Anonymita na sieti

(Študentská vedecká odborná činnosť)

Peter Kempec

Univerzita Pavla Jozefa Šafárika v Košiciach
Prírodovedecká fakulta
Ústav informatiky

Abstrakt Táto práca sa zaoberá problematikou anonymity v počítačových sietiach. Cieľom tejto práce je návrh schémy elektronického hlasovania na spoločnej broadcastovej doméne bez použitia dôveryhodnej autority.

1 Motivácia

Hlavným cieľom tejto práce je návrh, analýza a implementácia schémy elektronického hlasovania, v ktorej sú si všetci účastníci rovnocenní. To znamená, že každý z danných účastníkov môže zahájiť hlasovanie. Počas hlasovania vyberá oprávnený účastník práve jednu, alebo žiadnu voľbu z niekoľkých možných. Predpokladáme, že hlasovanie prebieha na spoločnej broadcastovej doméme bez prítomnosti dôveryhodnej autority. Do hlasovania sa teda môžu zapojiť len účastníci dannej broadcastovej domény.

Formálnejšie by so to dalo vyjadriť nasledovne: máme N účastníkov nejakej broadcastovej domény, ktorí vyberajú z L volieb (hlasujú za jednu z L možností). Našou úlohou je navrnúť schému elektronického hlasovania, ktorá by umožnila iniciátorovi hlasovania zistiť počet účastníkov, ktorí si vybrali 1.voľbu, počet účastníkov hlasujúcich za 2.voľbu, ... a počet hlasujúcich za L.voľbu tak, že žiadny účastník nezverejní hodnotu svojej voľby.

Uvažujme implementáciu tejto schémy do školského prostredia. Študenti a prednášajúci majú k dispozícii elektronické zariadenia, ktoré tvoria broadcastovú doménu. Nech A je prednášajúci, ktorý si chce overiť, či študenti skutočne pochopili prednášanej téme. Pomocou elektronického zariadenia inicializuje hlasovanie k otázke z práve odprednášanej témy, ku ktorej ponúkne niekoľko možných odpovedí, z ktorých práve jedna je správna. Študenti $V_1, \ldots, V_N$ (N respondentov) majú možnosť anonymne označiť jednu z ponúknutých odpovedí za správnu. To znamená, že študenti $V_1, \ldots, V_N$ cez elektronické zariadenie odošlú svoju odpoveď prednášajúcemu A s tým, že A nevie ktorá odpoveď patrí ktorému študentovi, ale pre každú ponúkanú odpoveď pozná počet študentov, ktorí ju označili za správnu.

2 Kryptografické primitíva

2.1 Diskrétny logaritmus

Bezpečnosť mnohých šifrovacích systémov závisi od zložitosti riešenia problému diskrétneho logaritmu. V kryptografii sa diskrétny logaritmus veľmi často počíta pri základe, ktorý je generátorom cyklickej grupy. V takomto prípade je existencia diskrétneho logaritmu zaručená.

Definícia 1 (Diskrétny logaritmus) *Nech $(G, \cdot)$ je konečná cyklická grupa rádu $n \in \mathbb{N}$, nech $g, y \in G$ a nech g je generátor tejto grupy. Diskrétnym logaritmom y pri základe g nazývame číslo $x \in \mathbb{Z}_n$ také, že $g^x = y$. Úlohu nájsť diskrétny logaritmus pre danné g a y nazývame problém diskrétneho logaritmu.*

Efektívny algoritmus na riešenie problému diskrétneho logaritmu v súčastnosti neexistuje. Pre prvočíselné grupy $(Z_p^*, \cdot)$ síce existujú efektívne algoritmy, avšak vychádzajú zo špeciálneho tvaru prvočísla p. Použitím silného prvočísla p (také prvočíslo $p = 2q + 1$, kde aj q je tiež prvočíslo) sa tieto algoritmy stávajú prakticky nepoužiteľnými.

2.2 Zero-knowledge dôkaz

Zero-knowledge dôkazom dokazujeme pravdivosť výroku bez odhalenia akejkoľvek inej informácie než je pravdivosť výroku. Slovo „dôkaz“ tu však nemá tradičný matematický význam. Slovom „dôkaz“ máme na mysli pravdepodobnostný protokol (algoritmus), v ktorom chce jeden účastník tohto protokolu presvedčiť iného účastníka o pravdivosti danného výroku.

Každý zero-knowledge dôkaz má tri nasledujúce vlastnosti :

- **úplnosť** – ak je výrok pravdivý, tak čestný účastník presvedčí čestného overovateľa o pravdivosti tohto výroku;
- **spoľahlivosť** – ak je výrok nepravdivý, nečestný účastník môže presvedčiť čestného overovateľa o pravdivosti výroku len s veľmi malou pravdepodobnosťou;
- **zero-knowledge** – ak je výrok pravdivý, tak nečestný overovateľ nemôže odhaliť žiadnu inú informáciu.

2.3 Interaktívne a neinteraktívne dôkazy

V tejto časti si predstavíme interaktívne dôkazy v ElGamalovom šifrovacom systéme, ktoré vychádzajú zo zložitosti problému diskrétneho logaritmu. Tieto dôkazy sa v rôznych variantoch často používajú v schémach elektronických volieb. Každý z uvedených interaktívnych dôkazov môžme použitím Fiat-Shamirovej metódy premeniť na neinteraktívny dôkaz.

Fiat-Shamirová metóda Cieľom všetkých nižšie spomenutých protokolov je to, že jeden z účastníkov chce dokázať pravdivosť nejakého výroku P. Tento účastník preto odošle overovateľovi nejaké A, ktorý následne odpovedá náhodne generovanou výzvou C. Dokazujúci účastník vypočíta a odošle odpoveď $R = respond(P, A, C)$. Komunikácia $(P; A, C, R)$ a skutočnosť, že dokazujúci účastník v čase generovania A nevie nič o C, presvedčí overovateľa o pravdivosti výroku P.

Z tohto interaktívneho protokolu spravíme neinteraktívny protokol tak, že náhodnú výzvu C si dokazujúci účastník vygeneruje sám. Musíme však zabezpečiť to, aby účastník nemohol vygenerovať výzvu C ešte pred tým ako vytvorí P a A. Vo Fiat-Shamirovej metóde je C výsledkom hašovacej funkcie $H : C = H(P, A)$. Neinteraktívny dôkaz má tvar

$$(P; A, H(P, A), R)$$

V tomto dôkaze odpoveď R účastník vypočíta ako $R = respond(P, A, H(P, A))$.

Rovnosť diskrétnych logaritmov V tejto časti si predstavíme zero-knowledge protokol, ktorý umožní dokazujúcemu účastníkovi ukázať rovnosť diskrétnych logaritmov. Ten má k dispozícii štvoricu čísel (g, x, h, y), kde $g, x, h, y \in Z_p$ a vykonaním protokolu preukazuje znalosť takého čísla α, že $x = g^\alpha$ a $y = h^\alpha$. Účastník vlastne dokazuje pravdivosť výroku

$$\log_g x = \log_h y.$$

Ak účastník presvedčí overovateľa o pravdivosti daného výroku, preukáže tým znalosť čísla α bez jeho prezradenia (zero-knowledge). Priebeh protokolu vyzerá nasledovne :

1. Účastník si náhodne zvolí $\omega \in Z_p$;
2. Vypočíta $(a, b) \leftarrow (g^\omega, h^\omega)$ a odošle dvojicu (a, b) overovateľovi;
3. Overovateľ si náhodne zvolí $c \in Z_p$ a odošle ho dokazujúcemu účastníkovi;
4. Účastník vypočíta $r \leftarrow \omega + ac$ a odošle ho overovateľovi;
5. Overovateľ overí, či platí $(g^r = ax^c) \wedge (h^r = by^c)$.

Akceptujúca konverzácia pre náhodne zvolené čísla c, r je $(g^r x^{-c}, h^r y^{-c}, c, r)$. Účastník, ktorý dokazuje znalosť α, nemôže bez jeho znalosti vypočítať príslušné r, ktoré by spĺňalo overovateľove požiadavky.

Neinteraktívna verzia

- Dokazujúci účastník uskutoční tie isté výpočty ako v interaktívnej verzii s tým rozdielom, že si sám vygeneruje výzvu $c = H(a, b, x, y)$, kde H je bezpečná hašovacia funkcia.
- Hodnoty c, r odošle overovateľovi, ktorý skontroluje platnosť vzťahu

$$c = H(g^r x^{-c}, h^r y^{-c}, x, y)$$

Komunikácia v interaktívnej verzii pozostávala z výmeny štyroch elementov medzi účastníkmi. Zmenou na neinteraktívnu verziu sme znížili komunikačnú zložitosť len na odoslanie dvoch elementov.

Prešifrovanie 1 z L správ Chceme dokázať, že pre šifrovanú správu (x, y) v ElGamalovom šifrovacom systéme existuje jej prešifrovanie medzi L šifrovanými správami $(x_1, y_1), \ldots, (x_L, y_L)$.

Nech prešifrovanie (x, y) je (x_t, y_t) a nech svedok prešifrovania je v, čiže $(x_t, y_t) = (xg^v, yh^v)$.

1. Dokazujúci účastník náhodne zvolí dva vektory

   $$d = (d_1, \ldots, d_L) \quad r = (r_1, \ldots, r_L)$$

   také, že $d_i, r_i \in Z_p$ pre $i = 1, \ldots, L$. Vypočíta $w \leftarrow vd_t + r_t$ a vektory

   $$a = (a_1, \ldots, a_L) \quad b = (b_1, \ldots, b_L)$$

   také, že $a_i = (\frac{x_i}{x})^{d_i} g^{r_i}$ a $b_i = (\frac{y_i}{y})^{d_i} h^{r_i}$. Vektory a, b odošle overovateľovi.
2. Overovateľ náhodne zvolí $c \in_R Z_p$, ktoré odošle dokazujúcemu účastníkovi.
3. Dokazujúci účastník dosadí za $d_t \leftarrow c - \sum_{j \neq t} d_j$ a za $r_t \leftarrow w - vd_t$. Overovateľovi pošle vektory d, r.
4. Overovateľ skontroluje platnosť vzťahov

   $$c = d_1 + \cdots + d_L \qquad a_i = \left(\frac{x_i}{x}\right)^{d_i} g^{r_i} \qquad b_i = \left(\frac{y_i}{y}\right)^{d_i} h^{r_i}$$

V tomto protokole overovateľ vyzýva dokazujúceho účastníka na zmenu jeho vektorov d a r tak, aby súčet prvkov vektora d bol c. Účastník následne modifikuje hodnoty d_t, r_t tak, aby spĺňali tento vzťah a odošle ich overovateľovi. Týmto krokom sa overovateľ presvedčí, že jedna z L šifrovaných správ je prešifrovaná správa (x, y) a že dokazujúci účastník skutočne pozná svedka prešifrovania. Bez jeho znalosti totiž nemôžme prispôsobiť súčet prvkov vektora na požadovanú hodnotu.

Neinteraktívna verzia

- Dokazujúci účastník uskutoční tie isté výpočty ako v interaktívnej verzii s tým rozdielom, že si sám vygeneruje výzvu

  $$c = H(a_1, \ldots, a_L, b_1, \ldots, b_L, x, y, x_1, \ldots, x_L, y_1, \ldots, y_L)$$

  H je bezpečná hašovacia funkcia.
- Hodnoty $c, d_1, \ldots, d_L, r_1, \ldots, r_L$ odošle overovateľovi, ktorý skontroluje platnosť vzťahu

  $$c = H(a_1, \ldots, a_L, b_1, \ldots, b_L, x, y, x_1, \ldots, x_L, y_1, \ldots, y_L)$$

  Pre tento vzťah platí, že $a_i = (\frac{x_i}{x})^{d_i} g^{r_i}$ a $b_i = (\frac{y_i}{y})^{d_i} h^{r_i}$.

Komunikácia v interaktívnej verzii pozostávala z výmeny $4L+1$ elementov medzi účastníkmi. Zmenou na neinteraktívnu verziu sme znížili komunikačnú zložitosť na odoslanie $2L + 1$ elementov.

Výber 1 z L možností Pre zašifrovanú správu $E(m) = (x, y)$ v ElGamalovom šifrovacom systéme chceme bez odhalenia správy m dokázať, že m je jedna z L možných správ $G_1, \ldots, G_L$. Predpokladáme, že diskrétne logaritmy prvkov $G_1, \ldots, G_L$ sú neznáme. Našim cieľom je dokázať platnosť výroku

$$\log_g x = \log_h(y/G_1) \vee \cdots \vee log_g x = \log_h(y/G_L)$$

Pomocou protokolu z predchádzajucej časti nám tedá stačí dokázať, že medzi prvkami

$$(x_1, y_1) = (x, y/G_1)$$

$$\vdots$$

$$(x_L, y_L) = (x, y/G_L)$$

sa nachádza prešifrovanie správy $(1, 1)$.

2.4 Asymetrické šifrovanie

RSA

Inicializácia

1. Zvolíme si dve prvočísla p a q také, že $p \neq q$.
2. Položíme $n = p \cdot q$.
3. Vyberieme prirodzené číslo e také, že $1 < e < \phi(n)$ a $nsd(e, \phi(n)) = 1$.
4. Vypočítame d také, že $e \cdot d \equiv 1 \pmod{\phi(n)}$.
5. Dvojica čísel (e, n) tvorí verejný kľúč. Číslo d predstavuje súkromný kľúč.

Šifrovanie

$$E(m) = m^e \bmod n$$

Dešifrovanie

$$D(c) = c^d \bmod n$$

El Gamal

Inicializácia

1. Zvolíme veľké prvočíslo p a prvok $g \in Z_p^*$.
2. Náhodne zvolíme $x \in_R \{2, 3, \ldots, p-2\}$ a vypočítame $y \equiv g^x \pmod{p}$.
3. Trojica čísel (y, p, g) tvorí verejný kľúč. Číslo x predstavuje súkromný kľúč.

Šifrovanie Nech Z_p je priestor správ a nech $m \in Z_p$ je správa, ktorú chceme šifrovať.

1. Zvolíme náhodné $k \in_R \{1, 2, \ldots, p-1\}$.
2. Zašifrovanú správu predstavuje dvojica (r, s), kde
   $r = g^k \bmod p$
   $s = y^k \cdot m \bmod p$.

Dešifrovanie

$$m = r^{x-1} \cdot s \bmod p$$

2.5 Homomorfné šifrovanie

Uvažujme nejakú pravdepodobnostnú šifrovacú schému. Nech P je priestor správ a C je priestor šifier také, že P je grupa nad binárnou operáciou $\oplus$ a C je grupa nad binárnou operáciou $\otimes$. Inštanciu E pravdepodobnostnej šifrovacej schémy vytvoríme vygenerovaním jej verejných a súkromných kľúčov. Nech $E_r(m)$ je správa m zašifrovaná pomocou náhodneho parametra r v inštancii E.

Hovoríme, že pravdepodobnostná šifrovacia schéma je $(\otimes, \oplus)$- homomorfná, ak pre každú inštanciu E šifrovacej schémy a pre každé $c_1 = E_{r_1}(m_1), c_2 = E_{r_2}(m_2)$ existuje r také, že

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

2.6 Schémy na zdieľanie tajomstva

Účelom schém na zdieľanie tajomstva je rozdeliť tajomstvo medzi n účastníkov takým spôsobom, že jeho rekonštrukcia je možná len za prítomnosti určitého minimálneho (prahového) počtu účastníkov.

Shamirova schéma Shamirova $(t+1, n)$ schéma na zdieľanie tajomstva umožňuje každej skupine aspoň $t+1$ z n účastníkov odhalenie tajomstva.

Inicializácia

1. Zvolíme prvočíslo $p > n+1$ a tajnú zdieľanú informáciu $s \in Z_p$.
2. Zvolíme n rôznych prvkov $x_1, \ldots, x_n \in Z_p$, kde $x_i \neq x_j$ pre všetky $i \neq j$.
3. Zvolíme náhodný polynóm $f(x)$ stupňa najviac t nad Z_p, pre ktorý platí: $f(0) = s$. Teda $f(x) = a_t x^t + \ldots a_1 x + a_0$, kde $a_t, \ldots, a_1 \in_R Z_p$ a $a_0 = s$.
4. Každý účastník P_i obdrží dvojicu $(x_i, f(x_i))$, kde $f(x_i)$ je súkromná informácia účastníka P_i.

Rekonštrukcia tajomstva Každá skupina $t+1$ čestných účastníkov dokáže zrekonštruovať tajomstvo. Rekonštrukcia sa robí pomocou Lagrangeovho interpolačného polynómu.

1. Do vzťahu
$$f(x) = \sum_{i=1}^{t} (f(x_i) \cdot \prod_{\substack{j=1 \\ i \neq j}}^{t} \frac{x - x_j}{x_i - x_j})$$
dosadíme príslušné x_i, x_j a $f(x_i)$.
2. Vypočítame $f(0) = s$.

Feldmanova schéma Feldmanová schéma na zdieľanie tajomstva vznikla rozšírením Shamirovej metódy o možnosť príjemcov overiť si konzistenciu podielov na tajomstve, ktoré obdržali od dealera a možnosť vylúčiť pri rekonštrukcii tajomstva nekorektné podiely obdržané od nečestných účastníkov. Konzistencia podielov na tajomstve jednotlivých účastníkov znamená, že každá podmnožina $t+1$ podielov dáva rovnaké tajomstvo.

Podobne ako v Shamirovej schéme dealer vygeneruje náhodný polynóm $f(x)$ stupňa t nad Z_p taký, že $f(0) = s$ a každému účastníkovi pošle jeho podiel na tajomstve $(x_i, f(x_i))$. Dealer navyše zverejní verifikačné hodnoty $A_k = g^{a_k} \bmod p$ pre $k = 0, \ldots, t$. Účastníci si môžu skontrolovať či hodnoty s_i skutočne predstavujú podiely na tajomstve overením platnosti vzťahu

$$g^{s_i} = \prod_{k=0}^{t} (A_k)^{x_i^k} \bmod p$$

Ak účastnk P_i obdrží podiel, pre ktorý táto podmienka neplatí, zverejní sťažnosť voči dealerovi. Dealer odhalí podiel s_i každého sťažujúceho sa účastníka P_i. Ak niektorý z odhalených podielov nespĺňa vyššie uvedenú podmienku, dealer je diskvalifikovaný. Rovnakú podmienku použijeme aj pri rekonštrukcii tajomstva na detekciu nekorektných podielov obdržaných od nečestných účastníkov.

Pedersenova schéma Narozdiel od Feldmanovej metódy poskytuje dokonalú tajnosť podielov na tajomstve. Predpokladáme tu však to, že útočník (hlave v roli dealera) nevie riešiť problém diskrétneho logaritmu.

Dealer náhodne vygeneruje dva polynómy $f(z), f'(z)$ stupňa t nad Z_p také, že $f(0) = s$ je zdieľané tajomstvo. Každmu účastníkovi pošle jeho tajný podiel (s_i, s_i'), kde $s_i = f(z_i), s_i' = f'(z_i)$. Dealer taktiež zverejní hodnoty $C_k = g^{a_k} h^{b_k} \bmod p$ pre $k = 0, \ldots, t$ kde $f(z) = \sum_k a_k z^k$ a $f'(z) = \sum_k b_k z^k$. Účastníci si môžu skontrolovať či hodnoty s_i, s_i' skutočne predstavujú tajomstvá overením platnosti vzťahu

$$g^{s_i} h^{s_i'} = \prod_{k=0}^{t} (C_k)^{x_i^k} \bmod p$$

Ak účastník P_i obdrží podiel, pre ktorý táto podmienka neplatí, zverejní sťažnosť voči dealerovi. Dealer odhalí podiel (s_i, s_i') každého sťažujúceho sa účastníka P_i. Ak niektorý z odhalených podielov nespĺňa vyššie uvedenú podmienku, dealer je diskvalifikovaný.

3 Návrh schémy

3.1 Prahový ElGamal kryptosystém

Prahové šifrovacie systémy majú za úlohu nazdielať súkromný dešifrovací kľúč medzi účastníkov systému tak, že dešifrovať jednotlivé správy je možné len za spolupráce určitej skupiny účastníkov. Šifrovanie správ prebieha v prahovej verzii ElGamalovho kryptosystému rovnako ako v pôvodnej verzii. Potrebujeme však zmeniť postup pri generovaní kľúčov a dešifrovaní správ.

Generovanie kľúčov. Nech $P = \{P_1, \ldots, P_n\}$ je množina účastníkov systému. Účelom generovania kľúčov je to, aby každý účastník P_i obdržal tajný podiel x_i zo súkromného kľúča x. Verejný kľúč y po generovaní poznajú všetci účastníci. Každý účastník P_i musí zverejniť hodnotu $y_i = g^{x_i}$. Súkromné podiely x_i sú také, že tajná hodnota x môže byť zrekonštruovaná z každej skupiny $t+1$ podielov. Akákoľvek množina t spolupracujúcich účastníkov nedokáže odhaliť tajnú hodnotu x. Nazdieľanie tajnej hodnoty x medzi účastníkov systému môžme dosiahnuť použitím Shamirovej $(t+1, n)$ schémy na zdieľanie tajomstva. Táto schéma však predpokladá prítomnosť dôveryhodnej tretej strany. Pre naše účely použijeme bezpečné distribuované generovanie kľúčov, ktorého popis je v ďalšej sekcii. Čiže platí:

$$x = \sum_{i \in P} x_i \lambda_{i,P} \qquad \lambda_{i,P} = \prod_{l \in P - \{i\}} \frac{l}{l - i}$$

Verejný kľúč je (p, g, y), kde $y = g^x$. Hodnota x predstavuje súkromný kľúč.

Dešifrovanie. Ak chcú účastníci dešifrovať správu $(r, s) = (g^k, y^k m)$ bez odhalenia tajnej hodnoty x, musia vykonať nasledujúci protokol.

1. Každý účastník P_i zverejní hodnotu $w_i = r^{x_i}$ a zero-knowledge dôkazom ukáže, že
$$\log_g y_i = log_r w_i$$
2. Nech P je množina $t+1$ účastníkov, ktorí uspeli v zero-knowledge dôkaze. Správa môže byť zrekonštruovaná ako
$$m = \frac{s}{r^x}$$
$$r^x = r^{\sum_{i \in P} x_i \lambda_{i,P}} = \prod_{i \in P} w_i^{\lambda_i, P}$$

Z $(t+1)$ známych podielov na tajomstve x môžme Lagrangeovou interpolačnou metódou odhaliť tajomstvo a správu dešifrovať ako v pôvodnej verzii ElGamal šifrovacieho systému.

3.2 Distribuované generovanie kľúčov

V tejto sekcii ukážeme ako vygenerovať dvojicu čísel (x, y) takú, že platí :

- x je súkromný kľúč a y k nemu prislúchajúci verejný kľúč v ElGamal šifrovacom systéme;
- y je po ukončení protokolu známe všetkým účastníkom;
- x je nazdieľané medzi účastníkov systému tak, že každá skupina $t+1$ čestných účastníkov môže túto tajnú hodnotu odhaliť.

Vykonaním tohto protokolu (ďalej len `DKG` - protokol) v našom systéme vytvoríme inštanciu prahového ElGamal kryptosystému. Šifrovanie a dešifrovanie v tomto systéme sme ukázali v predchádzajúcej sekcii.

Generovanie x

1. Každý účastník P_i, vykonaním Pedersenovho protokolu v roli dealera, nazdieľa náhodne vygenerovanú hodnotu z_i:
   (a) P_i si náhodne zvolí dva polynómy $f_i(z), f_i'(z)$ stupňa t nad Z_q:

   $$f_i(z) = a_{i0} + a_{i1}z + \cdots + a_{it}z^t$$

   $$f_i'(z) = b_{i0} + b_{i1}z + \cdots + b_{it}z^t$$

   Nech $z_i = a_{i0} = f_i(0)$. P_i zverejní hodnotu $C_{ik} = g^{a_{ik}}h^{b_{ik}} \bmod p$ pre $k = 0, \ldots, t$. P_i spočíta podiely $s_{ij} = f_i(j), s_{ij}' = f_i'(j) \bmod q$ pre $j = 1, \ldots, n$ a odošle s_{ij}, s_{ij}' účastníkovi P_j.
   (b) Každý účastník P_j si overí podiely, ktoré obdržal od ďalších účastníkov. P_j pre každé $i = 1, \ldots, n$ skontroluje, či platí

   $$g^{s_{ij}}h^{s_{ij}'} = \prod_{k=0}^{t}(C_{ik})^{j^k} \bmod p \qquad \text{(A)}$$

   Ak pre nejaké i vzťah (A) neplatí, P_j zverejní sťažnosť voči účastníkovi P_i.
   (c) Každý účastník P_i, ktorý ako dealer obdržal sťažnosť od účastníka P_j, zverejní hodnoty s_{ij}, s_{ij}' spĺňajúce vzťah (A).
   (d) Diskvalifikovaný je každý účastník, ktorý buď
   - v kroku 1b obdržal viac ako t sťažností, alebo
   - v kroku 1c odpovedal na sťažnosť hodnotou nespĺňajúcou podmienku (A).
2. Každý účastník si vytvorí množinu nediskvalifikovaných účastníkov $QUAL$. (Všetci čestní účastníci si vytvoria rovnakú množinu, preto ju pre jednoduchosť označíme unikátnym globálnym menom.)
3. Žiadny účastník nedokáže explicitne vypočítať tajnú hodnotu x, pretože platí $x = \sum_{i \in QUAL} z_i \bmod q$. Každý účastník P_i si nastaví svoj podiel na tajomstve ako $x_i = \sum_{j \in QUAL} s_{ji} \bmod q$ a $x_i' = \sum_{j \in QUAL} s_{ji}' \bmod q$.

Zostrojenie $y = g^x \bmod p$

4. Každý účastník P_i,$i \in QUAL$, získa $y_i = g^{z_i} \bmod p$ pomocou Feldmanovej metódy:
   (a) Každý účastník P_i,$i \in QUAL$, zverejní $A_{ik} = g^{a_{ik}} \bmod p$ pre $k = 0, \ldots, t$.
   (b) Každý účastník P_j si overí zverejnené hodnoty účastníkov z množiny $QUAL$ tak, že pre každé $i \in QUAL$ skontroluje platnosť vzťahu

$$g^{s_{ij}} = \prod_{k=0}^{t} (A_{ik})^{j^k} \bmod p \qquad \text{(B)}$$

   Ak pre nejaký index i vzťah neplatí, P_j sa sťažuje voči P_i zverejnením hodnôt s_{ij}, s'_{ij}, ktoré spĺňajú podmienku (A), ale neplatí pre nich podmienka (B).
   (c) Pre účastníkov P_i, ktorí obdržali aspoň jednu platnú sťažnosť (hodnoty, pre ktoré platí (A) a neplatí (B)), ostatní účastníci pomocou rekonštrukčnej fázy Pedersenovho protokolu vypočítajú $z_i, f_i(z), A_{ik}$ pre $k = 0, \ldots, t$. Každému účastníkovi z množiny $QUAL$ nastavíme $y_i = A_{i0} = g^{z_i} \bmod p$. Vypočítame $y = \prod_{i \in QUAL} y_i \bmod p$.

3.3 Kódovanie výsledkov

V tejto časti si ukážeme ako prezentovať hlasy jednotlivých respondentov tak, aby dotazovateľ mohol určiť presný výsledok hlasovania (ankety). To znamená, že dotazovateľ vie z obdržaného kódu výsledku pre každú voľbu $a_1, \ldots, a_L$ zistiť počet respondentov, ktorí si ju zvolili.

Ak dotazovateľ zverejní otázku a k nej ponúkané odpovede $a_1, \ldots, a_L$, každý respondent má možnosť zvoliť si práve jednu, alebo žiadnu z týchto L odpovedí. Jednotlivé odpovede sú reprezentované ako čísla $l_1, \ldots, l_L$ v $(N+1)$ - ovej sústave.

Ak si respondent zvolí odpoveď a_i, tak dotazovateľovi odošle šifru $E(v)$, kde správa $v = g^{l_i}$. Z homomorfických vlastností ElGamalovho šifrovacieho systému vyplýva, že ak dotazovateľ obdrží šifry

$$E(v_1) = (g^{k_1}, y^{k_1} g^{l_a}) \qquad \text{a} \qquad E(v_2) = (g^{k_2}, y^{k_2} g^{l_b})$$

, kde $v_1 = g^{l_a}, v_2 = g^{l_b}$, vie spraviť

$$E(v_1) \cdot E(v_2) = E(v_1 \cdot v_2) = (g^{k_1+k_2}, y^{k_1+k_2} g^{l_a+l_b})$$

Po dešifrovaní šifry $E(v_1 \cdot v_2)$ získa dotazovateľ hodnotu $v_1 \cdot v_2 = g^{l_a+l_b}$.

l_i	$(N+1)^{L-1}$	...	$(N+1)^2$	$(N+1)^1$	$(N+1)^0$
l_0	0		0	0	0
l_1	0		0	0	1
l_2	0		0	1	0
l_3	0		1	0	0
$\vdots$					
l_L	1		0	0	0

Tabuľka 1. Kódovanie odpovedí

3.4 Komunikačný protokol

V tejto sekcii si predstavíme a podrobne vysvetlíme nami navrhnutý komunikačný protokol pre bezpečné elektronické hlasovanie vrámci spoločnej broadcastovej domény. Tento komunikačný protokol sa skladá zo štyroch hlavných častí.

Prvú časť nášho protokolu predstavuje registračná fáza. Po jej ukončení je známy iniciátor hlasovania (dotazovateľ) a respondenti, ktorí sú oprávnení hlasovať.

V druhej časti protokolu vstupujú registrovaní respondenti do fázy generovania kľúčov. Cieľom tejto fázy je vygenerovať verejný šifrovací a k nemu prislúšný súkromný dešifrovací kľúč v ElGamal prahovom šifrovacom systéme tak, že dešifrovací kľúč je po častiach rozdelený medzi registrovaných respondentov. Každý registrovaný respondent teda pozná verejný kľúč a svoj podiel zo súkromného dešifrovacieho kľúča. Z toho vyplýva, že zašifrovať správu môže každý respondent, avšak na dešifrovanie zašifrovanej správy je potrebná spolupráca určitého minimálneho počtu respondetov.

Po vygenerovaní kľúčov začína tretia fáza, ktorou je už samotné hlasovanie. V tejto časti komunikácie dotazovateľ zverejní anketu a k nej ponúkne na výber niekoľko možných volieb. Každý respondent pošle dotazovateľovi svoj hlas šifrovaný verejným kľúčom, ktorý si registrovaní respondenti vygenerovali v predchádzajúcej fáze. Po skončení tejto časti komunikácie má dotazovateľ k dispozícii zašifrovaný výsledok ankety.

V poslednej časti komunikácie zverejní dotazovateľ ankety jej šifrovaný výsledok. Respondenti následne vykonajú protokol, v ktorom tento výsledok spoločne dešifrujú. Dešifrovací protokol je navrhnutý tak, že po dešifrovaní správy zostáva súkromný dešifrovací kľúč aj naďalej nazdieľaný medzi respondentmi (dešifrovací kľúč ani žiadna z jeho tajných časti neboli počas dešifrovania zverejnené). Táto vlastnosť umožňuje dotazovateľovi inicializovať hlasovanie pre novú anketu bez toho, aby účastníci museli znova uskutočniť protokoly prvej a druhej fázy. Hlasovať v novovytvorenej ankete však môžu len respondenti, ktorí sa zaregistrovali pred prvou anketou. Ak chce dotazovateľ umožniť hlasovanie novým účastníkom, musí opäť vyvolať registračnú fázu a fázu generovania kľúčov.

V popise komunikačného protokolu používame nasledujúce značenia :

PK_Q, SK_Q : verejný a súkromný kľúč dotazovateľa (questioner)
PK_Q^s, SK_Q^s : overovací a podpisovací kľúč dotazovateľa
PK : verejný kľúč dotazníka (questionary)
SK : súkromný kľúč dotazníka nazdieľaný medzi respondentov
PK_i, SK_i : verejný a súkromný kľúč i -teho respondenta
PK_i^s, SK_i^s : overovací a podpisovací kľúč i -teho respondenta
$E_{PK}(m)$: správa m zašifrovaná kľúčom PK
$S_{SK}(m)$: správa m podpísaná podpisovacím kľúčom SK
$h(m)$: výsledok haš funkcie zo správy m

Registrácia Predpokladom protokolu je priamy kontakt všetkých účastníkov (všetci sú v jednej posluchárni, zasadacej miestnosti, ...). Dotazovateľ (questioner) ešte pred začatím elektronickej komunikácie musí zverejniť heslo pre vygenerovanie svojho verejného kľúča PK_Q mimo komunikačnú sieť (napíše ho na tabuľu, na papier, alebo ho prezradí ústne).

Elektronickú komunikáciu inicializuje dotazovateľ. Broadcastom ($\star$) zverejní identifikátor dotazníka (questionary) qid, identifikátor dotazovateľa Q a verejný overovací kľúč dotazovateľa PK_Q^s. Výstup hašovacej funkcie $h(qid, Q)$, ktorý vznikol po jej aplikovaní na identifikátor dotazníka qid a identifikátor dotazovateľa Q, podpíše svojím podpisovacím kľúčom SK_Q^s a pripojí na koniec tejto zverejnenej správy (1).

$$Q \to \star : \quad qid, Q, PK_Q^s, S_{SK_Q^s}(h(qid, Q)) \tag{1}$$

$$R_i \to Q : \quad E_{PK_Q}(R_i, PK_i, PK_i^s), S_{SK_i^s}(h(qid, R_i, PK_i, PK_i^s)) \tag{2}$$

Respondenti, ktorí majú záujem o účasť na tvorbe dotazníka, sa musia k dannému dotazníku zaregistrovať. Registráciou získavajú respondenti oprávnenosť hlasovať pri jednotlivých otázkach dotazníka.

Každý respondent R_i, ktorý sa chce zaregistrovať, si najprv musí vygenerovať verejný šifrovací kľúč PK_Q dotazovateľa Q. Tento verejný kľúč si vygeneruje z hesla, ktoré prezradil dotazovateľ ešte pred zahájením registrácie. Ďalším krokom respondenta R_i je vygenerovanie si dvoch párov asymetrických kľúčov:

- (PK_i, SK_i)
  - verejný šifrovací kľúč PK_i
  - príslušný súkromný dešifrovací kľúč SK_i
- (PK_i^s, SK_i^s)
  - verejný overovací kľúč PK_i^s
  - príslušný súkromný podpisovací kľúč SK_i^s

Respondent následne posiela dotazovateľovi registračnú správu (2). Prvá časť tejto správy obsahuje identifikátor respondenta R_i, jeho verejný šifrovací kľúč PK_i a jeho verejný overovací kľúč PK_i^s, ktoré sú šifrované verejným kľúčom

dotazovateľa. Druhú časť správy tvorí výstup hašovacej funkcie, dosiahnutý zo vstupu (qid, R_i, PK_i, PK_i^s), podpísaný podpisovacím kľúčom respondenta.

Dotazovateľ príma od respondentov registračné správy určitú dobu. Po uplynutí tohto časového limitu už respondenti nemajú možnosť registrácie. Dotazovateľ má po ukončení čakania na registračné správy k dispozícii zoznam registrovaných respondentov, ich verejné šifrovacie kľúče a ich verejné overovacie kľúče. Tento zoznam podpísaný podpisovacím kľúčom SK_Q^s musí sprístupniť všetkým registrovaným respondentom.

Generovanie kľúčov Cieľom tejto časti je vygenerovanie dotazníkového verejného šifrovacieho kľúča PK a dotazníkového súkromného dešifrovacieho kľúča SK takým spôsobom, že verejný kľúč PK po vygenerovaní poznajú všetci registrovaní respondenti, kým súkromný kľúč SK je medzi nich rozdelený po častiach.

Generovanie kľúčov inicializuje účastník, ktorý v predchádzajúcej registračnej fáze vystupoval ako dotazovateľ. Dotazovateľ teda broadcastom zverejní inicializačnú správu (3) fázy generovania kľúčov. Táto správa obsahuje identifikátor dotazníka qid, pre ktorý sa budú generovať kľúče a haš hodnotu z tohto identifikátora podpísanú dotazovateľovým podpisovacím kľúčom SK_Q^s.

Každý registrovaný respondent postupuje podľa protokolu pre distribuované generovanie kľúčov. V prvom kroku tohto protokolu musí každý účastník (respondent R_i) zverejniť hodnoty $C_{i0}, \ldots, C_{it}$. Tieto hodnoty spolu s identifikátorom respondenta R_i a podpísaným hašom z týchto hodnôt pošle každý respondent dotazovateľovi (4), ktorý ich zverejní všetkým respondentom.

$$Q \to \star: \quad qid, S_{SK_Q^s}(h(qid)) \tag{3}$$

$$R_i \to Q: \quad R_i, C_{i0}, \ldots, C_{it}, S_{SK_i^s}(h(C_{i0}, \ldots, C_{it})) \tag{4}$$

$$R_i \to R_j: \quad E_{PK_j}(R_i, s_{ij}, s'_{ij}), S_{SK_i^s}(h(qid, R_i, s_{ij}, s'_{ij})) \tag{5}$$

$$R_i \to Q: \quad R_i, A_{i0}, \ldots, A_{it}, S_{SK_i^s}(h(A_{i0}, \ldots, A_{it})) \tag{6}$$

Každý respondent R_i vypočta každému respondentovi R_j $(i \neq j)$ hodnoty s_{ij}, s'_{ij}, ktoré mu následne pošle v správe (5). Hlavičku správy predstavuje šifrovaný text, ktorý vznikol zašifrovaním identifikátora odosielateľa R_i a hodnôt s_{ij}, s'_{ij} verejným kľúčom PK_j príjemcu R_j. Odosielateľ R_i na koniec správy pridá jeho podpisovacím kľúčom SK_i^s podpísaný haš, ktorý vznikol aplikáciou použitej hašovacej funkcie na vstup tvorený identifikátorom dotazníka qid, identifikátorom odosielateľa R_i, a hodnôt s_{ij}, s'_{ij}.

Každý respondent R_j si skontroluje korektnosť všetkých obdržaných dvojíc (s_{ij}, s'_{ij}) overením platnosti vzťahu (A). Ak pre niektorú dvojicu (s_{ij}, s'_{ij}) tento vzťah neplatí, respondent R_j zverejní sťažnosť voči respondentovi R_i broadcastovou správou (5a). Ak sa voči respondentovi R_i sťažovalo viac ako t respondetov, je z generovania kľúčov vylúčený. Inak musí R_i v správe (5b) zverejniť hotnoty (s_{ij}, s'_{ij}), pre ktoré vzťah (A) platí.

$$R_j \to \star: \quad R_j, R_i, S_{SK_j^s}(h(R_j, R_i)) \tag{5a}$$

$$R_i \to \star: \quad R_i, R_j, s_{ij}, s'_{ij}, S_{SK_i^s}(h(R_j, s_{ij}, s'_{ij})) \tag{5b}$$

Teraz si je každý respondent R_i schopný (podľa tretieho kroku distribuovaného generovania kľúčov) lokálne vypočítať svoj podiel na súkromnom dešifrovacom kľúči SK, pričom kľúč ako celok nedokáže vypočítať žiaden z účastníkov. Potrebujeme ešte zverejniť dotazníkový verejný šifrovací kľúč PK. Každý respondent pošle dotazovateľovi (podobne ako v správe (4) hodnoty $C_{i0}, \ldots, C_{it}$) v správe (6) hodnoty $A_{i0}, \ldots, A_{it}$. Dotazovateľ tieto hodnoty zverejní pre zvyšných respondentov.

Každý respondent R_j kontroluje korektnosť týchto zverejnených hodnôt tak, že každému respondentovi R_i $(i \neq j)$ overí platnosť vzťahu (B). Ak pre niektorého respondenta R_i tento vzťah neplatí, respondent R_j zverejní sťažnosť voči respondentovi R_i broadcastovou správou (6a), ktorá obsahuje hodnoty s_{ij}, s'_{ij}. Ak neboli zverejnené žiadne sťažnosti, každý respondent si teraz podľa bodu 4(c) distribuovaného generovania kľúčov vie lokálne vypočítať verejný šifrovací kľúč PK. Ak však bola zverejnená sťažnosť napríklad voči respondentovi R_i, každý zvyšný respondent R_j pošle zadávateľovi v správe (6b) hodnotu s_{ij}, ktorý ju zverejní. Z týchto hodnôt dokážu čestní respondenti zrekonštruovať hodnotu A_{i0}, ktorá je potrebná na výpočet verejného šifrovacieho kľúča PK.

$$R_j \rightarrow \star : \quad R_j, R_i, s_{ij}, s'_{ij}, S_{SK_j^s}(h(R_j, R_i, s_{ij}, s'_{ij})) \tag{6a}$$

$$R_j \rightarrow Q : \quad R_j, R_i, s_{ij}, S_{SK_j^s}(h(R_j, R_i, s_{ij})) \tag{6b}$$

Hlasovanie Hlasovanie inicializuje dotazovateľ, ktorý v broadcastovej správe zverejní znenie otázky (7), ktorého súčasťou sú aj ponúkané odpovede $a_1, \ldots, a_L$. Za otázku *question* v inicializačnej správe tejto fázy dotazovateľ pripojí jeho podpisovacím kľúčom SK_Q^s podpísanú haš hodnotu, ktorá vznikla zo vstupu tvoreného identifikátorom dotazníka *qid*, identifikátorom otázky *quid* a samotným textom otázky.

$$Q \rightarrow \star : \quad quid, question, S_{SK_Q^s}(h(qid, quid, question)) \tag{7}$$

$$R_i \rightarrow Q : \quad E_{PK}(v_j), ZP_{1-of-L}(v_j), S_{SK_i^s}(h(E_{PK}(v_j), ZP_{1-of-L}(v_j))) \tag{8}$$

Po prijatí inicializačnej správy si každý respondent R_i zvolí jednu odpoveď a_j. Túto odpoveď zašifruje verejným kľúčom dotazníka PK, ktorý si respondenti vygenerovali v predchádzajúcej fáze. Pomocou neinteraktívnej metódy vypočíta dôkaz $ZP_{1-of-L}(v_j)$ toho, že šifra $E_{PK}(v_j)$ vznikla aplikáciou kľúča PK na jednu z L povolených hodnôt $v_1, \ldots, v_L$. Respondent R_i z dôkazu a šifry vypočíta haš hodnotu, ktorú podpíše svojím podpisovacím kľúčom SK_i^s. Šifru, dôkaz a podpísaný haš pošle respondent R_i dotazovateľovi (8).

Spočítanie výsledkov Po obdržaní šifier hlasov od respondentov musí dotazovateľ jednotlivé hlasy pomocou priloženého dôkazu overiť. Do výsledku hlasovania (*result*) sa započítavajú len tie hlasy, ku ktorým bol priložený korektný dôkaz. Vďaka homomorfickým vlastnostiam použitej šifrovacej schémy môže dotazovateľ lokálne spočítať šifru výsledku :

$$E_{PK}(result) = E_{PK}(v_{j_1}) \ldots E_{PK}(v_{j_N}) = E_{PK}(v_{j_1} + \cdots + v_{j_N})$$

Tento šifrovaný výsledok zverejní (9) v hlavičke inicializačnej správy tejto fázy. Táto hlavička musí obsahovať aj identifikátory dotazníka a otázky. Celá správa sa skladá z hlavičky a dotazovateľom podpísanej haš hodnoty z hlavičky správy.

$$Q \rightarrow \star : \quad qid, quid, E_{PK}(result), S_{SK_Q^s}(h(qid, quid, E_{PK}(result))) \tag{9}$$

$$R_i \rightarrow \star : \quad w_i, ZP_{DLE}(w_i), S_{SK_i^s}(h(qid, quid, w_i, ZP_{DLE}(w_i))) \tag{10}$$

Respondenti teraz pomocou `DKG` - protokolu spoločne dešifrujú výsledok hlasovania. V tomto protokole musí každý respondent zverejniť hodnotu w_i a dôkaz jej korektnosti. V našom komunikačnom protokole to každý respondent uskutoční v správe (10), kde $ZP_{DLE}(w_i)$ je dôkaz korektnosti hodnoty w_i. Po zverejnení hodnôt $w_1, \ldots, w_N$ si každý respondent dokáže lokálne dešifrovať výsledky hlasovania.

4 Záver

V tejto práci sme predstavili schému pre bezpečné elektronické hlasovanie na spoločnej broadcastovej doméne. Detailne sme popísali registračnú fázu, fázu generovanie kľúčov, priebeh hlasovania a zverejnenia výsledkov.

V ďalšej práci by sme chceli navrhnutú schému implementovať a formálne dokázať jej bezpečnostné vlastnoti.

Literatúra

[1] Rosario Gennaro, Stanislav Jarecki, Hugo Krawczyk, Tal Rabin: Secure distributed key generation for discrete-log basedcryptosystems. EUROCRYPT'99, 1999.

[2] A. Menezes, P. van Oorshot, S. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.