiden hyötyihin ja haittoihin. Lopuksi pohdin johtopäätöksissä esiin nousseita etuja ja haasteita nollatietotodistusten implementoinnissa sekä vertaan näitä perinteiseen salasanaan perustuvaan todentamismenetelmään, ja esitän jatkotutkimusehdotuksia.

2 SALASANAAN PERUSTUVA TODENTAMINEN

Verkkopalveluissa käyttäjätietojen todentaminen on yksi oleellisimpia toimintoja yksityisen informaation esittämisen ja käyttäjien identifioinnin kannalta. Käyttäjän tunnistetiedot jakautuvat päätasolla tietämykseen-, omistukseen- ja perintöön perustuviksi. Tietämykseen perustuviin tunnistetietoihin sisältyy kaikki käyttäjän itsensä tietämä, kuten salasanat ja turvakysymysten yksilölliset vastaukset. Omistukseen perustuvat ovat käyttäjän omaavia asioita kuten älykortti, ja perintöperustaiset sisältävät ominaisuuksia, jotka identifioivat käyttäjän itsensä, kuten sormenjäljen tai muut biometriset tiedot. (Wu, 1998). Tässä luvussa esitän lyhyesti laajasti hyödynnetyn (Bonneau, Herley, Oorschot & Stajano, 2012; Zheng & Jin, 2012) tunnistautumismenetelmän rakenteen, joissa tunnistetieto on tietämykseen perustuva salasana, sekä tämän rakenteen hyödyt ja haitat.

Salasanaan perustuvassa todentamismenetelmän osapuolia ovat perinteisesti asiakasohjelma, palvelin ja näiden välinen kommunikaatiokanava verkossa, jossa datan siirtäminen toteutetaan yleisesti hyödyntäen HTTPS-protokollaa (*Hypertext transfer protocol secure) (*Pathak ym., 2021). Lyhyesti HTTPS-protokolla on hyperlinkeillä sivujen lataamiseen käytetty protokolla, jossa merkintä ”S” muodostuu salausprotokollan (TLS tai SSL) käytöstä datan siirrossa. Menetelmässä tunnistautuminen alkaa palvelimen pyytäessä asiakasohjelmalta tunnistetietoja. Käyttäjä syöttää tämän jälkeen pyynnöstä käyttäjätunnuksen k ja salasanan s asiakasohjelmaan, jossa salasanasta muodostetaan tiivistefunktiolla $h(s)$ tiiviste x. Muodostetut tunnistetiedot lähetetään suoraan palvelimelle, joka vastaanotettuaan tunnistetiedot, vertaa näitä tietokantaan tallennettuihin käyttäjätietoihin. Tietokantaan tallennetut käyttäjätiedot koostuvat käyttäjätunnuksesta, ja tunnukseen liitetystä tiivistefunktion tuottamasta salatusta arvosta. Vastaavuuden perusteella palvelin lähettää tuloksen $k, x \in T = y$ asiakasohjelmalle, ja myöntää siten oikeudet palveluun. (Pathak ym., 2021.)



Kuvio 1: Perinteisen salasanaan perustuvan todentamisprotokollan rakenne perustuen Pathak ym. (2021) artikkeliin

Perinteinen salasanaan perustuva todentamismenetelmä tarjoaa seuraavia hyötyjä. Ensinnäkin salasanaan perustuvan todentamisen protokollan laskennallinen haastavuus on vähäistä, jonka vuoksi autentikointimenetelmän implementointimahdollisuudet ovat laajat, ja toteuttaminen kustannustehokasta ilman kallista laitteistoa ja infrastruktuuria. Toiseksi protokolla tarjoaa riittävän suojan useisiin verkkopalveluihin, mikäli käyttäjät valitsevat vahvan ja monimutkaisen salasanan.

Yksinkertaisessa salasanaan perustuvassa todentamismenetelmässä on kuitenkin useita turvallisuusriskejä ja haasteita sekä käyttäjän että palvelun ylläpitäjän näkökulmista. Useat verkkopalvelut vaativat tunnistautumiseen monimutkaisen salasanan, jolloin haasteeksi muodostuu useiden salasanojen muistaminen ja säilöntä. Usein käyttäjät kuitenkin uudelleenhyödyntävät salasanoja eri järjestelmissä, jolloin hyökkääjä kykenee tunkeutumaan yhdellä salasanalla käyttäjän tileille eri palveluissa. Perinteinen salasanaan perustuva todentamismenetelmä on myös altis hyökkäyksille, kuten näppäinlokille, kalastushyökkäyksille (Raza, Iqbal, Sharif & Haider, 2012), ja väliintulohyökkäyksille, joissa hyökkääjä esiintyy todentamiskommunikaation toisena osapuolena molemmille osapuolille. Hyökkääjä saattaa siten muuttaa kommunikaatiota ja urkkia sensitiivistä informaatiota. (Pathak ym., 2021.) Vaikka perinteisessä salasanaan perustuvassa todentamismenetelmässä palvelimelle lähetetään tiivistefunktiolla salasanasta generoitu salattu arvo, on yksi keskeinen riski salatun salasanan siirtäminen verkon yli. Siirto mahdollistaa väliintulohyökkääjälle salasanan tiivisteen sieppaamisen sekä murto-ohjelmalla tekstimuotoisen salasanan generoimisen, tai käyttäjän tietoihin pääsyn pelkällä tiivisteellä. (Pathak ym., 2021.)

Kokonaisuudessaan perinteinen salasanaan perustuva todentaminen ja sen rakenne muodostavat huomattavia haasteita verraten sen tarjoamiin vähäisiin hyötyihin. Vaikka menetelmän käyttöönotto ja ylläpito on kustannustehokasta eikä vaadi suurta laskentatehoa, menetelmän keskeinen vaihe – salatun salasanan lähettäminen luo paljon tietoturvahaasteita, joiden ratkaisemiseksi menetelmään ympärille sen turvallisuuden lisäämiseksi vaaditaan täydentäviä

tietoturvaratkaisuja, kuten tietoliikenneturvallisuus- ja tietokantojen turvallisuusratkaisuja, sekä ratkaisuja käyttäjille salasanojen turvalliseen säilömiseen.

3 NOLLATIETOTODISTUKSET

Perimmäinen kryptografinen ongelma on tarjota keinoja paljastaa ennalta määrättyä tietoa osapuolille, jotka eivät luota toisiinsa. Haasteina ovat, kuinka mahdollistetaan salaisuuden osan varmentaminen paljastamatta muita osia, ja onko mahdollista todistaa väite paljastamatta muuta kuin väitteen totuusarvo (Goldreich, 2003). Yleisesti väitteen todistusprosessissa todistaja paljastaa informaatiota väitteen totuusarvon lisäksi (tosi tai epätosi). Prosessia, jossa väitteen todistamisessa ei paljasteta muuta kuin sen totuusarvo, kutsutaan nollatietotodistukseksi. Nollatietotodistuksen termin (*Zero-Knowledge Proof* tai *ZKP*) toivat esille Goldwasser, Micali ja Rackoff (1989) kehittämässään teoriassa *interaktiivisesta todistusmenetelmästä* tutkiessaan tiedon siirtämisen määrää todistajalta varmentajalle interaktiivisessa todistusmenetelmässä. He osoittivat mahdolliseksi väittämän todistamisen paljastamatta muuta kuin väitteen totuusarvon.

Nollatietotodistus on siis erityinen interaktiivisen todistusmenetelmän muoto. Jotta voitaisiin ymmärtää nollatietotodistusten periaatteet, esittelen ensin informaalin esimerkin nollatietotodistukselle, ja interaktiivisen todistusmenetelmän sekä tämän periaatteet. Keskeinen variaatio nollatietotodistuksista on ei-interaktiivinen nollatietotodistus, jonka määrittelen luvussa 3.3.

3.1 Informaali esimerkki nollatietotodistuksesta

Tunnettuna esimerkkinä nollatietotodistuksesta käytännössä toimii tilanne, jossa halutaan todistaa Waldon sijainti kuvan väkijoukossa. Tilanteessa todistajan täytyy todistaa tieto Waldon sijainnista kuvassa paljastamatta sitä varmentajalle. Todistaminen voidaan toteuttaa käyttämällä esimerkiksi palaa kartonkia, joka on neljä kertaa suurempi kuin *Where is Waldo* -kirjan sivu, ja leikkaamalla kartongin keskelle reikä, josta voi nähdä vain Waldon kasvot. Tällä tavoin kirja voidaan asettaa kartongin palan taakse siten, että vain Waldon kasvot näkyvät, mutta varmentaja ei näe missä kohtaa kartonkia kirja sijaitsee ja päätellä siten Waldon sijainnin kuvassa. Prosessissa todistaja kykenee todistamaan varmentajalle

tietävänsä Waldon sijainnin kuvassa paljastamatta toteamuksesta mitään muuta kuin sen totuusarvon.

3.2 Interaktiiviset todistusmenetelmät

Goldreich (2003) esittää interaktiivisen todistusmenetelmän määritelmän viittaavan kahteen laskennalliseen tehtävään: todistuksen tuottaminen ja sen pätevyyden tarkistaminen (0 = hylkää, 1 = hyväksyy). Tehtävien toteutuksessa on kaksi osapuolta: todistaja, jonka tavoitteena on todistaa tietämys salaisesta informaatiosta, ja varmentaja, jonka tehtävänä on tarkistaa todisteen pätevyys. Perinteisesti matematiikassa todisteen nähdään luovan ehdoton varmuus todistamastaan väitteestä. Interaktiivisissa todistusmenetelmissä sen sijaan omaksutaan virhetodennäköisyys todistuksen luonteen ollessa probabilistinen.

Kaikilla interaktiivisilla todistusmenetelmillä on kaksi ominaisuutta: täydellisyys ja eheys. Täydellisyys viittaa todistajan kykyyn vakuuttaa varmentaja todenmukaisista väittämistä. Eheydellä tarkoitetaan vastaavasti sitä, että varmentajaa ei voida vakuuttaa hyväksymään epätosia väittämiä. (Goldreich, 2003.) Ominaisuudet eivät kuitenkaan perustu ehdottomuuteen, vaan interaktiivisessa todistusmenetelmässä todisteen probabilistisen luonteen vuoksi ehdottomuus korvataan ”erittäin suurella” todennäköisyydellä. Formaalin määritelmän mukaan interaktiivisten koneiden paria (P, V) kutsutaan interaktiiviseksi todistusmenetelmäksi kielelle L, jos kone V on polynomiaikainen ja seuraavat kaksi ehtoa ovat voimassa (Goldreich, 2003):

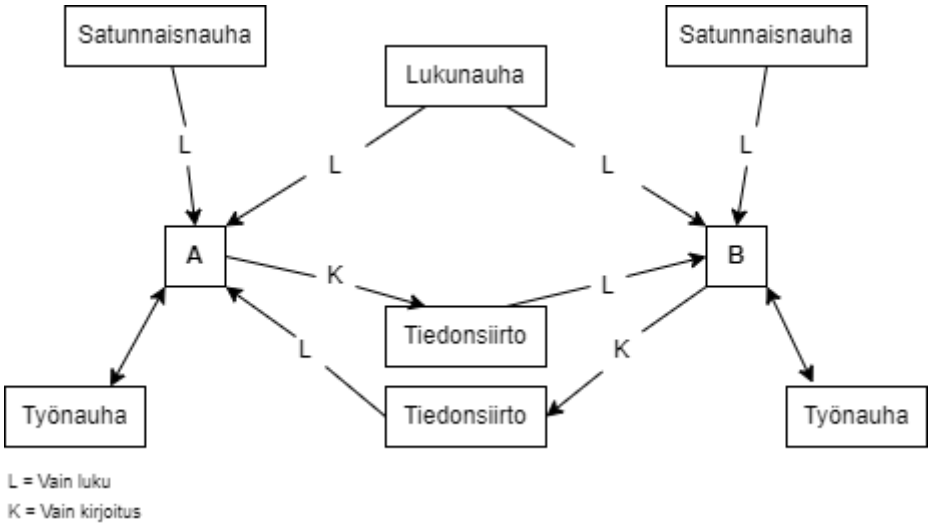
Täydellisyys: Jokaiselle $x \in L$,
$$\Pr[(P,V)(x) = 1] \geq \frac{2}{3}$$
Eheys: Jokaiselle $x \notin L$ *ja jokaiselle interaktiiviselle koneelle* B
$$\Pr[(B,V)(x) = 1] \leq \frac{1}{3}$$

Määritelmän mukaisessa interaktiivisessa todistusmenetelmässä täydellisyys viittaa kaikkiin potentiaalisiin todistajiin P, kun eheys viittaa vain määriteltyyn varmentajaan V. On huomioitava, että varmentajan on oltava polynomiaikainen, eikä todistajan laskentateholla ole rajoitteita kummassakaan ehdossa. Lisäksi ehtojen virhetodennäköisyydet $\frac{2}{3}$ ja $\frac{1}{3}$ pienenvät exponentiaalisesti (polynomiaalisten) toistojen myötä. Vaihtoehtoisesti alkuperäisessä interaktiivisen todistusmenetelmän määritelmässä virhetodennäköisyys ($|x|^{-k}$) ei ole kiinteä, vaan riippuvainen syötteen pituudesta $|x|$ ja vakiosta k (Goldwasser ym., 1989).

Interaktiivisessa todistusmenetelmässä oleellista on sen luonne yksityisen kolikon (*private coin*) menetelmänä, mikä tarkoittaa, että menetelmässä kunkin osapuolen generoidut satunnaisarvot ovat yksityisiä. Vastaavasti julkinen kolikko (*public coin*) viittaa satunnaisarvojen julkisuuteen molemmille osapuolelle.

Osapuolet interaktiivisessa todistusmenetelmässä ovat *interaktiivisia Turingin koneita*, joilla on luku-, työ-, satunnaistiedonsiirtonauha sekä yksi vain

lukukäyttöön tarkoitettu tiedonsiirtonauha, ja yksi vain kirjoituskäyttöön tarkoitettu tiedonsiirtonauha. Tiedonsiirtonauhoilla tarkoitetaan Turing-koneessa tallennustilaa, jota käytetään tiedon siirtämiseen ja lukemiseen. (Goldwasser ym., 1989.) Todistajan ja varmentajan satunnaistiedonsiirtonauhoilla tuodaan laskentaprosessiin satunnaisuutta ja tekee osapuolista *probabilistisia Turingin koneita*. (Goldreich, 2003)



Kuvio 2: Interaktiivisten Turingin koneiden pari (Goldwasser ym., 1989)

3.2.1 Interaktiiviset nollatietotodistukset (IZKP)

Interaktiiviset nollatietotodistusmenetelmät (IZKP) viittaavat interaktiivisiin todistusmenetelmiin (*P, V*) kielelle *L*, ”jos kaikki, mikä voidaan tehokkaasti laskea *P*:n kanssa vuorovaikutuksen jälkeen syötteestä $x \in L$, voidaan tehokkaasti laskea myös *x*:stä (ilman vuorovaikutusta).” (Goldreich, 2003). Määritelmä kuvaa sitä, kuinka nollatietoisuus ominaisuutena on todistajan pääomaa – suoja todistajalle varmentajan yrityksiltä hankkia tietoa vuorovaikutuksessa. IZKP-menetelmillä on täydellisyys- ja eheys -ominaisuuksien lisäksi myös *nollatietoisuus*-ominaisuus. Nollatietoisuudella tarkoitetaan todistusmenetelmän konstruktiota siten, että väitteen totuusarvon lisäksi menetelmä ei paljasta muuta informaatiota. Kryptografiassa nollatietoisuus-ominaisuuden saavuttamiseksi vaaditaan yleisesti simulaattorialgoritmin olemassaolo, jolla voidaan simuloida todistajan ja varmentajan vuorovaikutusta ja sen tulosteita.

Formaalin nollatietoisuuden määritelmän mukaan interaktiiviseen todistusmenetelmään kielelle *L* pätee nollatietoisuus, jos jokaiselle probabilistiselle polynomiaikaiselle varmentajalle *V* on olemassa probabilistinen polynomiaikainen simulaattori *M* siten, että seuraavat kaksi todennäköisyyskokonaisuutta ovat *laskennallisesti erottamattomat* (Goldreich, 2003; Goldwasser ym., 1989):

- $\{(P,V)(x)\}_{x\in L}$, eli varmentajan *V* tulosteiden kokonaisuus vuorovaikutuksen jälkeen *P*:n kanssa yhteisellä syötteellä x
- $\{M^*(x)\}_{x\in L}$, eli simulaattori *M*:n tulosteiden kokonaisuus syötteestä x

Edellä esiteltyä määritelmää nollatietotodistusmenetelmästä kutsutaan *laskennalliseksi nollatietoisuudeksi*. *M* ja (*P, V*) todennäköisyyskokonaisuuksien jakauman perusteella määrittelyssä käytetään myös termejä *täydellinen nollatietoisuus* sekä *tilastollinen nollatietoisuus*. Interaktiiviseen todistusjärjestelmään pätee täydellinen nollatietoisuus, mikäli edellä mainitut todennäköisyysjoukot ovat *identtisesti jakautuneet,* ja on siten määritelmistä vaativin. Tilastollisessa nollatietoisuudessa, josta Goldreich & Oren (1994) käyttävät käsitettä *lähes täydellinen nollatietoisuus,* vastaavasti todennäköisyysjoukkojen jakaumat ovat lähekkäin, jolloin näiden tilastollinen eroavaisuus nähdään merkityksettömänä. Goldreichin (2003) mukaan käytännön tarkoituksiin ei ole tarpeellista täydellisesti simuloida varmentajan tulostetta todistajan kanssa vuorovaikuttamisen jälkeen, vaan on riittävää, että mainittujen todennäköisyysjoukkojen jakaumat ovat laskennallisesti erottamattomat.

Informaalisti ilmaistuna kaksi todennäköisyysjakaumaa ovat laskennallisesti erottamattomat, jos mikään tehokas algoritmi D, merkityksetöntä todennäköisyyttä huomioon ottamatta, ei erota näitä toisistaan. Goldreichin (2003) mukaan formaalimmin määriteltynä todennäköisyyskokonaisuudet $\{R_x\}_{x\in L}$ ja $\{S_x\}_{x\in L}$ ovat laskennallisesti erottamattomat, mikäli jokaiseen probabilistiseen polynomiaikaiseen (erottaja) algoritmiin D, polynomiin p, ja riittävän pitkään $x \in L$ pätee:

$$|Pr[D(x, R_x) = 1] - Pr[D(x, S_x) = 1]| < \frac{1}{p(|x|)}$$

Määritelmässä $D(.)$ tarkoittaa algoritmin D tulosteita ($\in \{0, 1\}$) polynomiaaliajassa prosessoiduista todennäköisyyskokonaisuuksien otoksista. Jotta todennäköisyyskokonaisuudet olisivat laskennallisesti erottamattomat, on tulosteiden $D(x, R_x) = 1$ ja $D(x, S_x) = 1$ todennäköisyyksien erotuksen oltava pienempi kuin $\frac{1}{p(|x|)}$, jossa $|x|$ tarkoittaa syötteen x pituutta. (Goldreich, 2003.)

3.2.2 Nollatietotodistusmenetelmä kuvaajan väritykselle (Graph coloring)

Kuvaajan 3-värityksen (Graph 3-Coloring tai G3C) tiedetään olevan NP-täydellinen ongelma (Garey ym., 1976), jolle Goldreich ym. (1991) esittivät interaktiivisen nollatietotodistusmenetelmän. Idea menetelmässä on usean nollatietotodistusmenetelmän kaltainen jaettaessa todistus useaan osaan siten, että iteraatiot itsessään eivät paljasta väittämästä informaatiota. Menetelmässä – kuten useissa kryptografian protokollissa – oleellinen väline on kommittijärjestelmä (*commitment scheme*). Kommittijärjestelmät ovat kryptografian protokollien vakioelementtejä, jotka sallivat tiedon lähettämisen pitämällä sen salattuna, kunnes se ”avataan”. Kommittia voidaan verrata tiedon sulkemiseen kirjekuoreen, jolloin tieto on salattuna, mutta sitä ei voida enää muuttaa. Kommitti-järjestelmä on tehokas kaksiosainen protokolla (kommitti-vaihe ja paljastus-vaihe), jossa lähettäjä kommitoi arvon siten, että seuraavat kaksi ehtoa täyttyvät (Goldreich, 2003):

- **Salassapito:** Kommitti-vaiheen päätyttyä vastaanottaja ei kykene saamaan tietoa lähettäjän kommitoimasta arvosta.
- **Sitovuus:** Kommitti-vaiheen päätyttyä lähettäjä ei kykene onnistuneesti vakuuttamaan vastaanottajaa paljastamaan kaksi toisistaan eriävää arvoa paljastusvaiheessa.

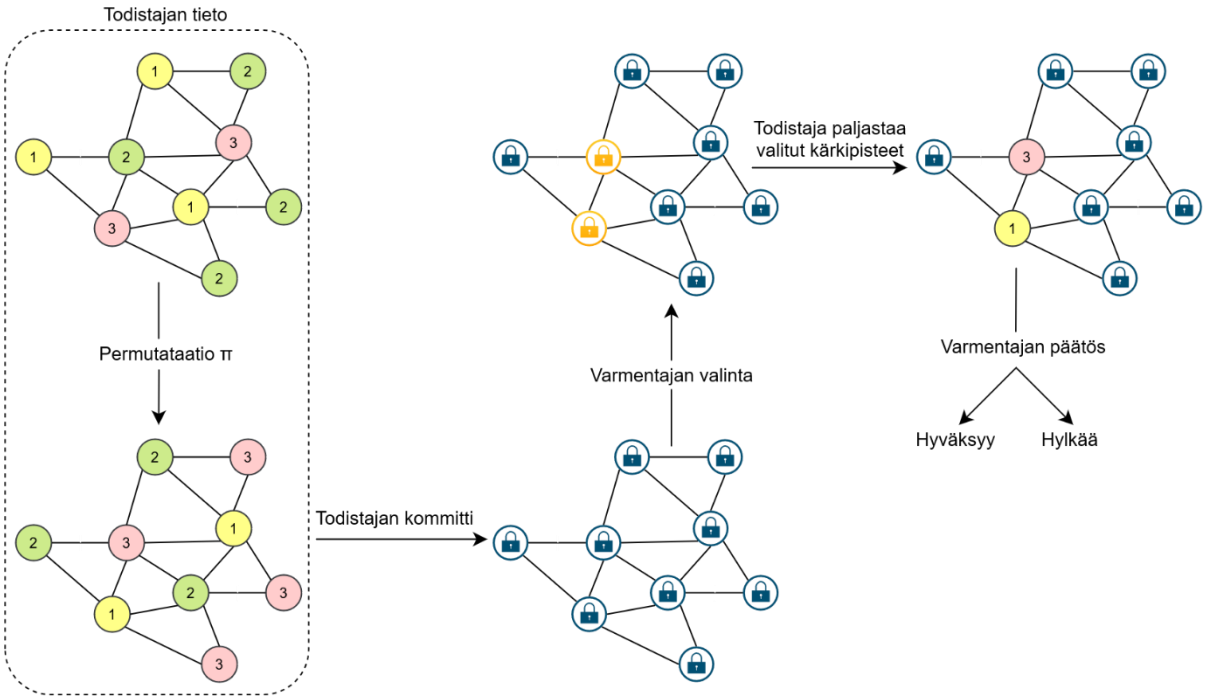
Toisin sanoen kommitti-vaiheessa vastaanottaja ei saa tietoa lähetetystä arvosta, mutta lähettäjä on sidottu yhteen kommitti-vaiheen määrittämään arvoon. Vastaanottaja hyväksyy yhden lähetetyn arvon, jos ja vain jos se vastaa kommitti-vaiheen transkriptiota (eli kommitti-vaiheessa ”lukittua” lähetettävää arvoa sekä tähän liitettyä satunnaisarvoa). Seuraavaksi esitän vaiheet G3C:n nollatietotodistusmenetelmässä perustuen Goldreichin ym. (1991) ja Goldreichin (2003) kirjallisuuteen.

Tavoitteena menetelmässä on todistaa 3-värisen graafin olemassaolo. Graafin $G(V, E)$ sanotaan olevan 3-väritetty, jos on olemassa graafin kuvaus $\phi: V \rightarrow \{1, 2, 3\}$ siten, että jokainen vierekkäinen kärkipiste $((u, v) \in E)$ on eriävä. {1,2,3} tarkoittaa graafin värityksessä käytettäviä eri värejä. Olkoon graafi $G = (V, E)$, jossa V tarkoittaa kärkipisteitä $\{v_1, v_2, \ldots, v_n\}$ ja E eri kärkipisteitä yhdistäviä reunoja esim. $\{v_3, v_5\} \in E$. Menetelmän vaiheet suoritetaan m^2 kertaa, jossa $m = |E|$.

- Olkoon ϕ 3-väritys G:stä. Todistaja valitsee satunnaisen permutaation $\pi \in \{1,2,3\}$. Todistaja kommitoi itsensä jokaiseen graafin kärkipisteeseen valitsemalla satunnaisarvon r_i jokaiselle kärkipisteelle $\phi_\pi(v_i)$. Todistaja muodostaa kommitit $c_i = C_{r_i}(\phi_\pi(v_i))$, jossa C_{r_i} tarkoittaa todistajan kommittia arvoon käyttäen satunnaisarvoa r_i. Todistaja lähettää kommitoidut arvot $\{c_1, \ldots, c_n\}$ varmentajalle.
- Varmentaja valitsee satunnaisesti kärkipisteiden välin eli reunan $e = (v_i, v_j) \in E$, ja lähettää sen todistajalle.
- Todistaja paljastaa kommitoidut *e*:n värit lähettämällä kärkipisteiden arvot $(r_i, \phi_\pi(v_i))$ ja $(r_j, \phi_\pi(v_j))$ eli kommittivaiheessa määritellyt satunnaisarvot sekä graafin permutaation kärkipisteiden värit varmentajalle.
- Varmentaja tarkistaa paljastettujen arvojen vastaavuuden kommitti-vaiheen transkriptioihin sekä ovatko paljastetut värit eriävät $\phi_\pi(v_i) \neq \phi_\pi(v_j) \in \{1,2,3\}$. Ehtojen täyttymisen perusteella varmentaja joko jatkaa seuraavaan iteraatioon, tai hylkää ja keskeyttää.

Toteutettuaan kaikki m^2 iteraatiota varmentaja hyväksyy. Menetelmässä kommittijärjestelmällä turvataan varmentajan varmuus siitä, että todistaja ei kykene muuttamaan kommitoituja arvoja kesken protokollan. Mikäli todistajan väite on tosi ja graafi todella on 3-väritys, varmentajan valinnasta riippumatta kärkipisteiden värit ovat aina eriävät, jolloin ehto *täydellisyydestä* täyttyy. Mikäli todistajan väite ei ole tosi, jokaisella iteraatiolla varmentajan todennäköisyys hylätä on vähintään $\frac{1}{m}$. Todennäköisyys hyväksymiseen (eli kaikkien iteraatioiden m^2 toteuttamiseen ilman hylkäämistä) on enintään $(1 - \frac{1}{m})^{m^2} \approx e^{-m}$ tarkoittaen sitä, että varmentajaa ei voida *eheys*-ehdon mukaisesti huijata hyväksymään

virheellistä todistusta poissulkien merkityksetön todennäköisyys (tässä tapauksessa e^{-m}). Menetelmän jokaisen iteraation paljastaessa varmentajalle vain satunnaisen permutaation kahden kärkipisteen värit, ei menetelmä siten paljasta todistajan väitteestä muuta kuin sen todenmukaisuuden. Lisäksi permutaatioiden käyttö jokaisella iteraatiolla estää varmentajaa muodostamasta 3-värityksestä totuusarvon lisäksi muuta informaatiota täyttäen *nollatietoisuus*-ehdon. (Goldreich ym., 1991; Goldreich, 2003.)



Kuvio 3: G3C:n nollatietotodistusmenetelmän iteraation kulku

3.3 Ei-interaktiiviset nollatietotodistukset

Nollatietoisuus on useissa käyttötarkoituksissa hyödyllinen todistusmenetelmän ominaisuus, mutta interaktiivisten todistusmenetelmien tiivis vuorovaikutteinen luonne saattaa luoda haasteita. Interaktiivisen nollatietotodistusmenetelmän vaatimus todistajan ja varmentajan samanaikaisesta läsnäolosta tekee menetelmistä skaalautumattomia, ja joissakin käyttötarkoituksissa vaikeita – usein jopa mahdottomia toteuttaa.

3.3.1 Ei-interaktiivisen nollatietotodistuksen käsite

Blum, Feldman ja Micali (1988) muodostivat käsitteen *ei-interaktiiviselle nollatietotodistukselle* (jatkossa viitattu NIZK) todistaessaan laskennallisen monimutkaisuuden korvaavan interaktiivisten todistusmenetelmien vuorovaikutuksen ja satunnaisuuden salassapidon (ks. yksityinen kolikko). He muodostivat

artikkelissaan *yhden teoreeman ei-interaktiivisen nollatietotodistusmenetelmän* NP-täydelliselle graafin 3-väritys ongelmalle todistaen menetelmän pätevyyden kaikille NP-kielen väittämille. Muodostettu menetelmä koostuu yksittäisestä viestistä todistajalta varmentajalle poistaen siten menetelmästä vuorovaikutuksen. Entiteettien välisen vuorovaikutuksen poistuessa todistusmenetelmästä, vaatii nollatietoisuuden ja tehokkuuden takaaminen muita keinoja.

Oleellista kryptografiassa menetelmien muodostamisessa on *todistettava turvallisuus.* Termi viittaa tarkkoihin matemaattisiin määritelmiin menetelmän turvallisuustavoitteista perustuen kryptografisiin alkutekijöihin (kuten alimman tason algoritmeihin) ja oletuksiin. Oletuksien liittyessä ainoastaan ongelmien laskennalliseen haastavuuteen, sanotaan menetelmän olevan todistettu turvalliseksi standardimallissa. Turvallisuustodisteiden saavuttaminen standardimallissa on tunnetusti erittäin vaikeaa ja esimerkiksi tehokkaan ja turvallisen NIZK-menetelmän luominen standardimallilla on siten haastavaa tai jopa mahdotonta. Seuraavaksi esittelen *Random Oracle* -mallin, jossa turvallisuustodisteita NIZK-todistusmenetelmälle on onnistuttu saavuttamaan idealisoidun satunnaisuuden implementoinnin vuoksi.

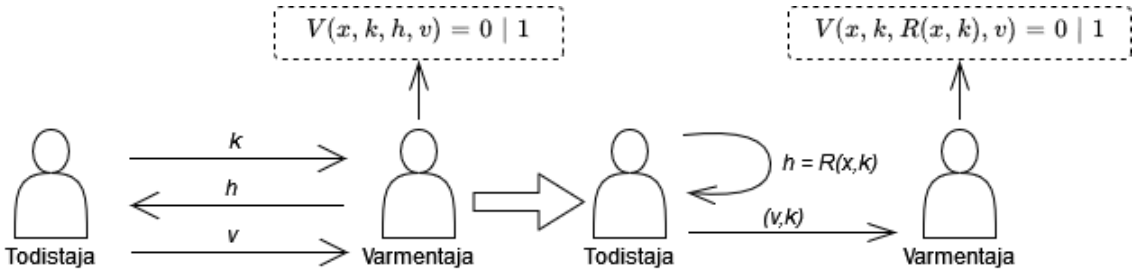
3.3.2 Random Oracle -malli (RO)

Näennäissatunnaisfunktioita (tai pseudosatunnaisfunktioita) käytetään useissa kryptografisissa algoritmeissa tuottamaan satunaisarvoja. Funktioiden tuotokset eivät teoriassa ole täysin satunnaisia, vaan ennalta arvaamattomia, sillä matemaattiset operaattorit itsessään eivät kykene luomaan täysin satunnaista arvoa. Esimerkiksi ohjelmoinnissa usein käytetty *Math.random* -funktio ainoastaan simuloi satunnaisuutta tuottamalla liukuluvun $0 \leq x < 1$ (MDN, 2022), sillä matemaattisilla algoritmeilla toimivat tietokoneen numerogeneraattorit eivät voi olla täysin satunnaisia.

Formaalissa menetelmän turvallisuuden todistamisessa kohdataan kysymys siitä, voiko jokin näennäissatunnainen funktio aiheuttaa turvallisuusriskin algoritmissa. RO-mallissa turvallisuustodisteet saavutetaan modularisoimalla algoritmi siten, että sen käyttämät näennäiset satunniasfunktiot korvataan *satunnaisoraakkeleilla*, joiden palauttamat arvot ovat aidosti satunnaisia (Bellare & Rogway, 1993). Satunnaisoraakkelilla tarkoitetaan idealisoitua tiivistefunktiota, jonka satunnaisuutta ei rajoita algoritmit, ja jonka toiminta ei näy ulkopuolelle (kts. *black box*). Satunnaisoraakkeli palauttaa jokaisesta syötteestä itsenäisesti muodostetun satunnaisarvon, mutta pitää kirjaa palautetuista arvoista siten, että syöte x palauttaa aina arvon $R(x)$. RO-mallin metodologian kehittivät Bellare ja Rogaway (1993). Mallissa kaikkien menetelmän osapuolten saataville annetaan funktio R, jonka jälkeen menetelmä todistetaan turvalliseksi olettaen R:n palauttavan todella satunnaisen arvon syötteestä x. Myöhemmin käytännössä R korvataan hyvällä kryptografisella tiivistefunktiolla, kuten esimerkiksi MD5:lla (Rivest, 1992) tai SHA-3:lla (NIST, 2015).

Jo ennen RO-mallin metodologian kehittämistä Fiat ja Shamir (1987) esittivät merkityksellisen tavan hyödyntää satunnaisoraakkeleita, mitä kutsutaan Fiat-Shamir-heuristiikaksi. Menetelmässä he muuttivat interaktiivisen *public coin*

-tunnistautumisprotokollan ei-interaktiiviseksi digitaalisen allekirjoituksen protokollaksi. Huomionarvoista protokollassa on luotetun osapuolen (*Trusted Authority*) olemassaolo, jonka tehtävä on myöntää todistajan haltuun tunnistautumiseen käytettävät tiedot. Alkuperäisessä konstruktiossa luotettu osapuoli on esimerkiksi hallitus, joka myöntää tunnistautumistiedot sisältävän älykortin. (Fiat & Shamir, 1987.)



Kuvio 4: Yksinkertaistettu kuvaus Fiat-Shamir-heuristiikasta, jossa väittämä identiteetistä on x (Fiat & Shamir, 1987).

Kuvassa 4 vasemmalla esitettynä on interaktiivinen Fiatin ja Shamirin (1987) luoma tunnistautumisprotokolla, jossa todistaja aloittaa lähettämällä kommitoidun satunnaisarvon k varmentajalle. Varmentaja palauttaa satunnaisesti valitun haasteen h, johon todistaja palauttaa vastauksen v. Todistajan palauttaman vastauksen jälkeen varmentaja tekee päätöksen, jota merkitään $V(x, k, h, v)$ todistettavan väittämän (esimerkiksi salaisen numerosarjan) ollessa x. Muutoksessa vuorovaikutus poistetaan korvaamalla todistajan varmentajalta vastaanottama haaste satunnaisoraakkelin palauttamalla arvolla $R(x, k)$, ja käytännön implementaatioihin satunnaisoraakkeli korvataan kryptografisella tiivistefunktiolla. Todistajan varmentajalle lähettämä arvo on tällöin (v, k), joka sisältää alussa kommitoidun satunnaisarvon digitaalisen allekirjoituksen varmentamista varten. (Fiat & Shamir, 1987.)

RO-mallissa turvalliseksi todistetut menetelmät nostavat esiin myös kiistanalaisuuksia. Esimerkiksi sijoitettaessa ”riittävän hyvä” kryptografinen tiivistefunktio idealisoidun satunnaisoraakkelin tilalle, voidaan kyseenalaistaa saavutetut turvallisuustodisteet, minkä vuoksi Bellaren ja Rogwayn (1993) mukaan RO-mallin turvallisuustodisteisiin ei tule tukeutua käytännön implementaatioissa. Lisäksi Canetti, Goldreich ja Halevi (2004) kritisoivat artikkelissaan RO-mallin turvallisuustodisteiden epämääräisyyttä, ja muodostivat RO-mallissa turvalliseksi todistetun menetelmän, jolla ei standardimallissa turvallisuustodisteita voitu saavuttaa. Vaikka RO-mallin implementaatioiden turvallisuus nähdään sattumanvaraisena ja useissa niistä on todettu turvallisuusuhkia, uskotaan laajalti, että RO-malli todistaa menetelmän rakenteellisen eheyden yleisiä – helposti havaittavia haavoittuvuuksia vastaan (Canetti ym., 2004).

4 NOLLATIETOTODISTUSTEN HYÖDYNTÄMINEN TODENTAMISESSA

Nollatietotodistuksia hyödyntämällä sensitiivisiä todentamiseen vaadittuja tietoja ei säilötä keskitetyissä tietokannoissa. Tällöin on mahdollista eliminoida haasteet tietokantojen turvallisesta ylläpidosta ja mahdolliset riskit tietovuodoista. Edellisessä luvussa käsitellyissä nollatietotodistuksien määritelmissä nousevat esille kaksi keskeistä entiteettiä: todistaja ja varmentaja. Verkkoympäristössä tapahtuvassa tunnistautumisessa todistaja viittaa käyttäjän operoimaan asiakasohjelmaan ja varmentaja asiakasohjelman kanssa kommunikoivaan verkkopalvelimeen.

Tässä luvussa käsittelen nollatietotodistusten hyödyntämistä verkkotodennuksessa kahden esimerkin avulla. Ensimmäisenä tarkastelen Wu:n (1997) kehittämää Secure Remote Password -protokollaa, joka on yksi yleisimpiä salasanan todentamiseen käytettäviä nollatietotodistusprotokollia. Toisena esittelen lyhyesti M-Pin-protokollan (Scott, 2017), jonka toiminta perustuu pitkälti Fiatin ja Shamirin (1987) työhön. Molempien protokollien tavoitteena on korvata luvussa 2 esitellyn menetelmän tapaiset tunnistautumisen protokollat erinäisissä käyttökohteissa.

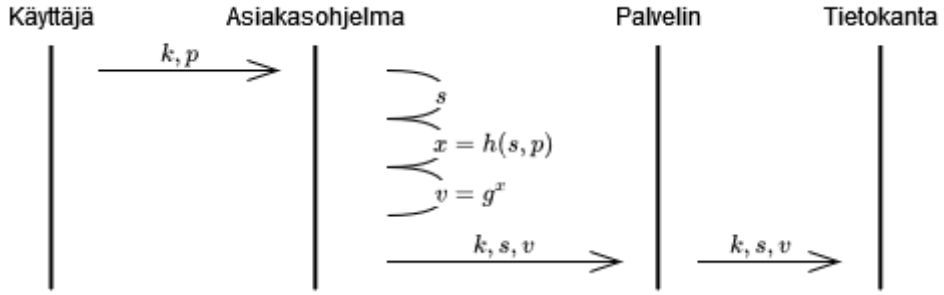
4.1 Secure Remote Password (SRP)

SRP-protokolla koostuu kahdesta vaiheesta: rekisteröinti ja todentaminen. Protokollan osapuolina ovat asiakasohjelma ja verkkopalvelin, jotka todistavat toisilleen tiedon rekisteröintivaiheessa luoduista salatuista arvoista. Asiakasohjelman salattu arvo on sen generoimasta *suolasta* eli satunnaisesta salasanaan lisättävästä merkkijonosta ja käyttäjän salasanasta tiivistefunktiolla generoitu arvo. Verkkopalvelimen salattua arvoa kutsutaan *varmentajaksi*, joka on

rekisteröintivaiheessa asiakasohjelman generoima ja tämän salatusta arvosta johdettu satunnainen merkkijono. (Sherman ym. 2020.)

Protokollan kaikki laskutoimitukset suoritetaan syklisessä ryhmässä $\mathbb{Z}_q$, jossa q on ennalta valittu suuri alkuluku. Näin ollen kaikki kerto-, jakolaskut ja exponentiaalit suoritetaan modulo q. Ryhmän virittäjää merkitään g ja h on yksisuuntainen tiivistefunktio. Seuraavaksi esittelen rekisteröintivaiheen toiminnan yksinkertaistettuna, jossa asiakasohjelma on A ja palvelin on P. Tarkempi kuvaus rekisteröintivaiheesta on kuvassa 5.

1. A vastanottaa käyttäjältä käyttäjätunnuksen ja salasanan.
2. A generoi suolan, luo tiivistefunktiolla suolasta ja salasanasta salatun arvon, sekä johtaa tästä varmentajan.
3. A lähettää P:lle käyttäjätunnuksen, suolan ja varmentajan.
4. P tallentaa vastaanottamansa tiedot tietokantaan.



Kuvio 5: SRP-protokollan rekisteröintivaiheen kuvaus pohjautuen Shermanin ym. (2020) artikkeliin.

Rekisteröintivaiheen jälkeen käyttäjän tunnistautuminen sisältää kaksi vaihetta: avaimen luominen ja todentaminen. Alla esittelen yksinkertaistettuna tunnistautumisen vaiheet. Tarkempi kuvaus tunnistautumisvaiheesta on kuvassa 6.

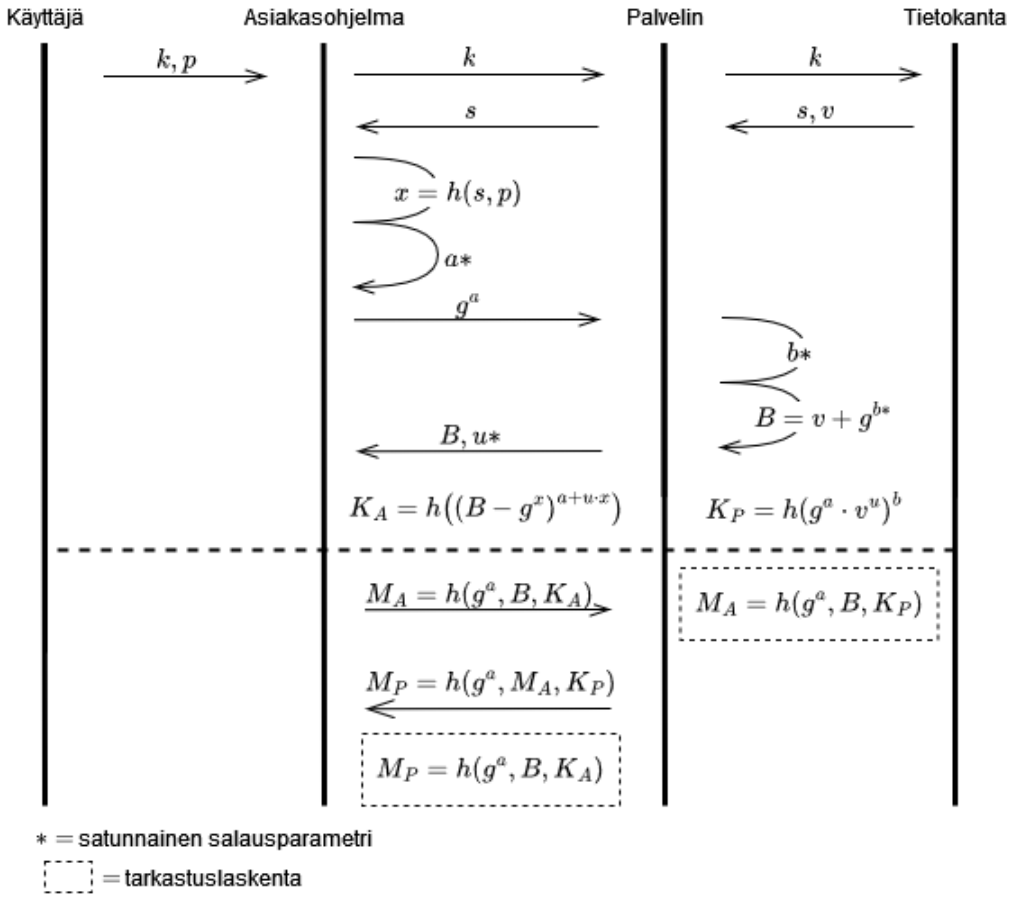
Avaimen luominen:

- A vastaanottaa käyttäjältä käyttäjätunnuksen ja salasanan.
- A lähettää P:lle käyttäjätunnuksen, ja P palauttaa tämän perusteella rekisteröintivaiheessa tietokantaan tallennetun suolan.
- A luo salatun arvon vastaanotetusta suolasta ja salasanasta, generoi satunnaisen salausparametrin a ja lähettää P:lle kerta-arvon g^a (*nonce*).
- P generoi satunnaiset salausparametrit b ja u, johtaa b:stä kerta-arvon g^b, ja lähettää A:lle $(v + g^b, u)$
- A ja P luovat sessioavaimet K_A ja K_P.

Avaimen todentaminen:

- A laskee arvon M_A, lähettää sen P:lle, joka tarkastaa arvon laskemallaan sessioavaimella.

- P laskee arvon M_P, lähettää sen A:lle, joka vuorostaan tarkistaa arvon omalla sessioavaimellaan.
- Todentaminen onnistuu vain, jos tarkistuslaskennat onnistuvat, eli $K_A = K_P$.



Kuvio 6: SRP-protokollan todentamisen kuvaus pohjautuen Shermanin ym. (2020) artikkeliin.

SRP-protokollassa on nähtävillä edellisissä osiossa käsiteltyjä nollatietotodistusten piirteitä. Protokolla voidaan nähdä interaktiivisena nollatietotodistusmenetelmänä, jossa todistaja on asiakasohjelma, ja varmentaja on verkkopalvelin. Osapuolten vuorovaikutuksessa ei nähdä sensitiivistä informaatiota, eikä palvelin saa tietoonsa menetelmän aikana salasanaa missään muodossa, mistä tämän voisi generoida, jolloin käyttäjän salasana on turvassa väliintulohyökkääjän yrityksiltä saada se haltuunsa.

SRP-protokolla ei kuitenkaan osoittaudu täysin varmaksi todentamisen menetelmäksi tietoturvariskejä vastaan. Shermanin ym. (2020) SRP-protokollan formaalissa analyysissa havaittiin, että haittapalvelin voi väärentää todennusistunnon asiakasohjelman kanssa ilman tämän osallistumista. Kuitenkaan suuria rakenteellisia heikkouksia protokollasta analyysissa ei löytynyt. Turvallisuus SRP-protokollassa perustuu yleiseen kryptografian laskennalliseen oletukseen - diskreetin logaritmin laskemisen haastavuuteen (Wu, 1998), jolloin ollakseen turvallinen täytyy protokollassa käytettävien lukujen olla satoja numeroita pitkiä.

Verrattuna perinteiseen tiivistefunktiota käyttävään käyttäjätunnus/salasana -protokollaan ei SRP vaadi turvallista palvelinta salattujen salasanojen käsittelyyn ja tallentamiseen. SRP-protokolla on lisäksi immuuni uusintahyökkäyksille, joissa validia verkkokommunikaatiota käytetään saavuttamaan kyberrikollisen tavoitteita, ja jopa lyhyillä salasanoilla voidaan saavuttaa huomattavasti parempi turvallisuuden taso kuin perinteisissä salasanaan perustuvissa todennusprotokollissa.

4.2 M-Pin

M-Pin-protokolla on nollatietotodistuksiin pohjautuva usean tekijän todentamismenetelmä, joka sallii käyttäjän (todistaja) todentaa itsensä palvelimelle (varmentaja) käyttäen myös Fiatin ja Shamirin (1987) työssä esiintyvän luotetun osapuolen (*Trusted Authority* tai TA) myöntämää identiteettisidonnaista salaisuutta. Menetelmässä todentamisen tekijät muodostuvat käyttäjän valitsemasta PIN-koodista, ja verkkotunnisteesta, joka johdetaan PIN-koodista ja TA:n myöntämästä salaisuudesta. (Scott, 2017.) TA M-Pin protokollassa on asiakasohjelman ja palvelimen ulkopuolinen entiteetti, joka salaisuuden myöntämisen lisäksi vastaa käyttäjän rekisteröinnistä M-Pin:in palvelimelle. TA toimii M-Pin-protokollassa samoin, kuin julkisen sertifikaatin myöntävä osapuoli, kuten Verisign, julkisen avaimen infrastruktuurissa (PKI), ja myöntää siten palvelinkohtaisen salaisuuden myös M-Pin-palvelimille. (Scott, 2017.) Hyödyntämällä TA:ta salaisuuden myöntämisessä ja rekisteröinnin toteuttamisessa, voidaan Scottin (2017) mukaan välttää suuret vahingot yhden palvelimen vaarantuessa.

M-Pin-protokollassa todentamisen oleellinen vaihe on palvelimella käyttäjän syötteen validiteetin tarkistaminen. Protokollassa tämä suoritetaan parituksella (Scott, 2017). Paritus viittaa funktioon, jonka syötteenä on elementti ryhmistä $\mathbb{G}_1$ ja $\mathbb{G}_2$, sekä tulos pistetulo ryhmästä $\mathbb{G}_T$. Ryhmien elementit ovat elliptisen kuvaajan pisteitä, ja paritusfunktion palauttama pistetulo on arvo, joka voidaan esittää pisteenä toisella käyrällä, jota kutsutaan parituskäyräksi. M-Pin-protokollassa ryhmät ovat syklisiä, joiden järjestys on suuri alkuluku q. Ryhmät jaetaan käyttäjän salaisuuksiin $\mathbb{G}_1$ sekä palvelimen salaisuuksiin $\mathbb{G}_2$, joiden virittäjät ovat P ja Q, ja joissa vastaavasti osapuolten laskutoimitukset suoritetaan. Tämä viittaa siihen, että esimerkiksi käyttäjän identiteetistä (käyttäjätunnus, sähköposti tai muu identifioiva merkkijono) muodostetaan tiivistefunktiolla arvo $A \in \mathbb{G}_1$. M-Pin-protokollan konstruktiossa tiivistefunktio $H(.)$ on mallinnettu satunnaisoraakkelina (kts. luku 3.3.2), jonka tuottamat arvot ovat aidosti satunnaisia. (Scott, 2017.)

Protokollassa TA omaa salaisuuden s. Rekisteröintivaiheessa TA myöntää palvelimelle salaisuuden sQ, joka on johdettu kertomalla s ja yllä mainittu kiinteä virittäjä Q toisillansa. Käyttäjän identiteetistä ID johdetaan tiivistefunktiolla H salattu ja samalle kuvaajalle sijoitettu salaisuus sA, jossa $A = H(ID)$. Tämän

jälkeen käyttäjä valitsee PIN-koodin α, ja vähentää sen salaisuudestaan luodakseen tunnisteen $(s - \alpha)A$. Protokolla jatkuu seuraavasti (Scott, 2017):

- Käyttäjä generoi satunnaisarvon $x < q$ ja johtaa tästä $U = xA$.
- Käyttäjä lähettää palvelimelle ID, U
- Palvelin generoi satunnaishaasteen $y < q$ ja lähettää tämän käyttäjälle, minkä perusteella käyttäjä lähettää vastauksen $V = -(x + y)((s - \alpha)A + \alpha A)$
- Palvelin suorittaa tarkastuslaskennan $g = e(V, Q) \cdot e(U + yA, sQ)$, jossa e on paritusfunktio, ja g paritusfunktioiden pistetulo
- Mikäli paritusfunktion tulos $g \neq 1$, todentaminen epäonnistuu

Scott (2017) esittää artikkelissa myös M-Pin-protokollan olevan helposti muutettavissa digitaalisen allekirjoituksen protokollaksi muuttamalla palvelimen satunnaishaaste muotoon $y = H(m, U)$, jossa m on allekirjoitettava viesti. Edellä esitelty versio M-Pin-protokollasta on interaktiivinen käyttäjän ja palvelimen välillä sen sisältäen tiedonsiirtoa molempiin suuntiin. Scott (2017) esitti myös vaihtoehtoisen tavan muuttaa protokolla ei-interaktiiviseksi implementoimalla Fiat-Shamir-heuristiikan (Fiat & Shamir, 1987), jossa varmistajan lähettämä haaste korvataan todistajan itsensä generoimalla arvolla. M-Pin-protokolla voidaan muuttaa ei-interaktiiviseksi siten, että asiakasohjelma laskee satunnaishaasteen y aikaleiman ja käyttäjän salaisuuksien perusteella, ja lähettää tuloksen palvelimelle. Tämän jälkeen palvelin varmistaa aikaleiman tarkkuuden ennen protokollan loppuun saattamista. Lisäksi Scottin (2017) mukaan muodostettu ei-interaktiivinen versio protokollasta on tehokkaampi ja mahdollisesti turvallisempi vaihtoehto olemassa perinteisen käyttäjätunnus/salasana -menetelmän korvaamiseksi, sen vähentäessä asiakkaan ja palvelimen välisen tiedonsiirron määrää.

M-Pin-protokollan etuihin lukeutuu usean tekijän hyödyntäminen todentamisessa, mikä edistää turvallisuutta ja heikentää mahdollisuutta erinäisiin tietoturvariskeihin. Protokollassa tämä saavutetaan vaatimalla käyttäjältä tunnistautuessa PIN-koodi, sekä tunniste, joka johdetaan sekä käyttäjän identiteetistä että TA:n myöntämästä uniikista salaisuudesta. Lisäksi Scott (2017) mukaan M-Pin-protokollassa tunnistetiedot muodostavat tekijät voivat koostua varmenteen ja PIN-koodin lisäksi useista muistakin tekijöistä. M-Pin-protokollassa myös hyödynnetään nollatietotodistuksia, mikä sallii käyttäjän todentamisen palvelimelle paljastamatta identifioivaa salaisuutta sA. Nollatietotodistuksilla protokollassa saavutetaan suoja käyttäjän identiteetille jopa tilanteessa, jossa palvelin on vaarantunut. Protokollan turvallisuutta edistää puolestaan myös parituksen hyödyntäminen, sillä paritukseen perustuva salaus luo huomattavia haasteita hyökkääjälle väärentää todentamiseen vaadittavia tietoja.

Artikkelista esille noussut haaste on protokollan todistaminen turvalliseksi. M-Pin-protokollan turvallisuus pohjautuu osittain satunnaisoraakkelin olemassaoloon, joka ei tarjoa tasoltaan samoja turvallisuustakuita kuin perusteellisemmin turvalliseksi todistetut kryptografiset menetelmät. Verrattuna yksinkertaisempiin todentamisen protokolliin kuten luvussa 2 esiteltyyn rakenteeseen, on

M-Pin-protokolla huomattavasti haastavampi laskennallisesti esimerkiksi useiden paritusten vuoksi, mikä saattaa vaikuttaa järjestelmän skaalautuvuuteen.

5 JOHTOPÄÄTÖKSET

Tässä tutkielmassa käsiteltiin kirjallisuuskatsauksen menetelmin nollatietotodistusten hyödyntämistä käyttäjän todentamisessa verkkoympäristössä. Tutkielman tavoitteena oli selvittää nollatietotodistusten toimintaperiaatteita ja rakenteita todentamisen implementaatiossa kahden esimerkin avulla, jotka olivat Secure Remote Password -protokolla ja M-Pin-protokolla. Lisäksi tavoitteena oli tunnistaa nollatietotodistusten hyötyjä sekä mahdollisia haittoja todentamisessa. Nollatietotodistus on kryptografinen menetelmä, jonka kehittämisen motiivina oli luoda tapoja todistajalle todistaa väite varmentajalle paljastamatta prosessin aikana muuta kuin väitteen totuusarvon. Tätä kutsutaan myös kryptografian perimmäiseksi ongelmaksi. Verkkoympäristössä todistaja viittaa käyttäjän operoimaan asiakasohjelmaan, ja varmentaja verkkopalvelimeen. Nollatietotodistukset jakautuvat interaktiivisiin ja ei-interaktiivisiin menetelmiin sen mukaan, sisältyykö protokollaan osapuolten välistä molempiin suuntaan kulkevaa tiedonsiirtoa vai ei. Ei-interaktiivisessa nollatietoisuudessa molempiin suuntiin kulkeva tiedonsiirto korvataan lisätyillä laskennallisilla toimenpiteillä, jolloin todistettava turvallisuus kuitenkin muodostaa haasteita. Turvallisuustodisteiden saavuttamisessa yleistä on Random Oracle -mallin implementointi, jossa todentamisprotokollan satunnaisfunktioiden oletetaan olevan aidosti satunnaisia pseudosatunnaisuuden sijaan, joka voi luoda haavoittuvuuksia menetelmässä. Mallia on kuitenkin kritisoitu, sillä sen avulla saavutetut turvallisuustodisteet nähdään epämääräisinä.

SRP ja M-Pin ovat esimerkkejä tutkituista nollatietotodistuksia hyödyntävistä protokollista. SRP on laajasti käytössä oleva ja vakiintunut protokolla, ja M-Pin puolestaan uudempi protokolla, joka hyödyntää paritukseen perustuvaa salausta ja luotettua osapuolta. Nollatietotodistusten hyödyntäminen nostaa esille molemmissa protokollissa sekä hyötyjä että haasteita. Ensimmäiseksi, menetelmät eliminoivat tarpeen salattujen salasanojen säilytyksestä tietokannoissa tehden menetelmistä vastustuskykyisempiä erinäisille käyttäjätietovuotoja aiheuttaville hyökkäyksille. Toiseksi menetelmien tiedonsiirto on turvallisempaa kuin perinteisessä menetelmässä, sillä käyttäjän sensitiivisiä tunnistetietoja ei koskaan lähetetä verkkopalvelimelle, jolloin mahdollinen väliintulohyökkääjä saattaisi

kyetä esiintymään käyttäjänä ja urkkimaan tietoja siten aiheuttaen vahinkoa. M-Pin-protokollassa tämän lisäksi hyödynnetään todentamisessa useita eri tekijöitä. Tutkielmassa esitellyssä konstruktiossa tunnistetiedot muodostavat tekijät olivat PIN-koodi ja identiteetistä johdettu tunniste, mutta protokolla kykenee tukemaan useampia tekijöitä tunnistetietojen muodostamisessa. Lisäksi paritukseen perustuvan salauksen myötä M-Pin on hyvin vastustuskykyinen hyökkäyksille, joissa tunnistetiedot yritetään väärentää.

Kokonaisuudessaan nollatietotodistuksiin pohjautuvat todentamisen menetelmät kasvattavat huomattavasti verkkotodentamisen turvallisuutta ja luotettavuutta. Menetelmät sisältävät kuitenkin haasteita, kuten vaatimukset luotettavasta ja vahvasta satunnaisuuden implementoinnista sekä haastavista laskennallisista toimenpiteistä, mitkä tekevät implementaatioista vaativampia kuin yksinkertaisemmista todentamisen menetelmistä. Esimerkiksi SRP-protokollan turvallisuus perustuu haastavuuteen diskreetin logaritmin laskennassa sekä satojen numeroiden suuruisiin lukuihin. Vaikka SRP-protokolla estää tehokkaasti salasanaan kohdistuvat hyökkäykset lähetettäessä näitä palvelimelle, jää itsessään salasanan käytöstä haasteita ratkaistavaksi.

Jatkotutkimus on tarpeellista nollatietotodistusten kokonaisvaltaisen potentiaalin ymmärtämiseksi. Jatkotutkimuksessa voitaisiin esimerkiksi pureutua nollatietotodistuksia hyödyntävien menetelmien suuremman mittakaavan käyttöönottoon ja skaalautuvuuteen, sillä kirjallisuudessa käsitellään rajallisesti nollatietotodistusmenetelmien soveltuvuutta erinäisiin käyttötarkoituksiin ja eri tyypin tunnistetietoihin. Lisäksi jatkotutkimuksessa tulisi tutkia nollatietotodistusmenetelmien integrointia olemassa olevaan todentamisen infrastruktuuriin.

LÄHTEET

Bellare, M., & Rogaway, P. (1993). Random oracles are practical: A paradigm for designing efficient protocols. *Proceedings of the 1st ACM Conference on Computer and Communications Security - CCS '93*, 62–73.

Blum, M., Feldman, P., & Micali, S. (1988). Non-interactive zero-knowledge and its applications. *Proceedings of the twentieth annual ACM symposium on Theory of computing*, 103–112.

Blum, M., De Santis, A., Micali, S., & Persiano, G. (1991). Noninteractive Zero-Knowledge. *SIAM Journal on Computing*, 20(6), 35.

Bonneau, J., Herley, C., Oorschot, P. C. van, & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 IEEE Symposium on Security and Privacy, 553–567.

Canetti, R., Goldreich, O., & Halevi, S. (2004). The random oracle methodology, revisited. Journal of the ACM, 51(4), 557–594.

Dunphy, P., & Petitcolas, F. A. P. (2018). A First Look at Identity Management Schemes on the Blockchain. *IEEE Security Privacy*, 16(4), 20–29.

Fiat, A., & Shamir, A. (1987). How To Prove Yourself: Practical Solutions to Identification and Signature Problems. *Advances in Cryptology – CRYPTO' 86* (s. 186–194).

Garey, M. R., Johnson, D. S., & Stockmeyer, L. (1976). Some simplified NP-complete graph problems. *Theoretical Computer Science*, 1(3), 237–267.

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3), 690–728.

Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1), 1–32.

Goldreich, O. (2003). Foundations of Cryptography: Volume 1. *Cambridge University Press.*

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1), 186–208.

Grzonkowski, S., & Corcoran, P. (2014). A Practical Zero-Knowledge Proof Protocol for Web Applications. *Journal of Information Assurance & Security*, 9, 329– 343.

Ingram, D. (2018). Facebook says data leak hits 87 million users, widening scandal. Haettu 6.3.2022 osoitteesta *https://www.reuters.com/article/us-facebookprivacy/*

MDN. (2022). Math.random() - JavaScript. Haettu 29.5.2022 osoitteesta *https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Math/random*

NIST (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions *National Institute of Standards and Technology.*

Pathak, A., Patil, T., Pawar, S., Raut, P., & Khairnar, S. (2021). Secure Authentication using Zero Knowledge Proof. *2021 Asian Conference on Innovation in Technology*, 1–8.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). *A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication.* World Applied Sciences Journal, 19, 439–444.

Rivest, R. (1992). *RFC1321: The MD5 Message-Digest Algorithm*. https://www.ietf.org/rfc/rfc1321.txt

Scott, M. (2017). M-Pin: A Multi-Factor Zero Knowledge Authentication Protocol. https://miracl.com/assets/pdf-downloads/mpin4.pdf

Sherman, A. T., Lanus, E., Liskov, M., Zieglar, E., Chang, R., Golaszewski, E., Wnuk-Fink, R., Bonyadi, C. J., Yaksetig, M., & Blumenfeld, I. (2020). *Logic, Language, and Security: Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday* (s. 103–126).

Wu, T. (1998) The Secure Remote Password Protocol. *Proceedings of the Internet Society on Network and Distributed System Security*.

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, 99, 10205

Zhu, Y., Ma, L. and Zhang, J. (2015), An enhanced Kerberos protocol with noninteractive zero-knowledge proof. *Security Comm. Networks*, 8: 1108–1117.

Zheng, X., & Jin, J. (2012). Research for the application and safety of MD5 algorithm in password authentication. *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, 2216–2219.