Skupinski podpisi

Janoš Vidali, 63040303
Fakulteta za računalništvo in informatiko
Fakulteta za matematiko in fiziko
Univerza v Ljubljani

25. avgust 2008

Povzetek

Skupinski podpisi omogočajo podpisovanje posameznika v imenu skupine, pri čemer lahko identiteto podpisnika razkrije le nadzornik skupine. Podana sta formalni opis sheme za skupinske podpise in formalizacija varnostnih zahtev. Po pregledu osnovnih gradnikov shem sledita primera dveh shem za skupinske podpise, nato pa še pregled možnosti nadaljnega razvoja in uporabe shem za skupinske podpise.

Kazalo

1 Uvod

Koncept skupinskega podpisa sta podala David Chaum in Eugene van Heyst leta 1991 v [6]. Glavna ideja je podpisovanje v imenu skupine, kjer lahko zunanji preverjevalec za nek podpis ugotovi le, da ga je podpisal član skupine, identiteto podpisnika pa lahko razkrije le določena oseba - nadzornik skupine (*revocation manager*).

1.1 Motivacija in uporaba

Denimo, da imamo podjetje, v katerem lahko zaposleni podpisujejo dokumente v imenu podjetja, pri čemer nočemo, da stranke vedo, kdo je podpisal posamezen dokument. V primeru zlorabe s strani zaposlenega pa vseeno želimo, da ga lahko direktor identificira. Taki situaciji so skupinski podpisi pisani na kožo.

Še ena možnost uporabe skupinskih podpisov je pri spletnih licitacijah. Denimo, da se ponudnik zaveže, da bo za predmet dejansko plačal, če bo ponudil najvišjo ceno. Poleg tega želimo, da so ponudbe anonimne. Tako vzpostavimo skupino, katere člani so ponudniki, njen nadzornik pa je vodja licitacije. Vsaka ponudba se tako podpiše s skupinskim podpisom in anonimno objavi. Ko se licitacija konča, vodja odpre podpis najvišje ponudbe in tako izve, kdo jo je oddal.

Skupinski podpisi se uporabljajo tudi v druge namene, na primer za anonimno avtentikacijo [7], elektronski denar [11, 13] ali elektronske volitve [12, 10].

1.2 Definicija sheme za skupinske podpise

Shema za skupinske podpise je enajsterica

$$(\mathcal{M}, \mathcal{S}, \mathcal{K}_{gp}, \mathcal{K}_{gs}, \mathcal{K}_{us}, \mathcal{U}, \text{Gen}, \text{Issue}, \text{GSig}, \text{GVer}, \text{Open})$$

za katero velja:

- $\mathcal{M}$ je množica sporočil
- $\mathcal{S}$ je množica podpisov
- $\mathcal{K}_{gp}$ je množica javnih ključev skupine
- $\mathcal{K}_{gs}$ je množica tajnih ključev skupine
- $\mathcal{K}_{us}$ je množica članskih tajnih ključev
- $\mathcal{U}$ je množica potencialnih članov skupine
- $\text{Gen} : \emptyset \to \mathcal{K}_{gp} \times \mathcal{K}_{gs}$ je verjetnostni alogitem za generiranje ključev skupine
- $\text{Issue} : \mathcal{K}_{gp} \times \mathcal{K}_{gs} \times \mathcal{U} \to \mathcal{K}_{us}$ je algoritem za generiranje članskih ključev
- $\text{GSig} : \mathcal{K}_{gp} \times \mathcal{K}_{us} \times \mathcal{M} \to \mathcal{S}$ je algoritem za podpisovanje sporočila
- $\text{GVer} : \mathcal{K}_{gp} \times \mathcal{M} \times \mathcal{S} \to \{\top, \bot\}$ je algoritem za preverjanje podpisa
- $\text{Open} : \mathcal{K}_{gp} \times \mathcal{K}_{gs} \times \mathcal{PU} \times \mathcal{M} \times \mathcal{S} \to \mathcal{U} \cup \{\bot\}$ je algoritem za odpiranje podpisa

Označimo $(\mathit{gpk}, \mathit{gsk}) := \text{Gen}()$ in $\mathit{sk}_u := \text{Issue}(\mathit{gpk}, \mathit{gsk}, u)$ za nek $u \in U \subseteq \mathcal{U}$, kjer je U množica dejanskih članov skupine (takih, ki imajo svoj članski ključ, dobljen z Issue). Potem mora veljati še:

1. $\forall m \in \mathcal{M} : \sigma := \text{GSig}(\mathit{gpk}, \mathit{sk}_u, m) \Leftrightarrow \text{GVer}(\mathit{gpk}, m, \sigma) = \top \Leftrightarrow$
   $\Leftrightarrow \text{Open}(\mathit{gpk}, \mathit{gsk}, U, m, \sigma) = u$
2. $\forall m \in \mathcal{M}, \forall \sigma \in \mathcal{S} : \text{GVer}(\mathit{gpk}, m, \sigma) = \bot \Leftrightarrow \text{Open}(\mathit{gpk}, \mathit{gsk}, U, m, \sigma) = \bot$

Velja opomniti, da je algoritem za GSig lahko verjetnostni, tako da je potrebno točko 1. razumeti tako, da je σ le eden od *možnih* podpisov sporočila m, ki bi jih lahko izdal član skupine u - če tega ni nikoli storil, a preverjanje oziroma odpiranje podpisa uspeta, to pomeni, da je bil podpis uspešno ponarejen!

Pri podani formalni definiciji niso jasno razvidne posamezne vloge v skupini. V najbolj osnovnem primeru imamo le nadzornika skupine, ki ima tajni ključ skupine *gsk*, in člane skupine s svojimi tajnimi ključi sk_u. Pogosto se zahteva, da nimamo ene same avtoritete [2, 3], pač pa se ta razdeli, najpogosteje na izdajatelja (ki skrbi za članstvo v skupini) in odpiralca (ki lahko identificira podpisnika). V tem primeru se tudi tajni ključ skupine razdeli med avtoritete - vsak ima le del, ki ga potrebuje za svojo vlogo.

Še ena pomembna lastnost, ki ni razvidna iz definicije, je preverjanje pravilnosti izvajanja operacij. To velja tako za generiranje skupine, kot tudi za dodajanje člana v skupino in odpiranje podpisa. Pri prvih dveh operacijah sodelujejo le člani skupine in avtoritete, zato jih lahko izpeljemo kot protokole z dokazi brez razkritja znanja. Pri odpiranju podpisa pa želimo javnosti dokazati pravilnost odprtja, zato pridejo tukaj v upoštev neinteraktivni dokazi brez razkritja znanja.

Nazadnje povejmo še to, da je shema za skupinske podpise lahko *statična* ali *dinamična*. Pri statičnih shemah se skupina določi ob nastanku in je kasneje ni več mogoče spreminjati. Dinamične sheme ločimo na delno dinamične oziroma monotono rastoče sheme, kjer lahko člane v skupino le dodajamo, in popolnoma dinamične sheme, kjer lahko člane tudi izločimo iz skupine.

2 Varnostne zahteve

Da bo uporaba skupinskih podpisov utemeljena, morajo ustrezati določenim varnostnim zahtevam. Nekatere sledijo že iz definicije skupinskega podpisa, druge pa so bile naknadno dodane. Ker pa so te zahteve podane neformalno, bomo predstavili še njihovo formalizacijo iz [1] in [2].

2.1 Neformalne varnostne zahteve

Že iz same ideje skupinskih podpisov sledi zahteva o **anonimnosti** (*anonymity*): brez zasebnega ključa nadzornika skupine ni mogoče identificirati podpisnika. Iz definicije sledi tudi zahteva o **sledljivosti** (*traceability*), ki pravi, da lahko nadzornik skupine identificira avtorja vsakega veljavnega skupinskega podpisa. Že iz navadnih digitalnih podpisov pa imamo zahtevo o **neponaredljivosti** (*unforgeability*), torej da brez zasebnega ključa člana skupine ni mogoče ponarediti veljavnega skupinskega podpisa.

Zaželena lastnost sheme za skupinske podpise je tudi **odpornost proti koalicijam** (*coalition resistance*) - nobena koalicija članov skupine in njenega nadzornika ne more ponarediti skupinskega podpisa nekega člana skupine, ki ni del koalicije. Poseben primer te zahteve, ko je koalicija sestavljena iz enega samega člana (*exculpability*), bi lahko umestili tudi med osnovne zahteve. Drugi poseben primer imamo, ko koalicijo sestavljajo nadzornik in vsi člani skupine, z izjemo enega, katerega podpis se poskuša ponarediti (*framing*).

Zadnja zahteva, ki pa ni univerzalna, je **nepovezljivost** (*unlinkability*). Ta pravi, da brez zasebnega ključa nadzornika skupine za dva veljavna skupinska podpisa ni mogoče povedati, ali prihajata od istega člana. Ta lastnost je sicer ponavadi zaželena, v nekaterih primerih, kot so elektronske volitve, pa temu ni tako - takrat namreč želimo vedeti, ali ni morda kdo glasoval večkrat!

2.2 Formalizacija varnostnih zahtev

Vse navedene neformalne zahteve je mogoče formalizirati v dve zahtevi pri statičnih skupinah [1] oziroma tri zahteve pri dinamičnih skupinah [2]. Preden si jih pogledamo, definirajmo zanemarljivo funkcijo.

Def. Funkcija $f : \mathbb{N} \to \mathbb{R}$ je *zanemarljiva*, če za vsak neničelni polinom p obstaja tak m, da za vsak $n > m$ velja $|f(n)| < \frac{1}{|p(n)|}$.

V sledečih varnostnih zahtevah, ki veljajo za dinamične skupine, bodo zanemarljive funkcije prednosti nasprotnika, njihov argument pa (implicitni) varnostni parameter k, ki določa npr. dolžino ključev, velikost podpisa ipd.

- **Anonimnost**. Shema za skupinske podpise je anonimna, če je prednost $\mathrm{Adv}_A^{\mathrm{anon}}$ polinomskega nasprotnika A zanemarljiva:

  $$\mathrm{Adv}_A^{\mathrm{anon}} = |\Pr(\mathrm{anon}_A^0 = 1) - \Pr(\mathrm{anon}_A^1 = 1)| < \epsilon$$

  anon_A^b pri $b \in \{0, 1\}$ je tukaj poskus, ki ga opravi nasprotnik A. Pri njem ima dostop do orakljev za identifikacijo podpisnika, za dodajanje članov v skupino in za spreminjanje podatkov o članih skupine, poleg tega pozna tudi vse njihove tajne ključe $\boldsymbol{sk}_u$ za $u \in U$. A si izbere sporočilo m ter člana i_0 in i_1, nato pa i_b izda podpis σ sporočila m. Poskus uspe in vrne 1, če lahko A v polinomskem času identificira i_b kot podpisnika sporočila, brez da bi poklical oraklja za identifikacijo podpisnika na m in σ. A pri tem ne pozna vrednosti b vnaprej.

- **Sledljivost**. Shema za skupinske podpise je sledljiva, če je prednost $\mathrm{Adv}_A^{\mathrm{trace}}$ polinomskega nasprotnika A zanemarljiva:

  $$\mathrm{Adv}_A^{\mathrm{trace}} = \Pr(\mathrm{trace}_A = 1) < \epsilon$$

  trace_A je tukaj poskus, ki ga opravi nasprotnik A. Pri njem ima dostop do orakljev za dodajanje članov v skupino in za branje podatkov o članih skupine, poleg tega pa pozna tudi vse njihove tajne ključe $\boldsymbol{sk}_u$ za $u \in U$ in tajni ključ nadzornika skupine za identifikacijo podpisnika $\boldsymbol{gsk}$. A si izbere sporočilo m in poskuša ponarediti njegov podpis σ. Poskus uspe in vrne 1, če je podpis veljaven (torej $\mathrm{GVer}(\boldsymbol{gpk}, m, \sigma) = \top$), toda bodisi ni mogoče identificirati podpisnika

(Open(gpk, gsk, U, m, σ) $= \perp$), ali pa za identificiranega podpisnika ne obstaja veljaven dokaz.

- **Nepodtakljivost**. Shema za skupinske podpise je nepodtakljiva, če je prednost $\mathrm{Adv}_A^{\mathrm{nf}}$ polinomskega nasprotnika A zanemarljiva:

$$\mathrm{Adv}_A^{\mathrm{nf}} = \Pr(\mathrm{nf}_A = 1) < \epsilon$$

  nf_A je tukaj poskus, ki ga opravi nasprotnik A. Pri njem ima dostop do orakljev za podpisovanje z zasebnimi ključi članov skupine, za dodajanje članov v skupino in za spreminjanje podatkov o članih skupine, poleg tega pa pozna tajne ključe sk_u za podmnožico članov $u \in \mathcal{C}$ in tajni ključ nadzornika skupine za identifikacijo podpisnika gsk. A si izbere sporočilo m ter poskuša ponarediti njegov podpis σ in dokaz, da je podpisnik član skupine $i \notin \mathcal{C}$. Poskus uspe in vrne 1, če je podpis veljaven, dokaz pravilen in orakelj za podpisovanje ni bil poklican za sporočilo m in člana skupine i.

V primeru statičnih skupin orakljev za dodajanje članov v skupino in za spreminjanje podatkov o članih ni, tako da se v tem primeru sledljivost in nepodtakljivost združita v eno samo varnostno zahtevo - polno sledljivost. Analogno tudi zahtevo o anonimnosti v tem primeru imenujemo polna anonimnost.

2.3 Razmerja med neformalnimi in formaliziranimi zahtevami

Dokazali bomo, da formalizirane zahteve popolnoma pokrijejo neformalne zahteve.

- Anonimnost: Če bi lahko nasprotnik A z znatno zanesljivostjo identificiral podpisnika, potem bi poskusa anon_A^0 in anon_A^1 uspevala z znatno verjetnostjo, torej shema ne bi bila (polno) anonimna.

- Sledljivost: Če bi lahko nasprotnik A z znatno zanesljivostjo ponaredil veljaven podpis, za katerega ne bi bilo mogoče ugotoviti podpisnika, potem bi poskus trace_A uspel z znatno verjetnostjo in shema ne bi bila (polno) sledljiva.

- Neponaredljivost: Če bi lahko nasprotnik A z znatno zanesljivostjo ponaredil podpis člana skupine u, za katerega ne pozna zasebnega ključa, potem bi poskus nf_A uspel z znatno verjetnostjo, saj bi lahko s pomočjo ključa nadzornika skupine tvoril tudi dokaz, da je podpisnik član u. Shema tako ne bi bila nepodtakljiva.

- Odpornost proti koalicijam: Podobno kot neponaredljivost, le da tukaj poznamo še nekatere ostale zasebne ključe, ki pa so že vključeni pri nf_A.

- Nepovezljivost: Če bi lahko nasprotnik A za dva različna podpisa z znatno zanesljivostjo povedal, ali je njun avtor isti, bi lahko pri poskusu anon_A^b storil sledeče: izbral bi člana skupine i_0 in i_1, nato pa bi s tajnim ključem enega izmed njih izdal podpis σ' izbranega sporočila. Za podpis σ sporočila m, ki ga je izdal i_b, bi nato A ugotovil, ali prihaja od istega člana kot σ'. Poskus anon_A^b bi tako uspel z znatno verjetnostjo in shema ne bi bila (polno) anonimna.

3 Osnovni gradniki shem

Kakor bomo videli v naslednjem poglavju, sheme za skupinske podpise sestavljajo različni kriptografski primitivi. Najprej si bomo pogledali računske modele in nekatere predpostavke o računski zahtevnosti, uporabljene pri shemah za skupinske podpise, nato pa še splošne predpostavke za gradnike in nekaj primerov.

3.1 Računski modeli

Osnovni model, ki ga ponavadi privzamemo v kriptografiji, je **standardni model**. Pri njem predpostavljamo, da je nasprotnik omejen le s časom in računsko močjo, ki ju ima na voljo. Shema je varna v standardnem modelu, če njeno varnost lahko dokažemo le s predpostavkami o računski zahtevnosti.

Ker je dokaze v standardnem modelu pogosto težko najti, si zato pomagamo tako, da nadomestimo določene kriptografske primitive z njihovimi idealiziranimi različicami. Tipičen primer takega modela je **model z naključnim orakljem**. Tukaj namesto zgoščevalnih funkcij uporabimo naključnega oraklja (*random oracle*) - funkcijo, ki vrača naključen izhod, vendar je ta izhod pri istem vhodu vedno enak. Čeprav je bilo dokazano, da obstajajo sheme, ki so varne v modelu z naključnim orakljem, a se dajo trivialno razbiti v standardnem modelu [5], velja prepričanje, da to ne velja za sheme, ki so dejansko uporabne.

Še en model, ki se uporablja predvsem pri neinteraktivnih dokazih brez razkritja znanja, je **model s skupnim referenčnim nizom**. Pri njem predpostavljamo, da imajo vsi dostop do skupnega niza z (*common reference string*), ki je bil izbran po neki določeni distribuciji. Shema, ki je varna po tem modelu, je varna tudi v standardnem modelu, če se niz z izbere pravično, neodvisno od vseh vpletenih.

3.2 Predpostavke o računski zahtevnosti

Kakor pri večini javne kriptografije, ki se dandanes uporablja, tudi varnost večine shem za skupinske podpise temelji na predpostavkah o zahtevnosti problema razcepa števil in problema diskretnega logaritma oziroma sorodnih problemov. Opisali bomo nekaj takih, ki so uporabljenih pri shemah, predstavljenih v naslednjem poglavju.

- **Krepka RSA predpostavka**. Ta predpostavka temelji na krepkem RSA problemu, katerege cilj je za dano grupo G in njen element z najti tak par $(u, e) \in G \times (\mathbb{N} \setminus \{1\})$, da velja $u^e = z$. Predpostavka pravi, da obstaja verjetnostni algoritem K, tako da je za vsak polinomski verjetnostni algoritem A sledeča verjetnost zanemarljiva glede na red velikosti generirane grupe:

  $$\Pr\left(z = u^e \wedge e > 1 \mid (G, z) := K(), (u, e) := A(G, z)\right) < \epsilon$$

  V [3] je uporabljena varianta krepke RSA predpostavke, pri kateri omejimo možne vrednosti e na nek interval oblike $\left[2^a - 2^b .. 2^a + 2^b\right]$ pri $b < a < \ell_g$, kjer je ℓ_g dolžina reda grupe G.

- **Diffie-Hellmanova odločitvena predpostavka**. Naj bo G grupa in n deljitelj njenega reda. Označimo z $\mathcal{DH}(G)$ množico četveric (g_1, g_2, y_1, y_2), za katere velja $\mathrm{ord}(g_1) = \mathrm{ord}(g_2) = n$ in $\log_{g_1} y_1 = \log_{g_2} y_2$, s $\mathcal{Q}(G)$ pa množico takih četveric,

kjer velja le $\text{ord}(g_1) = \text{ord}(g_2) = \text{ord}(y_1) = \text{ord}(y_2) = n$. Predpostavka pravi, da obstaja verjetnostni algoritem K, tako da sta za vsak polinomski verjetnostni algoritem A sledeči verjetnosti računsko nerazločljivi, torej je njuna razlika zanemarljiva glede na red velikosti generirane grupe:

$$\Pr\left(a = 1 \mid G := K(), T \in \mathcal{DH}(G), a := A(T)\right)$$

$$\Pr\left(a = 1 \mid G := K(), T \in \mathcal{Q}(G), a := A(T)\right)$$

V obeh primerih je četverica T izbrana po uniformni distribuciji.

V [14] je uporabljena varianta Diffie-Hellmanove odločitvene predpostavke, ki jo imenujemo tridelna Diffie-Hellmanova odločitvena predpostavka. Pri njej imamo namesto četveric šesterice, saj dodamo še elementa y_3 in y_4. Pri šestericah iz $\mathcal{DH}(G)$ poleg $\text{ord}(g_1) = \text{ord}(g_2) = n$ velja še $\log_{g_1} y_4 = \log_{g_1} y_1 \log_{g_1} y_2 \log_{g_2} y_3$, pri $\mathcal{Q}(G)$ pa ima vseh šest elementov enak red n. V splošnem lahko g_1 in g_2 pripadata različnim grupam, pomembno je le, da sta istega reda. Če sta grupi ciklični s praštevilskim redom, potem lahko za g_1 in g_2 implicitno vzamemo kar njuna generatorja.

Velja opomniti, da Diffie-Hellmanova odločitvena predpostavka ne velja za vse grupe. Primer take grupe, da predpostavka ne velja, je $\mathbb{Z}^*_{pq}$, $p, q \in \mathbb{P}$. Tudi brez poznavanja faktorizacije pq lahko namreč Jacobijev simbol pove, da velja $\log_{g_1} y_1 \neq \log_{g_2} y_2$.

- q**-krepka Diffie-Hellmanova predpostavka**. Za vsako multiplikativno ciklično grupo G z generatorjem g reda $p \in \mathbb{P}$ in vsak polinomski verjetnostni algoritem A je sledeča verjetnost zanemarljiva glede na red velikosti grupe G:

$$\Pr\left(u = g^{(\gamma+e)^{-1}} \;\middle|\; \gamma \in \mathbb{Z}^*_p, (u, e) := A\left(g, g^{\gamma}, \ldots, g^{\gamma^q}\right)\right) < \epsilon$$

γ je tukaj izbran po uniformni distribuciji iz $\mathbb{Z}^*_p$.

3.3 Sheme za digitalne podpise

Prvi kriptografski primitiv, ki ga bomo predstavili, so sheme za digitalne podpise. Najpogosteje se navadni digitalni podpisi v shemah za skupinske podpise pojavljajo pri certifikatih o članstvu, lahko pa so tudi sestavni del samega skupinskega podpisa.

Da je uporaba sheme za digitalne podpise varna, mora biti neponaredljiva. To pomeni, da je prednost $\text{Adv}^{\text{unforg}}_A$ polinomskega nasprotnika A zanemarljiva:

$$\text{Adv}^{\text{unforg}}_A = \Pr(\text{unforg}_A = 1) < \epsilon$$

unforg_A je tukaj poskus, ki ga opravi nasprotnik A. Pri njem ima dostop do oraklja za podpisovanje z zasebnim ključem *sk*. A tega ključa nima, pač pa ima javni ključ *pk*, s katerim lahko preverja podpise. A si izbere sporočilo m in poskuša ponarediti njegov podpis σ. Poskus uspe in vrne 1, če je podpis veljaven in orakelj za podpisovanje ni bil poklican za sporočilo m.

3.4 Asimetrične šifrirne sheme

Asimetrične šifrirne sheme se v shemah za skupinske podpise uporabljajo predvsem za skrivanje identitete podpisnika. Identiteta je tako lahko zašifrirana z javnim ključem nadzornika skupine in se pri odpiranju podpisa odšifrira.

Da je uporaba asimetrične šifrirne sheme varna, mora zadostovati zahtevi o nerazločljivosti pri napadu z izbranim kriptogramom. To pomeni, da je prednost $\mathrm{Adv}_A^{\text{ind-cca}}$ polinomskega nasprotnika A zanemarljiva:

$$\mathrm{Adv}_A^{\text{ind-cca}} = |\Pr(\text{ind-cca}_A^0 = 1) - \Pr(\text{ind-cca}_A^1 = 1)| < \epsilon$$

ind-cca_A^b je tukaj poskus, ki ga opravi nasprotnik A. Pri njem ima dostop do oraklja za odšifriranje kriptogramov, šifriranih z javnim ključem pk, ki ga ima A. A izbere sporočili m_0 in m_1 in dobi kriptogram c, ki je zašifrirano sporočilo m_b. Poskus uspe in vrne 1, če lahko A v polinomskem času identificira m_b kot besedilo, ki ustreza kriptogramu c, brez da bi poklical oraklja za odšifriranje za kriptogram c. A pri tem ne pozna vrednosti b vnaprej.

3.5 Dokazi brez razkritja znanja

Zadnji primitiv, ki si ga bomo pogledali, so dokazi brez razkritja znanja. Čeprav ponavadi pod tem imenom mislimo na interaktivne protokole za dokazovanje, ki lahko pridejo prav tudi pri shemah za skupinske podpise (na primer pri pridruževanju skupini), pa se bomo tukaj osredotočili na neinteraktivne dokaze brez razkritja znanja, ki jim včasih pravimo tudi podpisi znanja (*signatures of knowledge*).

Neinteraktivni dokazi brez razkritja znanja niso mogoči v standardnem modelu [9], zato jih podajamo v modelu s skupnim referenčnim nizom. Zahtevi, da je skupni referenčni niz izbran neodvisno od vseh vpletenih, se lahko približamo tako, da zanj vzamemo kar sporočilo, ki ga podpisujemo. Tako lahko tudi kakršenkoli digitalni podpis razumemo kot neinteraktivni dokaz brez razkritja znanja o poznavanju tajnega ključa.

Neinteraktivni dokaz brez razkritja znanja označimo tako:

$$\pi = \text{SPK}\left\{(\alpha_1, \alpha_2, \ldots, \alpha_t) \mid P(x_1, x_2, \ldots, x_n, \alpha_1, \alpha_2, \ldots, \alpha_t)\right\}(m)$$

Tukaj so x_i, $i = 1, 2, \ldots, n$ javni parametri, α_j, $j = 1, 2, \ldots, t$ pa števila, za katera dokazujemo, da jih poznamo. Za slednja se v splošnem uporabljajo grške črke, za javne parametre pa latinske. P je predikat, ki mora veljati za znana in dokazovana števila. m je uporabljeni skupni referenčni niz. Opisali bomo nekaj primerov neinteraktivnih dokazov brez razkritja znanja, uporabljenih pri shemah za skupinske podpise, predstavljenih v naslednjem poglavju. Pri vseh primerih predpostavljamo, da imamo na voljo zgoščevalno funkcijo $\mathcal{H} : \{0,1\}^* \to \{0,1\}^k$. ℓ_g je dolžina reda grupe, v kateri računamo, $\epsilon > 1$ pa varnostni parameter.

- **Dokazovanje poznavanja diskretnega logaritma**.

  $$(c, s) = \text{SPK}\left\{(\alpha) \mid y = g^\alpha\right\}(m)$$

  $$c \in \{0,1\}^k, s \in \{-2^{\ell_g + k}, \ldots, 2^{\epsilon(\ell_g + k)}\}$$

  Če velja $c = \mathcal{H}(g \| y \| g^s y^c \| m)$, je (c, s) dokaz brez razkritja znanja, da izdajatelj dokaza pozna $\alpha = \log_g y$. Tedaj lahko namreč stori sledeče:

1. Naključno izbere $r \in \{0,1\}^{\epsilon(\ell_g+k)}$
2. Izračuna $c := \mathcal{H}(g\|y\|g^r\|m)$
3. Izračuna $s := r - c\alpha$ v $\mathbb{Z}$

Preverjanje dokaza je ekvivalentno preverjanju, ali (c,s) ustreza definiciji.

Dokaz je mogoče posplošiti na dokazovanje poznavanja takih $\alpha_1,\ldots,\alpha_n$, da velja $y = \prod_{i=1}^n g_i^{\alpha_i}$. V tem primeru namesto enega naključno izberemo n števil $r_1,\ldots,r_n \in \{0,1\}^{\epsilon(\ell_g+k)}$, v c vključimo vse g_i, $i = 1,\ldots,n$, namesto s pa imamo $s_i = r_i - c\alpha_i$ za $i = 1,\ldots,n$.

- **Dokazovanje poznavanja kvocienta dveh diskretnih logaritmov**.

$$(c,s_1,s_2) = \text{SPK}\left\{(\alpha,\beta) \;\middle|\; y_1^\alpha = g^\beta \wedge y_2 = h^\beta\right\}(m)$$

$$c \in \{0,1\}^k, s_1 \in \{-2^{\ell_g+k},\ldots,2^{\epsilon(\ell_g+k)}\}, s_2 \in \{-2^{\ell_g+k},\ldots,2^{\epsilon(\ell_g+k)}\}$$

Če velja $c = \mathcal{H}(g\|h\|y_1\|y_2\|y_1^c g^{s_1}\|y_2^c h^{s_2}\|m)$, je (c,s_1,s_2) dokaz brez razkritja znanja, da izdajatelj pozna $\beta = \log_h y_2$ in $\alpha = \beta(\log_g y_1)^{-1}$. Tedaj lahko dokaz izračuna po sledečem postopku:

1. Naključno izbere $r_1, r_2 \in \{0,1\}^{\epsilon(\ell_g+k)}$
2. Izračuna $c := \mathcal{H}(g\|h\|y_1\|y_2\|g^{r_1}\|h^{r_2}\|m)$
3. Izračuna $s_1 := r_1 - c(\beta\alpha^{-1})$ v $\mathbb{Z}$
4. Izračuna $s_2 := r_2 - c\beta$ v $\mathbb{Z}$

Pri tretji točki se $\beta\alpha^{-1}$ izračuna v grupi potenc, nato pa rezultat interpretira kot celo število in nadaljuje računanje v $\mathbb{Z}$.

Pri posebnem primeru, ko je znano, da je $\alpha = 1$ in dokazujemo le ekvivalenco dveh diskretnih logaritmov, lahko uporabimo $r_1 = r_2 = r$ in tako $s_1 = s_2 = s$. Dokaz je tedaj (c,s).

- **Dokazovanje intervala, v katerem leži diskretni logaritem**.

$$(c,s) = \text{SPK}\left\{(\alpha) \;\middle|\; y = g^\alpha \wedge 2^a - 2^{\epsilon(b+k)+1} < \alpha < 2^a + 2^{\epsilon(b+k)+1}\right\}(m)$$

$$c \in \{0,1\}^k, s \in \{-2^{b+k},\ldots,2^{\epsilon(b+k)}\}$$

Če velja $c = \mathcal{H}(g\|y\|g^{s-c2^a}y^c\|m)$ in $\epsilon(b+k)$, je (c,s) dokaz brez razkritja znanja, da izdajatelj pozna $\alpha = \log_g y$, ki leži na intervalu med $2^a - 2^{\epsilon(b+k)+1}$ in $2^a + 2^{\epsilon(b+k)+1}$. Dokaz brez razkritja znanja lahko izračuna tako:

1. Naključno izbere $r \in \{0,1\}^{\epsilon(b+k)}$
2. Izračuna $c := \mathcal{H}(g\|y\|g^r\|m)$
3. Izračuna $s := r - c(\alpha - 2^a)$ v $\mathbb{Z}$

Da je to dokaz o poznavanju diskretnega logaritma, se prepričamo na enak način kot pri prvem predstavljenem dokazu brez razkritja znanja. Če velja $\alpha \leq 2^a - 2^{\epsilon(b+k)+1}$, potem z visoko verjetnostjo velja $s > 2^{\epsilon(b+k)}$, če pa je $\alpha \geq 2^a + 2^{\epsilon(b+k)+1}$, pa z visoko verjetnostjo velja $s < 2^{b+k}$. Če pa α res leži v dokazovanem intervalu, pa tudi s leži med -2^{b+k} in $2^{\epsilon(b+k)}$. Verjetnost, da dokaz uspe za α izven zahtevanega intervala je večja, če α leži le malo izven intervala.

- **Dokazovanje, da je število produkt dveh praštevil**.

$$(y, r) = \text{SPK}\left\{(\alpha, \beta) \mid n = \alpha\beta \wedge \alpha, \beta \in \mathbb{P} \wedge \alpha, \beta \not\equiv 1(\text{mod}8) \wedge \alpha \not\equiv \beta(\text{mod}8)\right\}(x)$$

$$y, r, x \in \mathbb{Z}_n^*$$

Če velja $y^n \equiv x \pmod{n}$ in $r^2 \bmod n \in \{\pm x \bmod n, \pm 2x \bmod n\}$, je (y, r) dokaz brez razkritja znanja, da izdajatelj pozna taka $\alpha, \beta \in \mathbb{P}$, da velja $n = \alpha\beta$, $\alpha, \beta \not\equiv 1 \pmod{8}$, $\alpha \not\equiv \beta \pmod{8}$. V tem primeru lahko dokaz izračuna tako:

1. Izračuna $m := n^{-1} \bmod (\alpha - 1)(\beta - 1)$
2. Izračuna $y := x^m \bmod n$
3. Izračuna $r := \sqrt{s} \bmod n$ za $s \in \{\pm x, \pm 2x\}$

S preverjanjem y se prepričamo, da je n produkt samih različnih praštevil. V nasprotnem primeru namreč velja $\gcd(n, \varphi(n)) = d > 1$ in verjetnost, da velja $x \equiv y^n \pmod{n}$ za nek y je največ $\frac{1}{d}$.

Pravilno izračunan r je dokaz, da je n produkt dveh potenc praštevil. Ker velja $\left(\frac{-1}{\alpha}\right) = 1 \Leftrightarrow \alpha \equiv 1 \pmod{4}$ in $\left(\frac{2}{\alpha}\right) = 1 \Leftrightarrow \alpha \equiv \pm 1 \pmod{8}$ (in podobno za β), je pri $\alpha, \beta \not\equiv 1 \pmod{8}$ in $\alpha \not\equiv \beta \pmod{8}$ natanko eden od $\pm x$, $\pm 2x$ kvadratni ostanek in izdajatelj dokaza lahko zanj izračuna kvadratni koren. Če ta pogoj ne velja, je verjetnost, da je v množici $\{\pm x, \pm 2x\}$ kak kvadratni ostanek, največ $\frac{1}{2}$: če je n produkt več kot dveh različnih praštevil, potem je naključni element $\mathbb{Z}_n^*$ kvadratni ostanek z verjetnostjo največ $\frac{1}{8}$, torej je v množici kvadratni ostanek z verjetnostjo največ $\frac{1}{2}$. Če pa velja $\alpha \equiv 1 \pmod{8}$, $\beta \equiv 1 \pmod{8}$ ali $\alpha \equiv \beta \pmod{8}$, pa je eden od -1, 2 in -2 kvadratni ostanek in tako je v množici kak kvadratni ostanek z verjetnostjo $\frac{1}{2}$ (če pa velja $\alpha \equiv \beta \equiv 1 \pmod{8}$, so -1, 2 in -2 vsi kvadratni ostanki in zato je verjetnost le $\frac{1}{4}$).

Računanje kvadratnega korena ustreznega števila po modulu n je mogoče, če velja $\alpha \equiv \beta \equiv 3 \pmod{4}$. Izdajatelj izračuna kvadratni koren za tisto število $z \in \{\pm x, \pm 2x\}$, za katerega velja $\left(\frac{z}{\alpha}\right) = \left(\frac{z}{\beta}\right) = 1$.

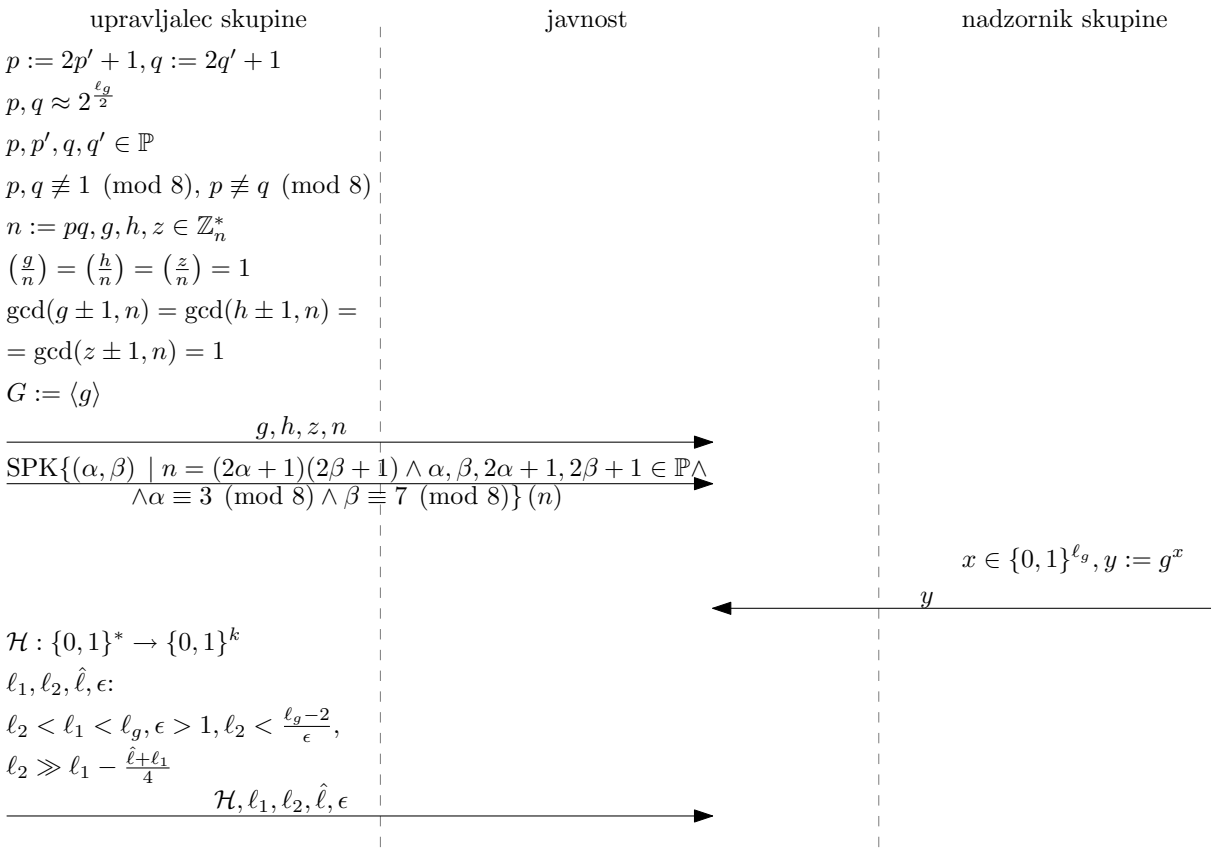
Dokaz je mogoče razširiti na dokaz, da je praštevilo produkt dveh kvazi-varnih (tipa $p = 2q^e + 1$, $p, q \in \mathbb{P}$) [8] oziroma varnih praštevil (tipa $p = 2q + 1$, $p, q \in \mathbb{P}$) [4].

4 Primeri shem za skupinske podpise

Predstavili bomo dve shemi za skupinske podpise: Camenisch-Michelsovo in Sujing-Dongdaijevo shemo. Prva je delno dinamična shema po definiciji iz uvoda, medtem ko bi za drugo shemo lahko rekli, da je monotono padajoča: število članov skupine se fiksira na začetku, kasneje pa se lahko le brišejo iz skupine.

4.1 Camenisch-Michelsova shema

Camenisch-Michelsova shema, predstavljena v [3], temelji na varianti krepke RSA predpostavke, problemu diskretnega logaritma in Diffie-Hellmanovi odločitveni predpostavki.

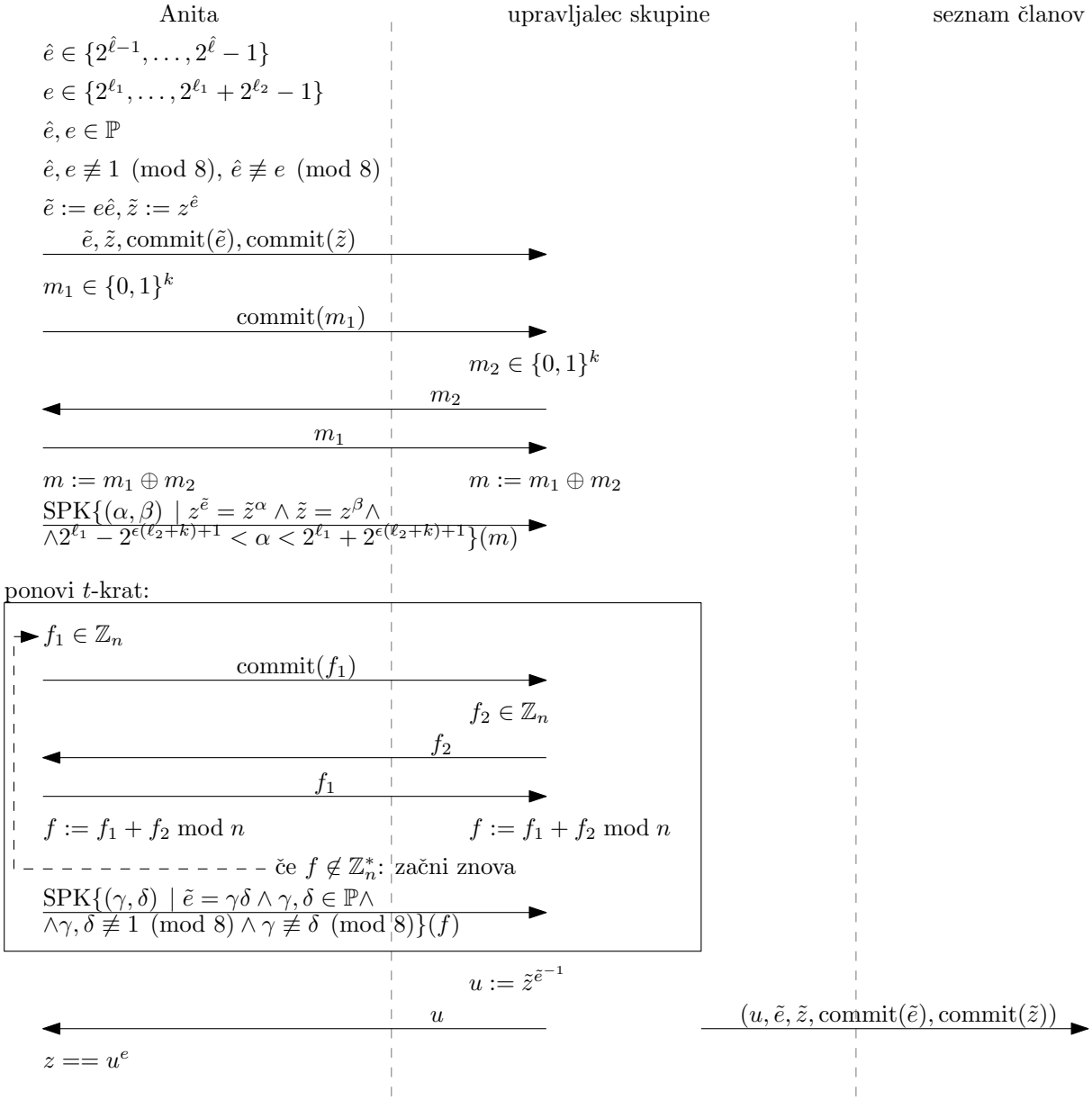


Slika 1: Protokol za vzpostavitev Camenisch-Michelsove sheme

Avtoriteta se pri tej shemi razdeli na dva dela - upravljalca skupine in nadzornika skupine. Prvi skrbi za vzpostavitev skupine in dodajanje članov vanjo, drugi pa za odpiranje podpisov. Pri vzpostavitvi upravljalec skupine izbere grupo $G = \langle g \rangle$ ter taka naključna elementa grupe z in h, tako da sta istega reda kot g. Ta red je približno 2^{ℓ_g} in ne sme biti praštevilo, kar mora upravljalec skupine tudi dokazati. V grupi G mora biti problem diskretnega logaritma težek, prav tako mora zanjo veljati krepka Diffie-Hellmanova predpostavka.

Možna izbira grupe G je podgrupa v $\mathbb{Z}_n^*$, tako da velja $n = pq$, kjer sta p in q varni praštevili, torej velja $p = 2p' + 1$, $q = 2q' + 1$, $p, p', q, q' \in \mathbb{P}$. p in q sta približno $2^{\frac{\ell_g}{2}}$, poleg tega mora veljati še $p, q \not\equiv 1 \pmod 8$, $p \not\equiv q \pmod 8$ in $\left(\frac{g}{n}\right) = 1$, tako da za grupo velja Diffie-Hellmanova odločitvena predpostavka. Nadzornik skupine objavi n, s čimer opiše grupo in tako pokaže tudi njen približen red. Da je n res produkt dveh varnih praštevil, se uporabi metoda iz [4]. Da so redi elementov g, z in h vsaj $p'q'$, lahko vsakdo preveri tako, da preveri $g \not\equiv \pm 1 \pmod n$, $\gcd(g \pm 1, n) = 1$ in $\left(\frac{g}{n}\right) = 1$ (in podobno še za z, h). Ker grupa $\mathbb{Z}_n^*$ ni ciklična, je maksimalen red elementa $2p'q'$, torej imajo kvadratni ostanki red največ $p'q'$.

Ko se izbere grupa in dokaže njena primernost, nadzornik skupine naključno izbere $x \in \{0, \ldots, 2^{\ell_g} - 1\}$, ki bo služil kot tajni ključ za odpiranje podpisov. Nato izračuna $y = g^x$ in ga objavi kot javni ključ skupine. Nazadnje upravljalec skupine izbere še zgoščevalno funkcijo $\mathcal{H} : \{0,1\}^* \to \{0,1\}^k$ in varnostne parametre ℓ_1, ℓ_2, $\hat{\ell}$, ϵ, tako da velja $\ell_2 < \ell_1 < \ell_g$, $\epsilon > 1$, $\ell_2 < \frac{\ell_g - 2}{\epsilon}$ in $\ell_2 \gg \frac{\hat{\ell} + \ell_1}{4}$.



Slika 2: Protokol za pridruževanje skupini

4.1.1 Pridruževanje skupini

Denimo, da se želi Anita pridružiti skupini. Tedaj naključno izbere praštevili $\hat{e} \in \{2^{\hat{\ell}-1}, \ldots, 2^{\hat{\ell}} - 1\}$ in $e \in \{2^{\ell_1}, \ldots, 2^{\ell_1} + 2^{\ell_2} - 1\}$, tako da velja $\hat{e}, e \not\equiv 1 \pmod 8$ in $\hat{e} \not\equiv e \pmod 8$. Nato izračuna $\tilde{e} := e\hat{e}$ in $\tilde{z} := z^{\hat{e}}$, zapriseže vrednosti $\tilde{e}$ in $\tilde{z}$ (na primer tako, da ju podpiše z osebnim tajnim ključem) ter $\tilde{e}$, $\tilde{z}$ in zaprisegi pošlje upravljalcu skupine. Da dokaže pravilnost poslanih podatkov, Anita in upravljalec skupine izvedeta protokol, ki ustreza sledečima dokazoma brez razkritja znanja:

$$\mathrm{SPK}\left\{(\alpha, \beta) \;\middle|\; z^{\tilde{e}} = \tilde{z}^{\alpha} \wedge \tilde{z} = z^{\beta} \wedge 2^{\ell_1} - 2^{\epsilon(\ell_2+k)+1} < \alpha < 2^{\ell_1} + 2^{\epsilon(\ell_2+k)+1}\right\}(m)$$

$$\mathrm{SPK}\left\{(\gamma, \delta) \mid \tilde{e} = \gamma\delta \wedge \gamma, \delta \in \mathbb{P} \wedge \gamma, \delta \not\equiv 1 \pmod 8 \wedge \gamma \not\equiv \delta \pmod 8\right\}(f)$$

Da bi spremenili neinteraktivni dokaz brez razkritja znanja v interaktivnega, Anita lahko prepusti izbiro m in f upravljalcu skupine, ali pa ju izbereta skupaj, tako da eden od njiju najprej naključno izbere npr. $m_1 \in \{0,1\}^k$ oziroma $f_1 \in \mathbb{Z}_n$ in pošlje drugemu zaprisego te vrednosti, nato pa drugi izbere $m_2 \in \{0,1\}^k$ oziroma $f_2 \in \mathbb{Z}_n$. Za tem se razkrije vrednost m_1 oziroma f_1 in se izračuna $m := m_1 \oplus m_2$ oziroma $f := f_1 + f_2 \bmod n$. Pri tem mora veljati $f \in \mathbb{Z}_n^*$, tako da se lahko zgodi, da je treba izbiro f ponoviti. Sicer pa je potrebno sam protokol za dokazovanje produkta dveh praštevil večkrat ponoviti, saj lahko pri posamezni ponovitvi verjetnost prevare doseže $\frac{1}{2}$. Če protokol ponovimo t-krat, je verjetnost prevare kvečjemu $1 - 2^{-t}$.

Ko se upravljalec skupine prepriča, da je Anita izbrala $\tilde{e}$ in $\tilde{z}$ na pravilen način, izračuna Anitin javni certifikat članstva $u := \tilde{z}^{\tilde{e}^{-1}}$. Anita preveri, da velja $\tilde{z} = u^{\tilde{e}}$, kar je ekvivalentno $z = u^e$. Upravljalec skupine doda $(u, \tilde{e}, \tilde{z})$ in zaprisegi na seznam članov skupine, Anita pa shrani e kot svoj tajni ključ za podpisovanje v imenu skupine.

4.1.2 Podpisovanje in preverjanje podpisa

Skupinski podpis sporočila m po Camenisch-Michelsovi shemi je neinteraktiven dokaz brez razkritja znanja:

$$(c, s_1, s_2, s_3, a, b, d) = \mathrm{SPK}\{(\eta, \theta, \xi) \mid zy^\theta = b^\eta \wedge a^\eta = g^\theta \wedge a = g^\xi \wedge d = g^\eta h^\xi \wedge$$

$$\wedge 2^{\ell_1} - 2^{\epsilon(\ell_2+k)+1} < \eta < 2^{\ell_1} + 2^{\epsilon(\ell_2+k)+1}\}\,(m)$$

Če hoče Anita podpisati sporočilo m v imenu skupine, stori sledeče:

1. Naključno izbere $w \in \{0,1\}^{\ell_g}$
2. Izračuna $a := g^w$, $b := uy^w$ in $d := g^e h^w$
3. Naključno izbere $r_1 \in \{0,1\}^{\epsilon(\ell_2+k)}$, $r_2 \in \{0,1\}^{\epsilon(\ell_g+\ell_1+k)}$ in $r_3 \in \{0,1\}^{\epsilon(\ell_g+k)}$
4. Izračuna $t_1 := b^{r_1} y^{-r_2}$, $t_2 := a^{r_1} g^{-r_2}$, $t_3 := g^{r_3}$, $t_4 := g^{r_1} h^{r_3}$
5. Izračuna $c := \mathcal{H}(g \| h \| y \| z \| a \| b \| d \| t_1 \| t_2 | t_3 \| t_4 \| m)$
6. Izračuna $s_1 := r_1 - c(e - 2^{\ell_1})$, $s_2 := r_2 - cew$ in $s_3 := r_3 - cw$ v $\mathbb{Z}$
7. Izda podpis $\sigma := (c, s_1, s_2, s_3, a, b, d)$

Če želi Boris preveriti, da je $\sigma = (c, s_1, s_2, s_3, a, b, d)$ veljaven skupinski podpis sporočila m, najprej preveri, ali komponente podpisa pripadajo ustreznim množicam:

$$c \in \{0,1\}^k, s_1 \in \{-2^{\ell_2+k}, \ldots, 2^{\epsilon(\ell_2+k)}\}, s_2 \in \{-2^{\ell_g+\ell_1+k}, \ldots, 2^{\epsilon(\ell_g+\ell_1+k)}\},$$

$$s_3 \in \{-2^{\ell_g+k}, \ldots, 2^{\epsilon(\ell_g+k)}\}, a, b, d \in G$$

Nato izračuna $t_1' := z^c b^{s_1 - c2^{\ell_1}} y^{-s_2}$, $t_2' := a^{s_1 - c2^{\ell_1}} g^{-s2}$, $t_3 := a^c g^{s_3}$ in $t_4' := d^c g^{s_1 - c2^{\ell_1}} h^{s_3}$ ter preveri, da velja

$$c = \mathcal{H}(g \| h \| y \| z \| a \| b \| d \| t_1' \| t_2' | t_3' \| t_4' \| m)$$

.

Prepričajmo se, da je preverjanje podpisa pravilno izvedeno. Ob predpostavki, da je zgoščevalna funkcija $\mathcal{H}$ brez trkov zadošča preveriti, da velja $t_i = t'_i$ za $i = 1, 2, 3, 4$:

$$t'_1 = z^c b^{s_1 - c2^{\ell_1} y^{-s_2}} = z^c b^{r_1 - ce} y^{-r_2 + cew} = u^{ce} b^{r_1} u^{-ce} y^{-cew} y^{-r_2 + cew} = b^{r_1} y^{-r_2} = t_1$$

$$t'_2 = a^{s_1 - c2^{\ell_1}} g^{-s2} = a^{r_1 - ce} g^{-r_2 + cew} = a^{r_1} g^{cew} g^{-r_2 + cew} = a^{r_1} g^{-r_2} = t_2$$

$$t'_3 = a^c g^{s_3} = g^{cw} g^{r_3 - cw} = g^{r_3} = t_3$$

$$t'_4 = d^c g^{s_1 - c2^{\ell_1}} h^{s_3} = g^{ce} h^{cw} g^{r_1 - ce} h^{r_3 - cw} = g^{r_1} h^{r_3} = t_4$$

4.1.3 Odpiranje podpisa

Da bi nadzornik skupine razkril podpisnika veljavnega skupinskega podpisa $\sigma = (c, s_1, s_2, s_3, a, b, d)$, izračuna $u' := ba^{-x}$, najde člana skupine s certifikatom članstva u' ter razkrije njegovo identiteto, $\tilde{e}$, $\tilde{z}$ in zaprisegi zanju. Kot dokaz, da je razkritje podpisnika pravilno, izda še podpis znanja:

$$P = \text{SPK}\left\{(\alpha) \;\middle|\; y = g^\alpha \wedge bu'^{-1} = a^\alpha \right\}(u' \| \sigma \| m)$$

Prepričajmo se, da je razkritje certifikata članstva pravilno:

$$u' = ba^{-x} = uy^w g^{-xw} = uy^w y^{-w} = u$$

Boris se s preverjanjem podpisa znanja prepriča, da ga je izdal nekdo, ki pozna x, torej nadzornik skupine, in da je razkriti certifikat članstva pravi. Identiteto podpisnika Boris preveri tako, da preveri, ali je zaprisegi za $\tilde{e}$ in $\tilde{z}$ izdal razkriti podpisnik, pri čemer mora veljati $\tilde{z} = u'^{\tilde{e}}$.

4.1.4 Varnost sheme

Pogledali si bomo varnostno analizo sheme glede na formalizirane varnostne zahteve.

- **Anonimnost**. Denimo, da prednost $\text{Adv}_A^{\text{anon}}$ polinomskega nasprotnika A ni zanemarljiva, kar je ekvivalentno zahtevi, da je verjetnost, da poskus anon_A^b pri $b \in \{0, 1\}$ uspe, bistveno različna od $\frac{1}{2}$. Pri poskusu A izbere člana skupine u_0 in u_1, nato pa mu je dan podpis σ, ki ga izda član u_b. Poskus uspe, če je član u', za katerega A trdi, da je podpisnik, res podpisnik sporočila.

  Po predpostavki iz modela z naključnim orakljem je zgoščevalna funkcija $\mathcal{H}$ ekvivalentna naključni funkciji, zato A iz c, s_1, s_2, s_3 ne more dobiti nobene koristne informacije. Ker je $u' = u_b$ z verjetnostjo, bistveno različno od $\frac{1}{2}$, je tudi verjetnost, da je odločitev, ali velja $\log_g a = \log_y(bu'^{-1}) = \log_h(dg^{-e})$, bistveno različna od $\frac{1}{2}$, kar je v nasprotju z Diffie-Hellmanovo odločitveno predpostavko. Camenisch-Michelsova shema je torej anonimna.

- **Sledljivost**. Pri poskusu trace_A je cilj nasprotnika A izdelati tak veljaven skupinski podpis, za katerega ni mogoče ugotoviti podpisnika oziroma ugotovitve ni mogoče dokazati. To lahko doseže le tako, da ponaredi zasebni ključ e in ustrezni certifikat članstva u, brez da bi izvedel protokol za pridruževanje skupini - veljaven podpis je namreč dokaz, da podpisnik taki števili pozna.

  Za ponarejena e in u mora veljati $z = u^e$, toda računanje takega para je po krepki RSA predpostavki računsko nedosegljivo. Shema je torej sledljiva.

- **Nepodtakljivost**. Podobno kot pri trace_A je tudi pri nf_A cilj nasprotnika A ponarediti veljaven skupinski podpis, le da mora tukaj znati ponarediti še dokaz, da je podpisnik član skupine, za katerega A ne poseduje tajnega ključa za izdajanje skupinskih podpisov.

  Tudi tukaj mora torej A poznati taka e in u, da velja $z = u^e$ in po krepki RSA predpostavki je računanje takega para računsko nedosegljivo, tako da si s spreminjanjem podatkov o članih A lahko pridobi le zanemarljivo prednost. Prav tako je za znan u po predpostavki o težkosti problema diskretnega logaritma računsko nedosegljivo računanje takega e, da velja $z = u^e$. Shema je torej nepodtakljiva.

4.1.5 Komentar

Predlagana izbira varnostnih parametrov v [3] je $\epsilon = \frac{9}{8}$, $\ell_g = \hat{\ell} = 1200$, $\ell_1 = 860$, $\ell_2 = 600$ in $k = 160$. Pri teh parametrih potrebujeta podpisovanje in preverjanje podpisa nekaj manj kot 13000 množenj po 1200-bitnem modulu, podpis pa je dolg nekaj več kot 1 kB.

Slabost sheme je, da ne omogoča brisanja članov iz skupine. Zaradi polne anonimnosti sheme tudi naiven pristop s preklicnim seznamom ne deluje.

4.2 Sujing-Dongdaijeva shema

Sujing-Dongdaijeva shema, predstavljena v [14], je v osnovi statična shema, ki pa omogoča brisanje članov iz skupine. Za dosego tega cilja uporablja preklicni seznam, pri čemer se mora preverjevalec podpisa za vsak vnos v preklicnem seznamu prepričati, da ne pripada podpisniku. Takemu pristopu pravimo **preklic pri preverjevalcu** (*verifier-local revocation*).

Shema temelji na q-krepki Diffie-Hellmanovi predpostavki in tridelni Diffie-Hellmanovi odločitveni predpostavki, poleg tega pa predpostavlja obstoj učinkovitih enosmernih bilinearnih preslikav $e : G \times G \to G$ z $e(g, g) \neq 1$ pri $G = \langle g \rangle$ - veljati mora torej $e(u^a, v^b) = e(u, v)^{ab}$ za vse $u, v \in G$, $a, b \in \mathbb{Z}$. Lahko se je prepričati, da za poljubne $u, v, w \in G$ velja $e(uv, w) = e(u, w)e(v, w)$ in $e(u, vw) = e(u, v)e(u, w)$.

Avtoriteta je pri tej shemi le ena - rekli ji bomo kar nadzornik skupine. Najprej izbere grupo $G = \langle g \rangle$ z $\text{ord}(g) = p \in \mathbb{P}$, naključen element $\tilde{g} \in G$, enosmerno bilinearno preslikavo $e : G \times G \to G$ z $e(g, g) \neq 1$ in zgoščevalno fukcijo $\mathcal{H} : \{0, 1\}^* \to \mathbb{Z}_p^*$ brez trkov. Nato naključno izbere $h_j \in G$ za $j = 1, \ldots, T$, kjer je T število časovnih intervalov, in $\gamma \in \mathbb{Z}_p$ ter izračuna $w := g^\gamma$. Nadzornik skupine objavi javni ključ skupine $(g, \tilde{g}, w, \{h_1, \ldots, h_T\})$. Določi se skupno število članov n ter za vsakega izmed njih nadzornik skupine naključno izbere $x_i \in \mathbb{Z}_p^*$ in izračuna $A_i := g^{(\gamma + x_i)^{-1}}$, $i = 1, \ldots, n$. Uporabnik i dobi (A_i, x_i), ki mu služi kot tajni ključ za podpisovanje v imenu skupine. Nazadnje nadzornik skupine izračuna še preklicne žetone $B_{ij} = h_j^{x_i}$ za $i = 1, \ldots, n$ in $j = 1, \ldots, T$. Če hoče nadzornik iz skupine izločiti člana skupine i v časovnem intervalu j, doda B_{ij} v preklicni seznam RL_j za časovni interval j.

4.2.1 Podpisovanje sporočila

Denimo, da želi član skupine i podpisati sporočilo m, ki vsebuje podatek o časovnem intervalu j, v katerem je nastalo. To lahko dosežemo tako, da neodvisna avtoriteta izda certifikat s časovnim žigom za sporočilo oziroma njegov izvleček. Potem je skupinski

podpis sporočila m po Sujing-Dongdaijevi shemi neinteraktiven dokaz brez razkritja znanja:

$$(c, s_1, s_2, s_3, s_4, s_5, s_6, s_7, a, b, d, f, u) = \text{SPK}\Big\{ (\alpha, \beta, \delta, \xi, \omega) \mid a = \omega\tilde{g}^{\alpha} \wedge$$

$$\wedge b = g^{\alpha}\tilde{g}^{\beta} \wedge d = h_j^{\xi\delta} \wedge f = u^{\delta} \wedge e(\omega, wg^{\xi}) = e(g, g) \Big\}(m) =$$

$$= \text{SPK}\Big\{(\alpha, \beta, \delta, \xi, \zeta, \eta, \theta) \Big| f^{\xi} = u^{\zeta} \wedge b = g^{\alpha}\tilde{g}^{\beta} \wedge d = h_j^{\zeta} \wedge f = u^{\delta} \wedge$$

$$\wedge b^{\xi} = g^{\eta}\tilde{g}^{\theta} \wedge e(a, w) = e(a^{-\xi}\tilde{g}^{\eta}, g)e(\tilde{g}^{\alpha}, w)e(g, g)\Big\}(m)$$

Naj bo Anita član i. Če želi podpisati sporočilo m v časovnem intervalu j, stori sledeče:

1. Naključno izbere $k, l, q \in \mathbb{Z}_p^*$, $u \in G$
2. Izračuna $a := A_i\tilde{g}^k$, $b := g^k\tilde{g}^l$, $d := h_j^{x_i q}$, $f := u^q$
3. Naključno izbere $r_1, r_2, r_3, r_4, r_5, r_6, r_7 \in \mathbb{Z}_p^*$
4. Izračuna $t_1 := f^{r_1}u^{-r_2}$, $t_2 := g^{r_3}\tilde{g}^{r_4}$, $t_3 := h_j^{r_2}$, $t_4 := u^{r_5}$, $t_5 := b^{r_1}g^{-r_6}\tilde{g}^{-r_7}$, $t_6 := e(a^{-r_1}\tilde{g}^{r_6}, g)e(\tilde{g}^{r_3}, w)$
5. Izračuna $c := \mathcal{H}(g\|\tilde{g}\|w\|a\|b\|d\|f\|u\|t_1\|t_2\|t_3\|t_4\|t_5\|t_6\|m)$
6. Izračuna $s_1 := r_1 - cx_i$, $s_2 := r_2 - cx_iq$, $s_3 := r_3 - ck$, $s_4 := r_4 - cl$, $s_5 := r_5 - cq$, $s_6 := r_6 - cx_ik$, $s_7 := r_7 - cx_il$ v $\mathbb{Z}_p$
7. Izda podpis $\sigma = (c, s_1, s_2, s_3, s_4, s_5, s_6, s_7, a, b, d, f, u)$

Prepričajmo se, da sta podana dokaza brez razkritja znanja ekvivalentna. Denimo, da izdajatelj pozna take $\alpha, \beta, \delta, \xi, \omega$, ki ustrezajo prvemu dokazu. Potem pozna tudi $\zeta = \xi\delta$, $\eta = \xi\alpha$ in $\theta = \xi\beta$, da velja:

$$f = u^{\delta} \Rightarrow f^{\xi} = u^{\xi\delta} = u^{\zeta}$$

$$d = h_j^{\xi\delta} \Rightarrow d = h_j^{\zeta}$$

$$b = g^{\alpha}\tilde{g}^{\beta} \Rightarrow b^{\xi} = g^{\xi\alpha}\tilde{g}^{\xi\beta} = g^{\eta}\tilde{g}^{\theta}$$

Dokažimo še veljavnost zadnje dokazovane enačbe:

$$e(g, g) = e(\omega, wg^{\xi}) = e(\omega, w)e(\omega, g^{\xi})$$

$$e(\omega^{-\xi}\tilde{g}^{-\xi\alpha}\tilde{g}^{\xi\alpha}, g)e(\tilde{g}^{\alpha}, w)e(g, g) = e(\omega, w)e(\tilde{g}^{\alpha}, w) = e(\omega\tilde{g}^{\alpha}, w)$$

$$e(a^{-\xi}\tilde{g}^{\eta}, g)e(\tilde{g}^{\alpha}, w)e(g, g) = e(a, w)$$

Tako smo dokazali, da iz poznavanja $\alpha, \beta, \delta, \xi, \omega$ iz prvega dokaza sledi poznavanje $\alpha, \beta, \delta, \xi, \zeta, \eta, \theta$ iz drugega dokaza. Dokažimo sedaj še obratno. Iz $f = u^{\delta}$ in $f^{\xi} = u^{\zeta}$ sledi $\zeta = \xi\delta$, iz $b = g^{\alpha}\tilde{g}^{\beta}$ in $b^{\xi} = g^{\eta}\tilde{g}^{\theta}$ pa še $\eta = \xi\alpha$ in $\delta = \xi\beta$. Izdajatelj lahko izračuna še $\omega = a\tilde{g}^{-\alpha}$, tako da velja:

$$\omega = a\tilde{g}^{-\alpha} \Rightarrow a = \omega\tilde{g}^{\alpha}$$

$$d = h_j^{\zeta} \Rightarrow d = h_j^{\xi\delta}$$

$$e(a^{-\xi}\tilde{g}^{\eta}, g)e(\tilde{g}^{\alpha}, w)e(g, g) = e(a, w) \Rightarrow$$

$$\Rightarrow e(g, g) = e(a, w)e(\tilde{g}^{-\alpha}, w)e((a\tilde{g}^{-\alpha})^{\xi}, g) = e(a\tilde{g}^{-\alpha}, w)e(a\tilde{g}^{-\alpha}, g^{\xi}) = e(\omega, wg^{\xi})$$

4.2.2 Preverjanje in odpiranje podpisa

Preverjanje pravilnosti skupinskega podpisa poteka v dveh korakih. Če želi Boris preveriti veljavnost podpisa $\sigma = (c, s_1, s_2, s_3, s_4, s_5, s_6, s_7, a, b, d, f, u)$, v prvem koraku izračuna $t'_1 := f^{s_1}u^{-s_2}$, $t'_2 := g^{s_3}\tilde{g}^{s_4}b^c$, $t'_3 := h_j^{s_2}d^c$, $t'_4 := u^{s_5}f^c$, $t'_5 := b^{s_1}g^{-s_6}\tilde{g}^{s_7}$ in $t'_6 := e(a^{-s_1}\tilde{g}^{s_6}g^{-c})e(a^c\tilde{g}^{s_3}, w)$ ter preveri, da velja

$$c = \mathcal{H}(g\|\tilde{g}\|w\|a\|b\|d\|f\|u\|t'_1\|t'_2\|t'_3\|t'_4\|t'_5\|t'_6\|m)$$

Prepričajmo se, da je preverjanje podpisa pravilno izvedeno. Ob predpostavki, da je zgoščevalna funkcija $\mathcal{H}$ brez trkov zadošča preveriti, da velja $t_i = t'_i$ za $i = 1, 2, 3, 4, 5, 6$:

$$t'_1 = f^{s_1}u^{-s_2} = u^{q(r_1-cx_i)}u^{-r_2+cx_iq} = u^{qr_1}u^{-r_2} = f^{r_1}u^{-r_2} = t_1$$

$$t'_2 = g^{s_3}\tilde{g}^{s_4}b^c = g^{r_3-ck}\tilde{g}^{r_4-cl}g^{ck}\tilde{g}^{cl} = g^{r_3}\tilde{g}^{r_4} = t_2$$

$$t'_3 = h_j^{s_2}d^c = h_j^{r_2-cx_iq}h_j^{cx_iq} = h_j^{r_2} = t_3$$

$$t'_4 = u^{s_5}f^c = u^{r_5-cq}u^{cq} = u^{r_5} = t_4$$

$$t'_5 = b^{s_1}g^{-s_6}\tilde{g}^{s_7} = g^{k(r_1-cx_i)}\tilde{g}^{l(r_1-cx_i)}g^{-r_6+cx_ik}\tilde{g}^{-r_7+cx_il} = g^k\tilde{g}^l g^{-r_6}\tilde{g}^{-r_7} = bg^{-r_6}\tilde{g}^{-r_7} = t_5$$

$$t'_6 = e(a^{-s_1}\tilde{g}^{s_6}g^{-c}, g)e(a^c\tilde{g}^{s_3}, w) = e(A_i^{-r_1+cx_i}\tilde{g}^{-k(r_1-cx_i)}\tilde{g}^{r_6-cx_ik}g^{-c}, g)e(A_i^c\tilde{g}^{ck}\tilde{g}^{r_3-ck}, g^\gamma) =$$

$$= e(A_i^{-r_1}\tilde{g}^{-kr_1}\tilde{g}^{r_6}, g)e(g^{cx_i(\gamma+x_i)^{-1}}g^{-c}, g)e(g^{c(\gamma+x_i)^{-1}}, g^\gamma)e(\tilde{g}^{r_3}, g^\gamma) =$$

$$= e(a^{-r_1}\tilde{g}^{r_6}, g)e(g, g)^{c(\gamma+x_i)(\gamma+x_i)^{-1}-c}e(\tilde{g}^{r_3}, w) = e(a^{-r_1}\tilde{g}^{r_6}, g)e(\tilde{g}^{r_3}, w) = t_6$$

Če prvi korak uspe, v drugem koraku Boris preveri, ali ni morda podpisnik bil odstranjen iz skupine v časovnem obdobju, ko je bil izdan podpis. Denimo, da je bilo sporočilo podpisano v časovnem obdobju j. Tedaj Boris za vsak $B \in RL_j$ preveri, ali velja $e(d, u) = e(B, f)$. Če obstaja tak B, da ekvivalenca velja, potem je bil podpisnik odstranjen iz skupine in skupinski podpis zato ni veljaven.

Če je nadzornik skupine v časovnem obdobju j iz skupine odstranil podpisnika - naj bo to član skupine i - potem RL_j vsebuje $B_{ij} = h_j^{x_i}$, ki ustreza zgornji enačbi:

$$e(d, u) = e(h_j^{x_iq}, u) = e(h_j^{x_i}, u^q) = e(B_{ij}, f)$$

Očitno je, da noben $B \in RL_j$ ne bo ustrezal enačbi, če i ni bil odstranjen iz skupine in torej $B_{ij} \notin RL_j$.

Odpiranje podpisa poteka po istem postopku kot preverjanje veljavnosti, s to izjemo, da se v drugem koraku namesto elementov preklicnega seznama uporabijo kar vsi preklicni žetoni za časovno obdobje j, v katerem je bil izdan podpis. Kot podpisnika nadzornik skupine identificira tistega člana skupine i, katerega žeton B_{ij} ustreza enačbi.

4.2.3 Varnost sheme

Ker formalizirane varnostne zahteve iz drugega poglavja ne upoštevajo možnosti, da se lahko člani odstranjujejo iz skupine, bomo tukaj uporabili nekoliko prirejene zahteve, kjer je tudi to predvideno.

- **Anonimnost**. Trivialno je videti, da shema *ni* anonimna po definiciji iz drugega poglavja. Ker ima nasprotnik A pri poskusu anon_A^b dostop do vseh tajnih ključev članov skupine, lahko izračuna $B_{ij} := h_j^{x_i}$ za poljubna $i = 1, \ldots, n$ in $j = 1, \ldots, T$ in tako lahko identificira podpisnika kateregakoli sporočila. Vidimo lahko tudi, da lahko vsak član skupine i izračuna B_{ij} za poljuben $j = 1, \ldots, T$, kar pomeni, da lahko član skupine identificira lastne podpise. To je lahko tudi prednost, saj lahko tako član skupine ugotovi, ali je bil morda njegov tajni ključ ukraden.

  Varnostna lastnost, ki jo bomo dokazali pri tej shemi, je **anonimnost z vzvratno nepovezljivostjo**. Neformalno to pomeni, da shema ohranja nepovezljivost tudi z odstranjevanjem članov iz skupine. Anonimnost z vzvratno nepovezljivostjo dobimo, če pri anonimnosti poskus anon_A^b nadomestimo z bu-anon_A^b. Pri njem lahko A počne isto kot pri anon_A^b, poleg tega pa lahko za vsakega člana skupine pridobi njegov preklicni žeton za poljubno časovno obdobje. Za izbrana člana i_0 in i_1 mora veljati, da A ni pridobil njunih preklicnih žetonov pred izbranim časovnim obdobjem J, iz katerega se generira podpis, katerega podpisnika mora A identificirati.

  Zaradi prej omenjene slabosti bomo dokazali nekoliko šibkejšo različico te zahteve. Namesto dostopa do vseh tajnih ključev članov skupine naj ima A dostop do oraklja za podpisovanje sporočil, tajne ključe članov pa lahko pridobi, vendar i_0 in i_1 ne smeta biti med temi člani skupine.

  Denimo, da lahko A z nezanemarljivo prednostjo $\text{Adv}_A^{\text{bu-anon}}$ razloči med skupinskima podpisoma dveh članov skupine. Po predpostavki iz modela z naključnim orakljem A iz c ne more pridobiti nobene informacije, prav tako ne iz s_i, $i = 1, \ldots, 7$, saj so r_i, $i = 1, \ldots, 7$ naključno izbrani. Zato mu morajo zadostovati a, b, d, f in u. Naj bo B algoritem, s katerim poskušamo razbiti tridelno Diffie-Hellmanovo odločitveno predpostavko. B dobi na vhod četverico $(g_1, g_2, g_3, Z) \in G^4$, kjer je $G = \langle g \rangle$, $g_1 = g^\alpha$, $g_2 = g^\beta$, $g_3 = g^\delta$. Cilj B je ugotoviti, ali velja $Z = g^{\alpha\beta\delta}$. B kliče A in odgovarja na njegove poizvedbe orakljem.

  Najprej se vzpostavi shema za skupinske podpise. Uporabi se grupa $G = \langle g \rangle$, iz katere B naključno izbere $\tilde{g}$, nato naključno izbere $\gamma \in \mathbb{Z}_p^*$ in izračuna $w := g^\gamma$. Postavi se $h_1 := g_1$, za $j = 2, \ldots, T$ pa se izračunajo $h_j := g^{r_j}$, kjer so r_j naključno izbrani iz $\mathbb{Z}_p^*$. Naključno se izberejo vrednosti $x_i \in \mathbb{Z}_p^*$ za $i = 2, \ldots, n$ ter izračunajo $A_i = g^{(\gamma + x_i)^{-1}}$ za $i = 2, \ldots, n$ in $B_{ij} := h_j^{x_i}$ za $i = 2, \ldots, n$ in $i = j, \ldots, T$. Za $i = 2, \ldots, n$ se postavijo $B_{i1} := g_1^{x_i}$, za $j = 2, \ldots, T$ pa $B_{1j} := g_2^{r_j}$. Vrednosti x_1, A_1 in B_{11} ostanejo neznane, saj bi moralo veljati $x_1 = \beta$, $A_1 = g^{(\gamma+\beta)^{-1}}$ in $B_{11} = g^{\alpha\beta}$.

  Če A zahteva skupinski podpis od člana skupine $i \neq 1$, potem lahko B po postopku za podpisovanje izda veljaven podpis, saj ima vse potrebne podatke. Če velja $i = 1$, a je zahtevano časovno obdobje j različno od 1, potem B naključno izbere $a, b, u \in G$ in $q \in \mathbb{Z}_p^*$ ter izračuna $d := B_{1j}^q$ in $f := u^q$, če pa velja $i = 1$ in $j = 1$, pa B naključno izbere $a, b \in G$ in $z_1, z_2 \in \mathbb{Z}_p^*$ ter izračuna $d := g_1^{z_1}$, $f := g^{z_1 z_2}$ in $u = g_2^{z_2}$. Očitno v slednjem primeru velja $d = g^{\alpha\beta q} = B_{11}^q$ in $f = u^q$, kjer je $q = z_1\beta^{-1}$. V obeh primerih preostanek podpisa izbere naključno, saj nima dovolj podatkov za izdajo dokaza brez razkritja znanja.

  Če A zahteva tajni ključ uporabnika $i = 1$ ali njegov preklicni žeton za obdobje $j = 1$, potem se B prekine in vrne naključno izbran odgovor. Ko A izbere sporočilo m, člana skupine i_0 in i_1 ter časovno obdobje J, B naključno izbere

$\phi \in \{0,1\}$ ter se prekine in vrne naključen odgovor, če velja $i_\phi \neq 1$ ali $J \neq 1$. V nasprotnem primeru A generira podpis tako, da naključno izbere $a, b \in G$ in $r \in \mathbb{Z}_p^*$ ter postavi $d := Z$, $f := g_3^r$ in $u := g^r$. Preostanek podpisa izbere naključno. Če velja $Z = g^{\alpha\beta\delta}$, potem je $d = h_1^{x_1\delta}$ in $f = u^\delta$, torej ustreza skupinskemu podpisu, ki bi ga izdal član $i = 1$ in zato A pravilno identificira podpisnika z verjetnostjo, bistveno večjo od $\frac{1}{2}$. Če pa velja $g_3 \neq g^{\alpha\beta\delta}$, potem generirani podpis ne ustreza podpisu od i_0 ali i_1 in A lahko le ugiba o podpisniku.

B vrne, da velja $Z = g^{\alpha\beta\delta}$ natanko tedaj, ko A kot podpisnika generiranega sporočila identificira člana skupine $i = 1$. Če torej res velja $Z = g^{\alpha\beta\delta}$, potem B to pravilno ugotovi z verjetnostjo $\frac{1}{2} + \frac{1}{nT}\mathrm{Adv}_A^{\text{bu-anon}}$, sicer pa z verjetnostjo $\frac{1}{2}$. Prednost B pri tridelnem Diffie-Hellmanovem odločitvenem problemu je tako $\mathrm{Adv}_B = \frac{1}{nT}\mathrm{Adv}_A^{\text{bu-anon}}$ in ni zanemarljiva. To je v protislovju s tridelno Diffie-Hellmanovo odločitveno predpostavko, tako da je Sujing-Dongdaijeva shema anonimna z vzvratno nepovezljivostjo.

- **Sledljivost**. Tudi tukaj bomo razširili varnostno zahtevo iz drugega poglavja, in sicer polno sledljivost, torej združeno zahtevo sledljivosti in nepodtakljivosti za statične sheme. Namesto poskusov trace_A in nf_A bo A izvajal poskus bu-trace_A. Pri tem poskusu ima dostop do vseh orakljev, do katerih ima dostop pri trace_A in nf_A, ter dostop do tajnih ključev podmnožice $\mathcal{C}$ članov skupine in do vseh preklicnih žetonov, za katere tudi ve, komu pripadajo. Poleg sporočila m in njegovega podpisa σ A izbere še časovni interval j, v katerem naj bi nastal podpis. Poskus uspe, če je σ veljaven skupinski podpis in zanj ni mogoče določiti podpisnika, ali pa je ta izven množice $\mathcal{C}$.

4.2.4 Komentar

Očitna slabost sheme je v tem, da nadzornik skupine poseduje tajne ključe vseh članov skupine in tako lahko izdaja podpise v imenu kateregakoli od njih. Če lahko to dejstvo zanemarimo, je potem Sujing-Dongdaijeva shema popolnoma dinamična, saj lahko nadzornik skupine enostavno poveča tako n kot T in izračuna manjkajoče h_j, x_i, A_i in B_{ij}.

Ker pa tega ponavadi nočemo, lahko to preprečimo tako, da pri vzpostavitvi skupine poleg nadzornika sodelujejo vsi člani skupine. Vsak član izbere svoj x_i ter ga pošlje nadzorniku skupine, ki izračuna A_i in ga pošlje nazaj članu skupine. Poleg tega izračuna še B_{ij} za $j = 1, \ldots, T$. Nato se član skupine prepriča, da je nadzornik zavrgel x_i in A_i. Kasnejše dodajanje članov je sicer mogoče po enakem postopku, večji problem pa predstavlja dodajanje novih časovnih intervalov - vsak član bi sicer lahko izračunal $B_{ij} := h_j^{x_i}$ za nove časovne intervale in s protokolom, ekvivalentnim

$$\mathrm{SPK}\left\{(\alpha) \mid B_{i1} = h_1^\alpha \wedge B_{ij} = h_i^\alpha\right\}(m)$$

dokazal pravilnost izračuna, vendar nadzornik skupine člana, ki bi zavrnil sodelovanje, ne bi mogel izločiti iz skupine, saj bi mu manjkal ravno podatek, ki je za to potreben.

5 Zaključek

Literatura

[1] M. Bellare, D. Micciancio in B. Warinschi: *Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions*. V E. Biham (ured.): *EUROCRYPT*, del 2656 iz *Lecture Notes in Computer Science*, str. 614–629. Springer, 2003, ISBN 3-540-14039-5.
http://www-cse.ucsd.edu/users/mihir/papers/gs.pdf .

[2] M. Bellare, H. Shi in C. Zhang: *Foundations of group signatures: The case of dynamic groups*, 2004.
http://www-cse.ucsd.edu/users/mihir/papers/bsz.pdf .

[3] J. Camenisch in M. Michels: *A group signature scheme based on an RSA-variant*. Research series RS-98-27, BRICS, Department of Computer Science, University of Aarhus, 1998.
http://www.brics.dk/RS/98/27/BRICS-RS-98-27.pdf .

[4] J. Camenisch in M. Michels: *Proving in zero-knowledge that a number is the product of two safe primes*. Lecture Notes in Computer Science, 1592:107–122, 1999.
http://www.springerlink.com/content/blqm17fy9wr5n1xx/fulltext.pdf .

[5] R. Canetti, O. Goldreich in S. Halevi: *The random oracle methodology, revisited*, 1998.
http://arxiv.org/pdf/cs/0010019v1 .

[6] D. Chaum in E. van Heyst: *Group signatures*. V D.W. Davies (ured.): *EUROCRYPT*, del 547 iz *Lecture Notes in Computer Science*, str. 257–265. Springer, 1991, ISBN 3-540-54620-0.
http://www.springerlink.com/content/yrk497a8yjge84fx/fulltext.pdf .

[7] N. Funabiki, T. Nakanishi, H. Takahashi, K. Miki in J. Kawashima: *A proposal of anonymous IEEE802.1X authentication protocol for wireless networks*. Second Workshop on Secure Network Protocols (NPSec), 0:26–31, 2006.

[8] R. Gennaro, D. Micciancio in T. Rabin: *An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products*. V *5th ACM Conference on Computer and Communication Security (CCS'98)*, str. 67–72, San Francisco, California, nov 1998. ACM, ACM Press.
http://www.cs.ucsd.edu/users/daniele/papers/GMR.pdf .

[9] O. Goldreich in Y. Oren: *Definitions and properties of zero-knowledge proof systems*. Journal of Cryptology, 7(1):1–32, 1994.
http://www.wisdom.weizmann.ac.il/~oded/PS/oren.ps .

[10] J. Liu, V. Wei in D. Wong: *Linkable spontaneous anonymous group signature for ad hoc groups*, 2004.
http://www.springerlink.com/content/7dp5c5cjwq5cg7eq/fulltext.pdf .

[11] G. Maitland in C. Boyd: *Fair electronic cash based on a group signature scheme*. Lecture Notes in Computer Science, 2229:461–465, 2001.
http://sky.fit.qut.edu.au/~boydc/papers/GOC-ECash.pdf .

[12] T. Nakanishi, T. Fujiwara in H. Watanabe: *A linkable group signature and its application to secret voting*. Transactions of Information Processing Society of Japan, 40(7):3085–3096, 1999.

[13] Y. Su in Y. Zhu: *A fair off-line e-cash system with group signature*. Wuhan University Journals Press, 9(5):745–748, 2004.
http://www.springerlink.com/content/4651642r50577218/fulltext.pdf .

[14] Z. Sujing in L. Dongdai: *A shorter group signature with verifier-location revocation and backward unlinkability*. Cryptology ePrint Archive, Report 2006/100, 2006.
http://eprint.iacr.org/2006/100.pdf .