Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Elektronické hlasovanie pri malom počte hlasujúcich

diplomová práca

2017

Bc. Marián Horňák

Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Elektronické hlasovanie pri malom počte hlasujúcich

diplomová práca

Študijný program:	Informatika
Študijný odbor:	2508 Informatka
Školiace pracovisko:	Katedra Informatiky
Školiteľ:	doc. RNDr. Daniel Olejár, PhD.

Bratislava, 2017

Bc. Marián Horňák

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Marián Horňák
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Elektronické hlasovanie pri malom počte hlasujúcich
Electronic voting with small number of voters

Cieľ: Návrh a teoretické zdôvodnenie systému umožňujúcemu elektronické hlasovanie (prezenčné aj dištančné) v malej skupine hlasujúcich (napríklad obhajoby dizertácií, hlasovanie v pracovnej skupine a pod.) Elektronické hlasovanie by malo mať rovnakú účinnosť ako hlasovanie klasickým spôsobom.

Kľúčové slová: elektronické hlasovanie, bezpečnosť, právna účinnosť hlasovania

Vedúci: doc. RNDr. Daniel Olejár, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Dátum zadania: 15.03.2017

Dátum schválenia: 25.04.2017 prof. RNDr. Rastislav Kráľovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie:

Ďakujem školiteľovi za nápad, spolubývajúcim za rozptyľovanie, kamarátom za podporu, kolegom za trpezlivosť, študijnej referentke za pevné nervy a rodine za pochopenie.

Abstrakt

Predmetom mnohých prác zameraných na kryptograficky bezpečné hlasovanie sú národné voľby. Tieto sú veľkoplošné, prebiehajú počas dlhšieho časového intervalu a predpokladajú špeciálne technické vybavenie. V našej práci sa, naopak, zameriame na hlasovania malých skupín ľudí, prebiehajúce v krátkom čase na jednom mieste a iba s bežnými osobnými zariadeniami. Identifikujeme hlavné problémy v týchto situáciách a navrhneme hlasovací protokol, ktorý ich rieši. Medzi najdôležitejšie vlastnosti patrí minimalizácia nutného počtu autorít a možnosť hlasovať bez vlastného zariadenia so zachovaním overiteľnosti a dôvernosti. Protokol tiež formálne zadefinujeme, čím uľahčíme jeho implementáciu. **Kľúčové slová: elektronické hlasovanie, bezpečnosť**

Abstract

The national elections are subject of many studies in the field of cryptographically secure voting. Usually, they are large-scale, they last for a longer period of time and they require some special hardware. Our aim, however, is to look at the voting of the small group of people that takes place in a single room, during the short period of time and with the basic personals devices available. We'll identify the major challenges of those situations and we'll suggest the voting protocol to solve them. The most important features are the reduction of the number of authoritires and the possibility to vote without personal device while preserving the verifiability and privacy. The protocol is also defined formally which should make the implementation easier. **Keywords: electronic voting, security**

Obsah

Úvod **1**

1 Základné pojmy **2**
1.1 Hlasovanie 2
1.2 Vlastnosti hlasovacieho protokolu 4
1.3 Účastníci hlasovania 7

2 Súvisiaci výskum **8**
2.1 Kryptografické konštrukcie 8
2.2 Hlasovacie protokoly 10

3 Hlasovnia malého rozsahu **12**
3.1 Súčasná prax 12
3.2 Aplikovateľnosť elektronického hlasovania 13
3.3 Modelová situácia 15

4 Návrh hlasovacieho protokolu **16**
4.1 Využitie osobných zariadení 16
4.2 Účastníci hlasovacieho procesu 17
4.3 Jadro protokolu 20
4.4 Hlasovanie bez zariadenia 22
4.5 Podporné mechanizmy 25

5 Formalizácia **27**
5.1 Východiskové konštrukcie 27
5.2 Typy správ 31
5.3 Vlastnosti správ 38

6 Výsledky **41**
6.1 Hlasovanie v reálnom čase ako slabo pokrytá oblasť 41
6.2 Protokol 41
6.3 Implementácia 42

Záver **44**

Príloha A **48**

Úvod

Mnoho každodenných procesov a služieb sa postupne v rámci zvyšovania efektivity a bezpečnosti elektronizuje. Môže sa zdať preto prekvapivé, že pri voľbách a hlasovaniach, ktoré sa snažíme elektronizovať už viac ako tridsať rokov, ešte stále výrazne prevládajú pôvodné, fyzické procesy. Nenecháme sa však týmto nepriaznivým faktom odradiť a pokúsime sa navrhnúť elektronizáciu špecifických hlasovacích situácií. Zistíme, aké sú ich krytické požiadavky a pokúsime sa navrhnúť kryptograficky bezpečný hlasovací protokol, ktorý tieto požiadavky spĺňa. S prekvapením zistíme, že súčasťou riešenia je tiež niekoľko teoreticky zaujímavých kryptografických konštrukcií.

Východiskovými situáciami budú hlasovania malých skupín ľudí, prebiehajúce na jednom mieste a v krátkom čase. Príkladom je hlasovanie poslancov mestkého zastupiteľstva alebo voľby nového predsedu na bytovej schôdzi. Napriek tomu, že pri takýchto hlasovaniach môže byť jednoduchšie použiť klasické hlasovanie s urnou, občas sa stane, že by chcel anonymne hlasovať aj hlasujúci, ktorý sa zúčastňuje diskusie cez videohovor alebo že vznikne podozrenie z podvodu. V oboch prípadoch je vhodným riešním použitie kryptograficky bezpečného hlasovania.

Na úvod práce si definujeme dôležité základné pojmy, ktoré budeme neskôr často využívať. Okrem pojmov týkajúcich sa hlasovania budeme potrebovať aj pojmy súvisiace s elektronickým hlasovaním, ktoré si predstavíme spolu s prehľadom najdôležitejšieho výskumu súvisiaceho s touto prácou. Ďalším krokom bude rozbor východiskových situácií a identifikácia ich spoločných znakov. Na základe týchto poznatkov potom vytvoríme modelovú hlasovaciu situáciu, pre ktorú bude treba navrhnúť protokol. Tomu sa bude venovať ďalšia kapitola, ktorá postupne popíše a odvôvodní, všetky dôležité návrhové rozhodnutia, ktoré nás viedli k finálnej podobe protokolu. Formálnym zápisom sa následne nielen pokúsime odvôvodniť tvrdenia, ktoré sme o protokole vyslovili, ale aj predspracujeme protokol pre prípadnú implementáciu. O možnostiach implementácie ako aj uskutočnených pokusoch budeme diskutovať v poslednej časti.

Najdôležitejšia časť práce je koncentrovaná najme v sekciách 4.4.3 a 5.1.3, kde sa popisuje implementácia hlasovania bez zariadenia. Zaujímavá je tiež sekcia 5.2 obsahujúca pôvodný formalizmus na popis protokolu.

1 Základné pojmy

Pojmy súvisiace s elektronickým hlasovaním alebo s hlasovaním vo všeobecnosti majú širokú škálu rôznych interpretácií. V tejto kapitole si preto dôležité pojmy vysvetlíme a zadefinujeme. Ako ilustračné príklady budeme využívať modely papierových volieb, ktoré by mali byť pre čitateľa známejšie ako ich elektronické alternatívy.

1.1 Hlasovanie

Hlasovanie možno vo všeobecnosti chápať ako proces, pri ktorom každý zo skupiny hlasujúcich vyjadrí svoj názor prostredníctvom syntakticky obmedzeného hlasu a následne sa podľa vopred dohodnutého postupu hlasy skombinujú do výsledku hlasovania, ktorý reprezentuje názor skupiny. V ďalšom texte si postupne rozoberieme jednotlivé spomenuté pojmy.

1.1.1 Hlasujúci

Hlasujúcim môže byť ľubovoľná entita obhajujúca názor. V prípade logických úvah bude pre nás pri hlasujúcom dôležitý iba jeho hlas a jednoznačná identifikovateľnosť. Pri fyzickom návrhu systému však budeme predpokladať, že hlasujúci je reprezentovaný fyzickou osobou. Budeme rozlišovať medzi oprávneným hlasujúcim, ktorý sa hlasovacieho procesu môže zúčastniť, a aktívnym hlasujúcim, ktorý sa procesu zúčastnil. Predpokladáme že oprávnených hlasujúcich je konečne veľa a sú vopred všeobecne známi.

1.1.2 Hlas

Hlasujúci reprezentuje svoj názor prostredníctvom hlasu. Pri súčasných hlasovaniach môže hlas predstavovať napríklad jednoduchú binárnu odpoveď, voľbu niekoľkých z vopred zadaných možností, doplnenie vlastného textu alebo aj kombináciu viacerých z týchto foriem. Pre účeli tejto práce, pokiaľ neuvedieme inak, budeme predpokladať, že hlas obsahuje práve jeden prvok z vopred danej konečnej množiny kandidátov.

Mnoho hlasovacích systémov má možnosť takzvaného zdržania sa hlasovania. Túto možnosť vieme modelovať špeciálnym kandidátom. Trochu odlišným prípadom je neúčasť oprávneného hlasujúceho na hlasovaní. V závislosti od charakteru hlasovania a implementačných detailov sa vieme rozhodnúť medzi reprezentovaním tejto možnosti iným špeciálnym kandidátom alebo absenciou hlasu.

1.1.3 Protokol a proces

Najdôležitejšou časťou hlasovania je hlasovací protokol. Popisuje zozbieranie hlasov jednotlivých hlasujúcich a ich kombináciu do výsledku. Výkon hlasovacieho protokolu budeme nazývať hlasovacím procesom.

Procesu sa okrem samotných hlasujúcich môžu zúčastniť aj ďalšie entity, spolu ich budeme nazývať účastníkmi hlasovania. Počas procesu dochádza k výmene informácií medzi účastníkmi. Na tieto výmeny môžu byť kladené dodatočné vlastnosti (napr. uchovanie obsahu hlasu v tajnosti), ktoré značne komplikujú zdanlivo jednoduchý návrh procesu. Niektoré takéto vlastnosti popíšeme v časti 1.2.

Účastníci hlasovania sa môžu chovať čestne a teda dodržiavať postupy určené protokolom alebo nečestne tieto postupy obchádzať. Aby protokol zabezpečil čestné chovanie, môže vyžadovať dodatočné úkony, ktoré by nečestného účastníka odhalili.

1.1.4 Výsledky

Pod výsledkom hlasovania budeme pre potreby tejto práce rozumieť priradenie, ktoré každému kandidátovi priradí počet hlasov, ktoré ho obsahujú. Alternatívne by sme napríklad od výsledku mohli požadovať aby obsahoval kandidátov zoradených podľa počtu hlasov, avšak bez informácie o počte samotnom. Na protokol by potom mohla byť kladená podmienka, aby sa žiadny z účastníkov hlasovania nedozvedel konrétne počty.

Výsledok hlasovania nemusí byť jediným výstupom hlasovacieho procesu. Častokrát sú zverejnené aj dodatočné informácie, ktoré potrebujeme na dokázanie konrétnych vlastností protokolu.

1.1.5 Definicícia

Pojmy vysvetlené v predchádzajúcich častiach si teraz formálnejšie zadefinujeme. Prvé dve definície budú matematicky exaktné, pretože ich budeme priamo využívať v ďalšom texte.

Definícia 1.1.1. *Parametrami hlasovania nazývame n-ticu* $(\mathcal{U}, \mathcal{H}, \mathcal{H}_{\mathcal{A}}, \mathcal{K}, \langle)$*, kde*

- $\mathcal{U}$ *je konečná množina účastníkov,*

- $\mathcal{H} \supseteq \mathcal{U}$ *je konečná množina oprávnených hlasujúcich,*
- $\mathcal{H}_\mathcal{A} \supseteq \mathcal{H}$ *je konečná množina aktívnych hlasujúcich,*
- $\mathcal{K}$ *je konečná množina kandidátov*
- $a \langle : \mathcal{V}_\mathcal{A} \to \mathcal{K}$ *je konštruktor hlasu.*

Definícia 1.1.2. *Výsledok hlasovania pre dané parametre je* $(\mathcal{U}, \mathcal{H}, \mathcal{H}_\mathcal{A}, \mathcal{K}, \langle)$ *realizácia funkcie* $s : \mathcal{K} \to \mathcal{Z}_0^+$*, kde* $s(k) = |\{x \mid x \in \mathcal{H}, \langle(x) = k\}|$.

Definícia protokolu a procesu je vágnejšia, pre potreby tejto práce však bude dostatočné.

Definícia 1.1.3. *Hlasovací protokol nad parametrami* $\mathcal{P}$ *je séria inštrukcií pre účastníkov hlasovania, ktorých plnením sa dopracujú k výsledku hlasovania pre* $\mathcal{P}$*. Vykon tohto protokolu nazývame hlasovacím procesom.*

1.2 Vlastnosti hlasovacieho protokolu

V tejto časti sa pozrieme na základné vlastnosti, ktoré môžu byť od hlasovacieho protokolu vyžadované. Hlasovacie systémy, ktoré ich spĺňajú, sa v angličtine nazývajú *End-to-end auditable voting systems*. Práve vytváranie takýchto protokolov je potom odborne zaujímavé, či už zo strany kryptológie alebo fyzickej implementácie.

Samotné vlastnosti sú pomerne silné a neočakáva sa, že budú splnené bezpodmienečne. Hlasovací protokol sa často krát spolieha na čestné chovanie niektorých účastníkov, prípadne na fyzické vlastnosti zariadení a komunikačných kanálov. S každou vlastnosťou sa preto uvádza aj zoznam podmienok nevyhnutných pre jej splnenie. Čím jednoduchšie sú tieto podmienky, tým je vlastnosť považovaná za silnejšiu.

1.2.1 Overiteľnosť

Overiteľnosť je možnosť presvedčiť seba alebo inú osobu, že výsledok hlasovania je správny. Absencia overiteľnosti môže účastníkov hlasovania motivovať k nečestnému chovaniu. Neexistuje totiž spôsob, ako takéto chovanie odhaliť. Možnosť podvádzať navyše znižuje dôveru vo výsledok. Je preto očakávateľné, že overiteľnosť bude požadovaná od väčšiny hlasovacích protokolov.

Štandardne sa overiteľnosť delí na tri časti. Tieto časti si postupne zadefinujeme a popíšeme si, ako je možné ich fyzicky zabezpečiť pri malých voľbách v jednej miestnosti s jednou urnou a pri veľkých voľbách s viacerými volebnými miestnosťami a komisiou.

Definícia 1.2.1. *Individuálna overiteľnosť (angl. individual verifiability) je vlastnosť hlasovacieho protokolu, pri ktorej si každý aktívny hlasujúci môže overiť, že jeho hlas je medzi hlasmi spracovanými hlasovacím procesom.*

Je dôležité si všimnúť, že táto vlastnosť hovorí iba o spracovaní hlasu a nie o jeho korektnom zarátaní. Je teda možné, že hlas bude síce spracovaný, ale pred zarátaním bude modifikovaný. V prípade malých volieb dosiahne hlasujúci individuálnu overiteľnosť sledovaním urny od doby, kedy vhodí hlas, po dobu sčítania. Podmienkou overiteľnosti je potom neschopnosť zvyšných účastníkov nepozorovane manipulovať s obsahom urny. Pri veľkých voľbách nie je neustále fyzické sledovanie možné a teda sa overiteľnosť je splnená len sa podmienok, že urnu neustále sleduje volebná komisia a zároveň sa chová čestne.

Definícia 1.2.2. *Všeobecná overiteľnosť (angl. universal verifiability) je vlastnosť hlasovacieho protokolu, pri ktorej si ktokoľvek môže overiť, že hlasovací proces spracoval hlasy korektne.*

Táto vlastnosť hovorí iba o korektnom spracovaní a nie o pôvode hlasov. Pri malých voľbách je možné ju dosiahnuť dohliadaním na samotné sčítanie. Pri veľkých voľbách máme opäť podmienku čestného chovania, v tomto prípade dokonca všetkých komisí súčasne (zaujímavé argumenty by však mohli byť postavené aj na štatistickom výskyte nečestných komisií).

Definícia 1.2.3. *Overiteľnosť platnosti (angl. eligibility verifiability) je vlastnosť hlasovacieho protokolu, pri ktorej si ktokoľvek môže overiť, že každý hlas, spracovaný hlasovacím procesom, bol vytvorený oprávneným hlasujúcim a že každý oprávnený hlasujúci vytvoril najviac jeden takýto hlas.*

Posledná vlastnosť teda vylučuje neplatné hlasy. Fyzicky ju možno zabezpečiť ochranným prvkom na platných hlasovacích lístkoch a evidenciou vytvorených a vydaných platných hlasov. Podmienka je nefalšovateľnosť ochranných prvkov. Veľké voľby požadujú aj v tomto prípade navyše dôveru v komisiu.

Vo vyššie uvedených príkladoch boli podmienky pre overiteľnosť pomerne silné, vyžadujúce čestných jednotlivcov a popierajúce ľudskú vynaliezavosť. Existuje však overiteľné hlasovanie s pomerne slabou podmienkou. Je ním verejné hlasovanie, pri ktorom každý hlasujúci zverejní svoj hlas a sčítavanie môže byť úplne transparentné. Podmienka overiteľnosti je potom iba dostupnosť zverejnených údajov a možnosť protestu v prípade ich nesprávnosti. Takéto hlasovanie však absentuje ďalšiu vlastnosť, dôvernosť.

1.2.2 Dôvernosť

Definícia 1.2.4. *Dôvernosť (angl. secrecy) je vlastnosť hlasovacieho protokolu, pri ktorej nikto okrem autora nedokáže zistiť obsah hlasu.*

Potreba dôvernosti hlasovacieho protokolu závisí od charakteru hlasovania. Hlasovania v poslancov mestkých zastupiteľstvách môžu byť verejné, aby si občania mohli spraviť predstavu o ich názoroch. Pri voľbách do mestkého zastupiteľstva sa, naopak, dôvernosť považuje za základné právo každého voliča. V prípadoch, kedy dôvernosť nie je potrebná, zvyčajne možno použiť už spomínané verejné hlasovanie. V ďalšom texte teda bude dôvernosť zväčša vyžadovaná.

Pri klasických hlasovaniach sa zvyčajne dôvernosť dosahuje vypĺňaním hlasu za plentou. Medzi podmienky dôvernosti potom patrí absencia monitorovacieho zariadenia v tomto priestore a nerozlíšiteľnosť jednotlivých hlasov.

1.2.3 Nedokladovateľnosť

Definícia 1.2.5. *Nedokladovateľnosť (angl. receipt freeness) je vlastnosť hlasovacieho protokolu, pri ktorej žiadny hlasujúci nevie druhej strane dokázať akúkoľvek informáciu o obsahu svojho hlasu.*

Nedokladovateľnosť chráni hlasovací proces pred vonkajším vplyvom. Útočník by sa mohol pokúsiť ovplyvniť hlas hlasujúceho nebezpečným vyhrážaním alebo výmenou za finančnú odmenu. Pokiaľ však nebude existovať spôsob, ktorým hlasujúci dokáže, že tak naozaj konal, môže sa rozhodnúť nezávisle od vonkajšieho vplyvu. Tým sa ovlyvňovanie stáva pre útočníka nevýhodné.

O nedokladovateľnosti má zmysel uvažovať iba v prípade dôverného hlasovacieho protokolu. Ďalšou podmienkou je neexistencia kandidátov s potenciálne nulovým počtom hlasov – hlasujúci by nehlasovaním za takéhoto kandidáta riskoval, že kandidát nezíska žiadne hlasy a teda bude jeho konanie odhalené.

V prípade parlamentných volieb, pri ktorých dostane hlasujúci zoznamy kandidátov za všetky strany, ale ako hlas použije iba jeden z nich, môže byť odovzdanie zvyšných zoznamov považované za dôkaz, že hlasoval v prospech konkrétnej parlamentnej strany. Prevenciou môže byť povinné odovzdanie týchto zoznamov pred odchodom z volebnej miestnosti.

1.2.4 Robustnosť

Robustnosť hlasovacieho protokolu je jeho schopnosť dopracovať sa k výsledku hlasovania aj v prípade chyby alebo zámerného škodlivého správania sa. Robustnosťou sa nebudeme zaoberať z formálneho hľadiska a teda sme nesformulovali ani jej definíciu.

Je však dôležité skúmať, ako sa proces vyvinie v prípade neočakávaného chovania a prípadne definovať správanie sa čestných účastníkov v takýchto situáciách. Súčasťou robustných protokolov môže byť aj postup na identifikáciu nečestných účastníkov a ich následné vyradenie z procesu. Treba si však dávať pozor, aby takéto postupy nemohli byť zneužité na vyradenie čestných účastníkov, najmä hlasujúcich.

1.3 Účastníci hlasovania

Okrem hlasujúcich existuje ešte niekoľko typov účastníkov hlasovania, s ktorými sa budeme pomerne často stretávať. V krátkosti ich čitateľovi priblížime.

1.3.1 Autority

Autority sú aktívni účastníci hlasovania, ktorí sa spolu s hlasujúcimi podielajú na konštrukcii hlasovacieho výsledku. Môžu rozdávať bezpečnostné prvky, zbierať hlasy, modifikovať ich alebo sčítavať. Množina autorít môže, ale nemusí byť disjunktná s množinou hlasujúcich, v závislosti od protokolu. Príkladom autorít pri papierových voľbách bývajú volebné komisie.

Aby sa zabránilo nečestnému chovaniu autorít, často krát vykonáva tú istú činnosť niekoľko nezávislých autorít, každá s čiastkovou infromáciou a celkový výsledok potom vznikne kombináciou ich čiastočných výsledkov. Častokrát je potom čestné správanie sa aspoň jednej autority podmienkou pre niektorú z vlastností hlasovacieho protokolu.

1.3.2 Nástenka

Nástenka (angl. bulletin board) je pasívny účastník hlasovania, ktorého úlohou je uchovávať a ďalej poskytovať verejné informácie. Verejný charakter nástenky umožňuje prístup k informáciám aj pre entity, ktoré nie sú účastníkmi hlasovania. Je preto vhodná na zverejňovanie informácií využívaných pri overiteľnosti.

Nečestné chovanie nástenky sa môže prejaviť odmietnutím zverejnenia informácie, zverejnením upravenej informácie alebo zverejnením vymyslenej informácie v mene niektorého z účastníkov. Bojovať proti tomu je možné systémom podpisov. Pred zverejnením účastník informáciu podpíše, aby nemohla byť v jeho mene zverejnená vymyslená informácia. Nástenka informácii priradí identifikátor, a podpíše kópiu presného znenia informácie, ktorá sa odovzdá ako doklad späť účastníkovi.

2 Súvisiaci výskum

V nasledujúcom texte si predstavíme výskum súvisiaci s touto prácou. Najskôr sa pozrieme na základné protokolmi využívané kryptografické konštrukcie a následne aj samotné protokoly.

2.1 Kryptografické konštrukcie

2.1.1 Podpisová schéma

Podpisová schéma umožňuje entite zaviazať sa k obsahu správy. Prerekvizitou na vytvorenie podpisu je vygenerovanie súkromného a overovacieho kľúča. Pomocou súkromného kľúča je možné transformovať správu na podpis (podpísať ju). Následne je možné použiť overovací algoritmus na potvrdenie faktu, že podpis zodpovedá danému overovaciemu kľúču a pôvodnej správe. Vyžaduje sa, aby overovacím algoritmom achválené podpisy bolo možné vytvoriť iba so znalosťou súkromného kľúča (alebo náhodne s malou pravdepodobnosťou).

Aby sme podpisu verili, potrebujeme veriť aj tomu, že použitý overovací kľúč naozaj patrí autorovi podpisu. Tento fakt (kľúč patriaci identite) je možné taktiež podpísať. Týmto mechanizmom vieme vytvoriť strom podpísaných kľúčov s ich vlastníkmi, ktorý má v koreni všeobecne uznávanú autoritu. Takýto strom sa nazýva aj infraštruktúra verejných kľúčov.

Medzi najznámejšie podpisové schémy patrí RSA [16] založená na náročnosti prvočíselného rozkladu veľkých zložených čísel. RSA možno modifikovať aj na slepú podpisovú schému, pri ktorej entita môže podpísať správu bez toho aby zistila jej obsah. Táto konštrukcia je použitá napríklad v protokole FOO [13]. Vo väčšine prípadov sú však postačujúce bežné podpisové schémy, ktoré sú všeobecne používané, implementovné a otestované. Patrí medzi ne aj DSA (Digital Signature Algorithm) založená na ElGamalovej schéme [11], ktorú štandardizoval NIST (Národný inštitút pre štandardy a technológie v Spojených štátoch amerických).

2.1.2 Asymetrické šifrovanie

Asymetrické šifrovanie je proces v istom zmysle opačný k elektronickému podpisu. Prijímateľ si vygeneruje dvojicu pozostávajúcu zo súkromného a verejného kľúča, súkromný kľúč uchová v tajnosti a verejný kľúč zverejní. Následne môže akýkoľvek odosielateľ s použitím verejného kľúča transformovať (zašifrovať) ľubovoľnú správu na zašifrovaný text. Spätná transformácia (dešifrovanie) zašifrovaného textu na správu je následne možná iba s použitím súkromného kľúča a teda je bezpečné zašifrovaný text odoslať verejným kanálom.

V hlasovacích protokoloch (napr. [9] alebo [2]) sa najčastejšie používa konštrukcia, ktorú navrhol ElGamal [11]. Je založená na náročnosti výpočtu diskrétneho logaritmu [10]. Medzi najdôležitejšie vlastnosti tohto šifrovania patrí prirodzená náhodnosť. Pri náhodnosti môže byť tá istá správa zašifrovaná na veľké množstvo zašifrovaných textov. Nemožno teda uhádnuť pôvodnú správu a následne si zašifrovaním overiť, či je správna. Medzi ďalšie výhody ElGamal šifrovania patrí homomorfickosť a možnosť zdielaného kľúča, ktoré umožňujú sčítanie hlasov a rozdelenie informácie medzi autority.

2.1.3 Bezznalostné dôkazy

Bezznalostné dôkazy sú protokoly, pomocou ktorých dokáže jeden účastník presvedčiť druhého, že pozná určitú informáciu, bez toho, aby túto informáciu prezradil. Požadovaná informácia môže byť skonštruovaná tak, aby ju účastník vedel iba v prípade, že v určitú operáciu vykonal čestne. Vďaka tomu je možné bezznalostné dôkazy redukovať na dôkazy správnosti postupu, čo je využiteľné pri overiteľnosti.

Využijeme napríklad Schnorrov protokol [18], ktorý umožňuje dokázať znalosť súkromného kľúča zodpovedajúceho konrétnemu verejnému kľúču v ElGamal šifrovaní. Zaujímavá je aj práca *How to prove yourself (Fiat, Shamir)* [12], ktorá popisuje transformáciu niektorých interaktívnych dôkazov na neinteraktívne. Pri neinteraktívnom dôkaze účatsník vypočíta a zverejení takú množinu hodnôt, ktorú by v prípade nečestného chovania nebol schopný skonštruovať. Ktokoľvek si teda môže overiť správnosť dôkazu.

2.1.4 Hešovanie

Hešovanie je deterministická transformácia textu na zdanlivo náhodnú hodnotu. V tejto práci budeme využívať výhradne kryptograficky bezpečné hešovanie, ktoré navyše zaručuje neexistenciu efektívneho algoritmu na hľadanie obrazu pre daný heš, neexistenciu efektívneho algoritmu na nájdenie dvoch textov s rovankým hešom a korelačnú nezávislost korelácie pôvodných textov od korelácie ich hešov (malá zmena textu bežne

spôsobí veľkú zmenu hešu).

Podobne ako pri podpisových shémach ani pri hešovaní sa nebudeme zaoberať implementačnými detailami, ale použijeme existujúce, všeobecne používané a overené riešenia. Ako príklad uvedieme rodinu šifrovacích funkcií Keccak [5], ktorú NIST štandardizoval ako SHA-3, tretiu generáciu všeobecne použiteľných hešovacích funkcií.

2.2 Hlasovacie protokoly

Prvé významné ucelené návrhy elektronických hlasovacích protokolov sa objavili v knihe Cohena a Fishera [7] a neskôr v práci Benaloha a Cohena [3]. Prvý z uvedených protokolov bol síce overiteľný ale nebol dôverný voči autorite, ktorá sčítavala hlasy. Druhý z protokolov bol overiteľný aj dôverný, bol však príliš komplikovaný, či už na pochopenie alebo na implementáciu. Už v týtcho prácach sa objavili myšlienky nástenky a viacerých nezávislých autorít.

V roku 1992 Fujioka, Okamoto a Ohta navrhli protokol [13] (ďalej len FOO protokol), ktorý bol individuálne aj všeobecne overiteľný, spĺňal overiteľnosť oprávnenia za podmienky čestnej autorizačnej autority a bol dôverný pri možnosti anonymného odosielania správ. V protokole hlasujúci najskôr na nástenke anonymne zverejnia autorizačnou autoritou slepo podpísané záväzky k ich hlasom. Autorizačná autorita im slepo podpíše najviac jeden hlas, a zverejnením jeho záväzku ho ďalej nemôžu meniť. Následne sa hlasovanie uzavrie a hlasujúci anonymne zverejnia informácie potrebné na odomknutie ich hlasov. Sčítavanie môže prebiehať verejne.

Výsledkov porovnateľných s FOO protokolom sa v nasledujúcich rokoch objavilo viacero. Pre nás však bude zaujímavá najmä práca Cramera, Gennara a Schoenmakersa v roku 1997 [9] (ďalej ako CGS protokol). Ich protokol zaručuje overiteľnosť a, v prípade aspoň jednej čestnej autority, aj dôvernosť, pri zachovaní pomerne nízkej výpočtovej náročnosti. Najdôležitejšími použitými konštrukciami je homomorfické asymetrické šifrovanie a bezznalostné dôkazy. Na tomto výsledku je založená aj podstatná časť tejto práce.

CGS protokol bol pomerne jednoducho implementovateľný, vyžadoval však malú a dopredu známu množinu kandidátov. FOO protokol, naopak, podporoval ľubovoľný obsah a rozsah hlasu (pokiaľ nebol dôverný) avšak implementácia anonymného zverejňovania bola pomerne náročná. Priblíženie k anonymnému zverejňovaniu umožňuje technológia miešacích sietí (angl. mixing networks). Použili ju aj Sako a Kilian v ich protokole [17], ktorý bol nielen overiteľný a dôverný, ale aj nedokladovateľný. Vyžadoval však existenciu fyzického dokonale anonymného kanálu od autority k hlasujúcemu.

V roku 2006 popísal Benaloh v článku Simple Verifiable Elections [2] protokol inšpirovaný okrem iných aj CGS protokolom a prácou Saka a Kiliana, ktorého primárnym

cieľom bola ľahká implementovateľnosť. Práce sa chytil Adida a o dva roky neskôr implementoval hlasovací systém Helios [1], ktorý bolo možné na využívať na online elektronické hlasovanie do doby písania tejto práce. Helios je overiteľný, dôverný a umožňuje vpisovanie nových kandidátov priamo do hlasu. Veľkou výhodou je aj intuitívne používateľské rozhranie, ktoré umožňuje systém využívať laickým používateľom.

Zaujímavá práca tiež prebiehala v oblasti nedokladovateľnosti. Často využívanými konštrukciami sú miešacie siete a prešifrovávanie (angl. reencryption). Podmienky zvyčajne zahrňujú bezpečné generátori náhodných čísel, neodpočúvateľné alebo anonymné komunikačné kanály či možnosť zverejniť niekoľko hlasov, pričom platný je posledný. Ako príklad môžeme uviesť prácu Juelsa, Catalana a Jacobssona [14].

3 Hlasovnia malého rozsahu

Napriek tomu, že elektronickým hlasovacím protokolom sa v dnešnej dobe venuje množstvo prác, existujú slabo pokryté oblasti. Jednou z nich sú hlasovania malého rozsahu konajúce sa v krátkom čase a v reálnom prostredí (napríklad v jednej miestnosti). Na základe rozboru existujúcich inštancií takýchto hlasovaní navrhneme modelovú situáciu, pre ktorú neskôr vytvoríme hlasovací protokol. Pre úplnosť dodáme, že malé hlasovania v online priestore výborne pokrýva napríklad systém Helios [1].

3.1 Súčasná prax

V tejto časti popíšeme hlasovacie praktiky a využitia hlasovania v súčastnosti na Slovensku. Cieľom nie je uviesť úplný zoznam, ale získať dostatok podkladu na návrh dostatočne všeobecnej modelovej situácie.

3.1.1 Fyzické hlasovacie protokoly

Jednou z možností verejného (nedôverného) hlasovania je hlasovanie zdvíhaním rúk. Moderátor hlasovania postupne prechádza zoznam kandidátov a pri každom z nich vyzve hlasujúcich, ktorý sa pre tohto kandidáta rozhodli, aby zdvihli ruky. Nevýhodou tohto prístupu je, že hlasujúci môžu byť ovplyvnení hlasovaním iných a na základe týchto infomácií upraviť svoj hlas. Túto výhodu navyše získavajú iba tí hlasujúci, ktorí sa rozhodli pre neskorších kandidátov.

Alernatívne verejné hlasovanie je hlasovanie súčasným odhalením hlasu. Každý hlasujúci vyjadrí svoj názor napísaním na kúsok papiera prípadne ho vyznačí na predpripravenom hlase. Hlas potom uchová v tajnosti až do momentu kedy sú všetky hlasy pripravené a súčasne sa odhalia. Nasleduje verejné spočítanie hlasov (pokojne aj zdvíhaním rúk, ktoré je však teraz už kontrolované).

Pri dôvernom hlasovaní je najčastejším protokolom hlasovanie s urnou. Hlasujúci v súkromí vyznačia svojho kandidáta na špeciálne upravenom kúsku papiera – hlase. Obsah hlasu sa skryje preložením alebo vložením do obálky a vhodí sa do verejne viditeľnej nádoby – urny. Po skončení hlasovania sa obsah urny vyloží, odtajní a verejne spočíta. Na zachovanie overiteľnosti je dôležité urnu neustále sledovať.

3.1.2 Príklady hlasovaní

Rôzne zhromaždenia (schôdza obyvateľov bytového domu, akademický senát, poslanci mestkého zastupiteľstva) majú kompetenciu na prijímanie určitých rozhodnutí. Zvyčajne však býva potrebné, aby s rozhodnutím súhlasila väčšina zúčastnených. Túto skutočnosť je možné overiť prostredníctvom hlasovania. Kandidátmi sú súhlas s návrhom, nesúhlas s návrhom a prípadne zdržanie sa hlasovania. Počet hlasujúcich v spomínaných príkladoch zhromaždení zvyčajne neprekračuje sto. Na jednom zhromaždení sa môže vyskytnúť niekoľko hlasovaní a potreba hlasovania môže vzniknúť spontánne.

Menej častým programom zhromaždení je voľba predsedu alebo inej špeciálnej funkcie. Zoznam kandidátov je pre každé hlasovanie špecifický, vo väčšine prípadov je však jednociferný. Hlasovanie spolu so zoznamom kandidátov zvykne byť oznámené niekoľko dní dopredu. Horný odhad na počet hlasujúcich ponecháme na čísle sto.

Hodnotiace komisie (pri obhajobe záverečných prác, pri polročnom uzatváraní hodnotenia v škole, porota na súťaži) vyjadrujú svoj názor stupňom hodnotenia. Výsledné hodnotenie je potom možné odvodiť z počtu výskytov jednotlivých hodnotení. Kandidátmi sú teda jednotlivé stupne hodnotenia. Prepokladajme, že počet stupňov hodnotenia ani počet členov komisie nebude väčší ako desať. Zaujímavá vlastnosť je, že množina kandidátov sa medzi jednotlivými hlasovaniami nemení. Môžeme očakávať väčšie množstvo hlasovaní v priebehu krátkeho obdobia.

Keďže funkcia počítajúca výsledné hodnotenie býva často jednoduchá a dobre matematicky popísateľná, bolo by zaujímavé ako výsledok hlasovania použiť priamo hodnotenie a protokol navrhnúť tak, aby skrýval aj distribúciu stupňov hodnotenia. V modelovej situácii, však takúto možnosť uvažovať nebudeme.

Všetky spomenuté hlasovania zvyčajne využívajú fyzické hlasovacie protokoly popísané vyššie. Nevyhnutnou súčasťou týchto protokolov je priame verejné sčítanie hlasov a teda je výsledok dostupný krátko po hlasovaní, pri väčšom počte hlasujúcich do niekoľkých minút. Okamžitý výsledok je preto očakávaný a musíme ho zahrnúť aj do nášho modelu.

3.2 Aplikovateľnosť elektronického hlasovania

Na to, aby elektronické hlasovanie nahradilo zaužívané postupy, je potrebné, aby jeho fyzická implementácia bola finančne aj používateľsky nenáročná a aby oproti pôvodným riešeniam prinieslo určité výhody. Pozrieme sa teda na technickú pripravenosť prostredia ako aj na smery, v ktorých môžeme dosiahnuť pokrok.

3.2.1 Výpočtové zdroje

Na realizáciu elektronického hlasovacieho protokolu sú potrebné výpočtové zariadenia a ich vzájomné prepojenie. Obstarávanie nových zariadení špeciálne pre účely hlasovania je vo väčšine spomenutých prípadov vylúčené. Je preto potrebné využiť zariadenia, ktoré hlasujúci alebo organizátori hlasovania už vlastnia. Organizátor by mal byť schopný pre potreby hlasovania zabezpečiť jeden prenosný osobný počítač, ktorý je vybavený bežným softvérom a hardvérom. Tento počítač môže byť mimo hlasovania bežne využívaný a preto naň nemôžu byť kladené žiadne neštandardné bezpečtnostné nároky.

V dnešnej dobe je v poriadku predpokladať, že väčšina hlasujúcich vlastní mobilné zariadenie s možnosťou prístupu na internet. Nájsť hlasovaciu miestnosť s prístupom na internet tiež nemôže byť problém. Je však nepravdepodobné, že by vlastníci poskytli svoje zariadenia na všeobecné používanie. V prípade využitia teda musia byť mobilné zariadenia obsluhované výlučne svojimi majiteľmi.

3.2.2 Externá účasť

Rôzne rady a zhromaždenia čoraz častejšie využívajú technológiu videohovorov na zapojenie členov, ktorí sa stretnutia osobne nemohli zúčastniť. Budeme preto predpokladať, že nie všetci hlasujúci sú fyzicky prítomný na mieste konania volieb. Takýto hlasujúci však vlastnia zariadenie s prístupom na internet a majú otvorený audiovizuálny komunikačný kanál so zvyšnými účastníkmi hlasovania. V ďalšom texte ich budeme nazývať distanční hlasujúci.

Práve externé hlasovanie pri zachovaní dôvernosti je problém, ktorý sa pri fyzických protokoloch zabezpečuje pomerne náročne. V prípade potreby teda môže byť hlavným dôvodom na prechod na elektronické alternatívy.

3.2.3 Vlastnosti volebného protokolu

Vďaka osobnej účasti všetkých hlasujúcich sú výsledky fyzických hlasovacích protokolov považované za overiteľné. Akékoľvek nahradenie neoveriteľným protokolom by preto bolo neakceptovateľné. Navyše, formálna overiteľnosť môže výsledku hlasovania dodať právnu vážnosť. Overiteľnosť teda určite budeme vyžadovať.

Dôvernosť nemusí byť potrebná a občas je aj nežiaduca. Návrh nedôverného protokolu je však pomerne jednoduchý a v prípade existujúceho audiovizuálneho kanálu medzi hlasujúcimi je možné použiť hlasovanie zdvíhaním rúk alebo hlasovanie súčasným odhalením hlasu. Budeme preto vyžadovať aj dôvernosť s prípadnou možnosťou jej deaktivácie.

Napriek tomu, že nedokladovateľnosť by bola pre hlasovanie prínosom, jej existujúce návrhy majú netriviálne hardvérové požiadavky (napr. neodpočúvateľný kanál [14] alebo neovplyvniteľné náhodné orákulum [15]). Riziko ovplyvnenia pri malom počte hlasujúcich je navyše pomerne malé. Od požiadavky na nedokladovateľnosť teda upustíme.

3.2.4 Používateľské hľadisko

Klasické protokoly sú pre hlasujúcich intuitívne. Účastník ľahko pochopí, ako má v jednotlivých situáciach konať a na čo treba dohliadnuť, aby bola zachovná overiteľnosť a dôvernosť. Pochopenie kľúčových konceptov elektronického hlasovania si však vyžaduje netriviálne matematické znalosti, ktoré od bežného hlasujúceho nemožno očakávať. Je teda nevyhnutné vytvoriť používateľské rozhranie, ktoré účastníka nielen prevedie celým procesom, ale navyše ho aj upozorní na možné riziká.

3.3 Modelová situácia

Poznatky nadobudnuté v predchádzajúcich častiach teraz preformulujeme do ucelenej modelovej situácie.

Modelová hlasovacia situácia je sústredená v jednej miestnosti vybavenej prístupom na internet. Hlasujúci sa môžu zúčastniť prezenčne alebo distančne. Distanční hlasujúci majú otvorený audiovizuálny komunikačný kanál so zvyšnými účastníkmi procesu. Prebiehajúcemu hlasovaciemu procesu sa všetci účastníci plne venujú (alebo to aspoň predstierajú) s cieľom dopracovať sa k výsledku hlasovania čo najrýchlejšie. Množina oprávnených hlasujúcich je známa pred začiatkom hlasovacieho procesu a jej veľkosť nepresiahne sto. Množina kandidátov je taktiež známa pred začiatkom hlasovacieho procesu a jej veľkosť nepresiahne desať. Všetci distanční a väčšina prezenčných hlasujúcich disponuje vlastným zariadením s prístupom na internet. K dispozícii je navyše jeden prenosný osobný počítač s bežnou výbavou. Od hlasovacieho protokolu sa vyžaduje overiteľnosť, deaktivovateľná dôvernosť a intuitívne používanie.

4 Návrh hlasovacieho protokolu

Na základe sformulovanej modelovej situácie navrhnem protokol pre elektronické hlasovanie. Budeme sa sústrediť hlavne na slovný popis protokolu, s dôrazom na odôvodnenie rozhodnutí a na pochopenie čitateľom. Formálnemu popisu, matematickým detailom a dôkazom sa povenujeme v kapitole 5. Najmä v prípade bezznalostných dôkazov iba spomenieme ich existenciu.

Predpokladáme, že čitateľ je zoznámený so základnými pojmami z teórie grúp a lineárnej algebry, základnými pojmami z kapitoly 1, so základnými kryptografickými pojmami z časti 2.1 a s modelovou situáciou popísanou v časti 3.3. Podrobnejší popis kryptografických sa nachádza napríklad v texte *Cryptographic Voting—A Gentle Introduction* [4].

V časti 4.4.3 predstavujeme teoreticky zaujímavý vlastný výsledok, v časti 4.3 popisujeme mierne upravený existujúci protokol. Zvyšné časti sú výsledkom autorovej kreatívnej práce, ktorá ale neprináša žiadny pokrok oproti existujúcim riešeniam.

4.1 Využitie osobných zariadení

Najzreteľnejším problémom modelovej situácie je absencia vlastných zariadení u niektorých prezenčných účastníkov. Kvôli nim bude potrebné vymyslieť alternatívny spôsob hlasovania. Na druhej strane, pri distančných účastníkoch je ich zariadenie jediným potenciálne dôverným spôsobom ako hlasovať. Zostáva teda rozhodnúť, či a ako využiť zariadenia prezenčných účastníkov.

Priamočiari spôsob ako problém vyriešiť by bolo zrealizovať dve paralelné hlasovania. Elektronické pre účastníkov s vlastnými zariadeniami a hlasovanie s urnou pre zvyšných. Táto metóda však čiastočne porušuje dôvernosť hlasovania, najmä v prípade, že jedna z množín hlasujúcich bude výrazne menšia. Avšak aj v prípade, keď zodpovedne rozdelíme hlasujúcich rovnomerne medzi oba spôsoby hlasovania, vznikne dodatočná povinnosť registrovať, ktorí z nich sa ktorého hlasovania zúčastnili, a tak zabrániť súčasnej účasti jednotlivca v oboch procesoch. Paralelným priebehom by mohol ľahko vzniknúť zneužiteľný chaos, postupný priebeh by mal zvýšené časové nároky. Nevylučujeme výhodnosť tohto spôsobu v špecifických prípadoch, ako všeobecné riešenie

ho však nepoužijeme.

Výhodou využitia osobného zariadenia je dôvera majiteľa k nemu. Pokiaľ sa nám zároveň podarí vzbudiť dôveru v použitý softvér, bude zariadenie konať absolútne v prospech majiteľa a majiteľ si toho bude vedomí. Autenticitu softvéru možno zabezpečiť napríklad využitím digitálnych podpisových schém alebo, v prípade webovej aplikácie, jej stiahnutím cez SSL pripojenie. Nebezpečenstvom môže byť prítomnosť škodlivého softvéru na zariadení. Budeme však predpokladať, že pri hlasovaniach malého rozsahu je takýto typ útoku príliš nákladný.

Konanie zariadenia v prospech majiteľa však môže byť v prípade nečestného účastníka zneužité. Nevieme zabrániť upraveniu hlasovacieho softvéru a následnému šíreniu a používaniu nečestnej verzie. Osobné zariadenie teda môžeme použiť iba na automatizáciu procesu vykonávaného konkrétnym účastníkom.

V prípade, že nejaký hlasujúci plne dôveruje inému účastníkovi, môže v prípade potreby zdielať jeho zariadenie a spustiť na ňom paralelný hlasovací proces. Existenciu takejto dôvery však nebudeme predpokladať.

Podobne, ako nemožno dôverovať cudzím osobným zariadeniam, nemožno dôverovať ani prenosnému počítaču, ktorý je v modelovej situácii tiež dostupný. Okrem upraveného hlasovacieho programu môže obsahovať aj monitorovací softvér. Nemožno ho teda využívať na žiadne dôverné operácie.

Sme nútený predpokladať, že ovplyvnené môže byť akékoľvek zariadenie použité v procese. Použitie viacerých zariadení a ich vzájomná kontrola však prípadný útok na protokol komplikuje. Bolo by teda škoda nevyužiť všetky dostupné zariadenia. Minimálne ich možno použiť ako kontrolný prostriedok pre majiteľa.

4.2 Účastníci hlasovacieho procesu

Okrem hlasujúcich bude protokol vyžadovať aj ďalších účastníkov. Môžu sa nimi stať prítomné zariadenia, prítomné osoby ale aj externé servre. Postupne ich identifikujeme a navrhneme ich realizáciu. Dopredu upozorňujeme, že spomenuté množiny účastníkov nemusia byť disjunktné, pokiaľ to explicitne neuvedieme.

4.2.1 Autority pracujúce s hlasmi

Začneme hneď najdôležitejšou funkciou. Keďže nedisponujeme zariadením, ktoré má plnú dôveru všetkých hlasujúcich, musíme buď použiť protokol nevyžadujúci čestné autority alebo rozdeliť zodpovednosť a informáciu autority medzi viacero zariadení. Druhá z možností priamo nadväzuje na myšlienku z predchádzajúcej časti – umožniť čo najviac zariadeniam kontrolovať volebný proces.

Predpokladajme teda, že by autoritou bolo každé zariadenie zapojené do hlasovania. Pri protokoloch založených na homomorfnom asymetrickom šifrovaní často krát stačí aby bola čestná aspoň jedna čestná autorita ([9], [4]). Dosiahli by sme teda stav, v ktorom by existencia jedného čestného účastníka s vlastným zariadením stačila zachovanie dôvernosti a overiteľnosti. Z pohľadu samotného hlasujúceho so zariadením je táto podmienka vždy splnená.

Nevýhodou by bola možnosť každého z týchto účastníkov proces sabotovať neaktivitou. Ak však budeme vedieť sabotéra identifikovať, môžeme takéto správanie vylúčiť mimoprotokolovými prostriedkami (napr. hrozbou sankcií). Treba tiež zvážiť či mobilné zariadenia zvládnu výpočtovú náročnosť úkonov vykonávaných autoritou či vplyv množstva autorít na sieťovú komunikáciu a dĺžku výpočtov.

Druhá z úvodných možností, nevyžadovať čestnú autoritu, je redukovateľná na súčastné riešenie. Nevyžadujeme čestnú autoritu, pretože každý je zároveň aj autoritou.

K zoznamu autorít však môžeme pristúpiť absolútne liberálne. Pokiaľ výpočtová sila niektorého zo zariadení neumožní jeho využitie v úlohe autority a zároveň majiteľ plne dôveruje inému účastníkovi s výkonnejším zariadením, môžeme za dôkladného upozornenia povoliť hlasujúceho, ktorý nie je zároveň autoritou. Naopak, ak je k dispozícii výkonný počítač a niektorý z účastníkov zaň prevezme zodpovednosť, môže byť tento počítač zaradený k autoritám. Za štandardných okolností však autoritami budú práve hlasujúci so zariadením.

4.2.2 Nástenka

Implementácia nástenky je pomerne jednoznačne určená okolnosťami. Keďže podporujeme distančných hlasujúcich musí byť verejne prístupná na internete. Spustiť verejne dostupný server na lokálnom zariadení je technicky náročné a u mnohých poskytovateľov internetového pripojenia aj nemožné zakázané. Nástenka preto musí byť poskytovaná externým serverom. Vzhľadom na jej neutrálnu úlohu to však nebude problém. Zároveň je možné jedným nástenkovým serverom obsluhovať väčšie množstvo hlasovacích skupín.

Čestné správanie nástenky možno zabezpečiť už spomínaným podpisovým protokolom. Po prijatí správy ju nástenka podpíše a podpis odošle späť ako dôkaz zverejnenia. Informáciu môže odsielateľ považovať za verejnú po overení podpisu. Správa je zároveň podpísaná aj jej autorom a teda nástenka nemôže svojvoľne zverejňovať falošné správy. V prípade, že nástenka odmietne zobraziť zverejnenú správu, je možné obrátiť sa na jej prevádzkovateľa so sťažnosťou a zároveň aj s dôkazom, že informácia bola zverejnená. V prípade, že nástenka odmietne prijať správu, môže sa autor pokúsiť o odoslanie prostredníctvom iného účastníka a v prípade opakovaného odmietnutia tak vznikne skupina svedkov takéhoto nečestného chovania. Prevádzkovateľ nástenky tak síce vie

sabotovať proces hlasovania, ale vždy bude identifikovaný a čin mu bude dokázaný.

4.2.3 Autorizačná autorita

Rozšírenou praktikou hlasovacích protokolov je vytvorenie nezávislých inštancií šifrovacích a podpisových kľúčov pri každom hlasovaní. Je ale potrebné dôveryhodne odkomunikovať nové verejné a overovacie kľúče prislúchajúce konkrétnej identite. Toto je možné dosiahnuť podpísaním týchto informácií kľúčom, ktorého autorita je overiteľná mimo hlasovacieho protokolu.

Jednou možnosťou je využiť už existujúcu infraštruktúru verejných podpisových kľúčov a požiadať účastníkov o zapojenie sa do tejto infraštruktúry. Pri začiatku hlasovania potom použijú ich všeobecný kľúč na podpis dočasných kľúčov. Alternatívne môžeme použiť ďalší externý server – autorizačnú autoritu. Účastník sa autorizuje voči tomuto serveru, odošle mu potrebné údaje a server ich podpíše jeho všeobecne akceptovaným kľúčom.

Protokol by mal fungovať s ľubovoľným riešením, ktoré vyprodukuje podpis dočasných kľúčov spolu s identitou. Dôveryhodnosť takéhoto podpisu potom bude podmienkou pre overiteľnosť platnosti hlasovacieho protokolu. Odporúčané riešenie je použiť infraštuktúru podpisových kľúčov. Akceptovateľné riešenie je použiť spôsob autorizácie, ktorý účastníci používajú pri iných dôverných operáciách.

4.2.4 Zakladateľ

Aj sú keď parametre hlasovania známe už pred hlasovaním, je potrebné ich do procesu nejakým spôsobom začleniť. Okrem toho je potrebné identifikovať autority a autorizovať hlasujúcich. Všetky tieto aktivity sa budú diať v úvodnej fáze protokolu počas ktorej bude dôležitý špeciálny účastník, zakladateľ.

Zakladateľ vyhlási začiatok hlasovacieho protokolu zverejnením všetkých dopredu známych informácií. Autority a hlasujúci zverejnenia svoje dočasné kľúče autorizované dohodnutým spôsobom a podpisom sa prihlásia k zverejneným informáciám podpisom. Pomocou audiovizuálneho kanálu sa zakladateľ presvedčí, že všetci účastníci sa úspešne prihlásili a následne zverejní a podpíše oficiálny zoznam účastníkov hlasovania. Toto je zároveň posledná akcia zakladateľa. Od tohto momentu môže akákoľvek autorita hlasovanie zrušiť zverejnením tejto informácie na nástenke. Ak tak učiní musí odôvodniť, prečo tak konala. Jedným z dôvodov môže byť nesúhlas so zoznamom účastníkov. Ak autorita so zoznam účastníkov súhlasí, je povinná túto skutočnosť potvrdiť jej podpisom. Podpisom zoznamu poslednou autoritou sa končí úvodná fáza. Hlasovať teda môže ľubovoľná skupina hlasujúcich so zariadením, ktorá sa zhodne na zozname účastníkov. Popísaný model zatiaľ neuvažuje hlasujúcich bez zariadenia.

V prípade, že niektorá autorita hlasovanie zruší, nasleduje verejná konfrontácia zakladateľa s protestujúcou autoritou, vyriešenie sporu a pokus o založenie nového hlasovania. Úmyselné sabotovanie hlasovania by teda malo byť pomerne ľahko odhaliteľné a riešiteľné vylúčením autority a zároveň aj prislúchajúceho hlasujúceho.

4.3 Jadro protokolu

V tejto časti sa popíšeme jadro hlasovacieho protokolu za predpokladu, že všetci hlasujúci majú vlastné zariadenia. Hlasujúcim bez zariadenia sa samostatne povenujeme v časti 4.4.3. Celý protokol vznikol upravením práce *A secure and optimally efficient multi-authority election scheme* [9] na podmienky uvedené v modelovej situácii. Niektoré detaily boli inšpirované dielami [1], [2] a [4].

4.3.1 Komunikácia

Komunikácia medzi zariadeniami prebieha výlučne na základe zverejňovania správ na nástenke. Každá správa obsahuje jednoznačný identifikátor autora, neprázdny zoznam identifikátorov starších správ, z ktorých informácie boli využité pri konštrukcii tejto správy a kryptograficky bezpečný heš správ z tohto zoznamu. Následne správu podpíše, odošle nástenke, tá jej priradí identifikátor a tiež ju podpíše.

Podpisom sa autor zaväzuje k obsahu správy ale len za podmienky, že je reakciou na pôvodné správy v tom znení, v ktorom ich zahešoval. Čitateľ správy je povinný heš aj podpis overiť. V prípade nesprávneho hešu je povinný hlasovanie zrušiť. Následne obe strany doložia nástenkou podpísané správy, ktoré použili na výpočet hešu. Všetci teraz môžu nahliadnuť, či pochybila niektorá zo strán konfliktu alebo nástenka poskytovala dve verzie správy s tým istým identifikátorom. V prípade zlého podpisu sa správa ignoruje, pretože nemožno doložiť jej autora. Na doloženie správ sa použije iný komunikačný kanál ako nástenka. Ak niektorá zo strán odmietne komunikovať, považuje sa za vinnú.

4.3.2 Dodatočné vlastnosti asymetrického šifrovania

V protokole použijeme ElGamalovo asymetrické šifrovanie [11] využívajúc niekoľko jeho dodatočných vlastností, ktoré si najskôr stručne popíšeme. Podrobnejší popis možno nájsť v časti 5.1.1. Šifrovanie operuje nad cyklickou podgrupou G grupy H. Generátor G označme g. Samotné správy vieme vyberať buď priamo ako prvky H alebo ich vieme kódovať ako exponent m v prvku $g^m \in H$. Grupovú operáciu grupy H nazveme pre jednoduchosť násobením.

Prvou vlastnosťou je homomorfickosť, čo znamená že vynásobením dvoch zašifrovaných správ dostaneme zašifrovaný text súčinu pôvodných správ. V prípade, že použijeme kódovanie exponentom, vynásobením dvoch zašifrovaných správ sčítame pôvodné správy. Práve túto vlastnosť využijeme pri hlasovaní a teda v ďalšom texte predpokladáme kódovanie správy exponentom

Vieme tiež skombinovať niekoľko verejných kľúčov do jedného spoločného. Na odšifrovanie správ zašifrovaných spoločným kľúčom potom treba spoluprácu vlastníkov všetkých pôvodných kľúčov. Každý odšifruje svoju časť a výsledky sa skombinujú do pôvodnej správy.

Okrem toho existuje množstvo protokolov pre bezznalostné dôkazy. Vieme dokázať, že sme zašifrovali konkrétnu hodnotu alebo niektorú z malej množiny hodnôt. Tiež vieme dokázať správne odšifrovanie či znalosť súkromného kľúča prislúchajúceho verejnému.

4.3.3 Protokol

1. Každá autorita si v úvodnej fáze vygenerovala dvojicu kľúčov. Verejný z nich spolu s dôkazom znalosti súkromného zverejní na nástenke.

2. Zakladateľ vymenoval presný zoznam autorít a teda si každý môže vypočítať spoločný verejný kľúč všetkých autorít.

3. Každý hlasujúci vytvorí svoj hlas. Pre každého kandidáta zašifruje binárnu hodnotu vyjadrujúcu, či si ho vybral, spoločným kľúčom. Aby dokázal koretnosť hlasu priloží bezznalostný dôkaz, že každá z pôvodných hodnôt je nula alebo jedna. Navyše dokáže, že súčin zašifrovaných hodnôt je zašifrovanou jednotkou, čiže súčet pôvodných hodnôt je jedna a teda hlasujúci vybral práve jedného kandidáta.

4. Každý si teraz môže vypočítať homomorfický súčet zašifrovaných textov pre každého kandidáta.

5. Jednotlivé autority čiastočne odšifrujú súčty pre jednotlivých kandidátov a priložia dôkáz správnosti odšifrovania.

6. Každý si teraz môže z čiastočných výsledkov pre jednotlivých kandidátov vypočítať výsledok hlasovania.

7. Moderátor oznámi výsledok hlasovania. Prepis komunikácie dokazuje, že jednotlivé autority s výsledkom súhlasia.

V úvodnej fáze autority doložili znalosť súkromného kľúča a teda aj fakt, že verejný kľúč nebol zvolený účelovo. Spoločný kľúč teda možno považovať za bezpečný, pokiaľ

nespolupracujú všetky autority. Kľúč použijú hlasujúci na zašifrovanie hlasu a doložia, že ich hlas je korektný. Všetky nasledujúce operácie s hlasmi sú úplne transparentné. Súčty môže prepočítať a overiť ktokoľvek, správnosť odšifrovania autority doložia a finálnu kombináciu čiastočne odšifrovaných súčtov môže vykonať taktiež ktokoľvek. Odšifrované sú až súčty hlasov, teda pôvodné hlasy zostávajú v tajnosti. Hlasovanie je teda dôverné pokiaľ nespolupracujú všetky autority, individuálne overiteľné a všeobecne overiteľné.

Nahliadnime ešte na robustnosť. Ak akýkoľvek účastník hlasovania uvedie nesprávny dôkaz, je objaviteľ tohto faktu povinný hlasovanie zrušiť. V prípade dlhej neaktivity je možné účastníka konfrontovať a ak niektorá z autorít považuje čakaciu dobu za neakceptovateľnú, môže hlasovanie zrušiť. V prípade zrušenia nastáva konfrontácia a určí sa vinník. Hlasovanie sa zopakuje, potenciálne bez vinníka.

4.4 Hlasovanie bez zariadenia

4.4.1 Prenos informácie

Môžeme predpokladať, že aj keď hlasujúci nepoužíva vlastné zariadenie priamo počas hlasovania, má možnosť prístupu na internet z dôveryhodného počítača v dostupnom čase pred hlasovaním alebo v dostupnom čase po hlasovaní. Takýto prístup potom môže využiť na prípravu ľubovoľných, v hlasovaní využiteľných, informácií. Tiež si vie dodatočne skontrolovať správnosť informácií zverejnených na nástenke.

Pokiaľ si hlasujúci predpripravil nejaké údaje, potrebuje ich, efektívnym spôsobom, použiť počas protokolu. Hodnoty vyskytujúce sa v kryptografických konštrukciách však častokrát bývajú príliš veľké na zapamätanie si alebo na bezchybné prepisovanie. Jeden veľmi efektívny spôsob prenosu takýchto informácií je použitie grafických kódov (napr. čiarové kódy alebo QR kódy). Väčšina mobilných zariadení je v súčastnosti vybavená digitálnou kamerou a existuje množstvo softvéru rozpoznávajúceho tieto kódy. Hlasujúcemu teda stačí vytlačiť si grafické informácie a naskenovať ich počas hlasovania. Za predpokladu, že nástenka je poskytovaná ako neustále dostupná služba, môžeme väčšie množstvá verejných informácií zverejniť na nástenke a pomocou grafického kódu prenášať iba identifikátor zverejnenej správy s podpisom.

4.4.2 Suplovacie zariadenie

Priamočiarym riešením je použiť dostupný prenosný počítač ako náhradu za chýbajúce osobné zariadenie a dodatočnými operáciami ho donútiť k čestnému správaniu sa. Takýto počítač nazveme suplovacie zariadenie. Ak by sme použili iba suplovacie zariadenie bez kontrolných techník, hlasujúci by si nemohol overiť ani fakt, že jeho hlas

obsahoval správneho kandidáta.

Ak si hlasujúci vytvoril dvojicu kľúčov asymetrického šifrovania, môže verejný kľúč poskytnúť suplovaciemu zariadeniu a vyžiadať si zverejnenie zašifrovaného dôkazu faktu, že zariadenie volilo správne. Toto riešenie využíva dokladovateľnosť protokolu, je nedôverné a v prípade, že zariadenie zahlasuje inak, hlasujúci sa o tom síce dozvie, ale nemôže s tým nič spraviť.

Trochu interaktívnejší prístup je nechať hlasujúceho hlasovať dva krát, počkať, kým zariadenie publikuje hlasy, a následne jednu voľbu zverejniť. Zariadenie musí následne dokázať, že zverejnený kandidát súhlasí s kandidátom na zodpovedajúcom hlase. Ak zariadenie zamení kandidáta v niektorom z hlasov, riskuje konflikt. Je však nerozlíšiteľné, či konflikt vznikol pochybením kandidáta alebo zariadenia. Samostatne je teda tento postup nepoužiteľný.

Aby sme zmiernili následky účelovej zámeny kandidáta, môžeme nechať hlasujúceho aby si dopredu zvolil náhodnú permutáciu kandidátov. Pri hlasovaní sa bude riadiť podľa tejto permutácie a po publikovaní hlasu na nástenke ju zverejní. Permutácia sa následne verejne aplikuje na zariadením vytvorený hlas. Suplovacie zariadenie síce stále môže zameniť kandidáta v hlase, ale už iba na náhodnú hodnotu.

Všetky spomenuté riešenia je možné kombinovať a aspoň trochu sa tým priblížiť k overiteľnosti. Suplovacie zariadenie však stále bude mať úplnú informáciu o tom, ako sa hlasujúci rozhodol. Potrebujeme ju rozdeliť medzi viacero zariadení.

4.4.3 Predpripravený hlas

Predpokladajme, že účastník si svoj hlas pripravil už vopred a zverejnil ho na nástenke. V dobe prípravy však ešte nemusel poznať množinu kandidátov. Mohol teda zhora odhadnúť ich počet, zahlasovať za náhodného a potom, počas hlasovania, zverejniť priradenie kanditátov na jeho hlase k tým reálnym. Viacero hlasových kandidátov môže byť priradených k jednému reálnemu - hlas si aj tak obsahuje práve jednu jednotku.

Väčším problémom bude, že v dobe prípravy hlasu nepoznáme ani spoločný kľúč ktorým hlas treba zašifrovať. Zašifrujeme ho teda verejným kľúčom vytvoreným špeciálne pre tento účel. Na použitie v protokole však potrebujeme hlas prešifrovať.

Na vysvetlenie princípu prešifrovania budeme potrebovať niekoľko úvah z lineárnej algebry. Grupu G v ElGamal šifrovaní vieme zvoliť tak, aby mala prvočíslený rád. Násobenie zašifrovaných správ potom bude sčítaním pôvodných správ v modulárnom konečnom poli F. Ak m bude počet kandidátov v predpripravenom hlase, potom si tento hlas vieme predstaviť ako vektor zo štandardnej bázy m-rozmerného priestoru nad F. Nech teda $\overrightarrow{h}$ je predpripravený hlas. Uvažujme maticu A s m riadkami a $n > m$ stĺpcami takú, že ľubovoľných m stĺpcov je lineárne nezávislých (napríklad môžme položiť $a_{ij} = j^{(i-1)}$). Potom rovnica $A \cdot \overrightarrow{x} = \overrightarrow{h}$ má aspoň jedno riešenie. Nech

je to $\overrightarrow{s}$ so súradnicami s_1, s_2, ..., s_n.

Spolu s predpripraveným hlasom a dôkazom, že je korektný, zverejní hlasujúci aj zašifrované súradnice s_1, s_2, ..., s_n a maticu A. Vďaka homomorfickosti šifrovania si každý môže overiť, že $A \cdot \overrightarrow{s} = \overrightarrow{h}$. Pôvodné hodnoty s_i spolu s detailami ich zašifrovania t_i si vytlačí. Počas hlasovacieho procesu hlasujúci zverejní identifikátor predpripraveného hlasu a oznámi priradenie kandidátov, ktoré si zvolil. Tieto informácie sa zverejnia na nástenke. Následne rozdá vytlačené pôvodné hodnoty s_i a t_i autoritám, každú inej. Zvolené autority zašifrujú s_i pomocou verejného kľúča platného pre hlasovanie a za pomoci t_i zostroja dôkaz (konštrukciu popíšeme v časti 5.1.3), že zašifrovaná hodnota je identická s tou, ktorá sa nachádza v predpripravenom hlase. Zašifrovanú hodnotu aj s dôkazom zverejnia. Každý si teraz vie vypočítať zašifrovaný hlas.

Popísaný protokol je zjavne overiteľný - každý jeden krok je buď vykonaný verejne alebo je k nemu doložený dôkaz. Dôverný je za podmienky, že aspoň m z n autorít, ktoré spracovávali hlas je čestných. Túto vlastnosť možno odvodiť z faktu, že aj keď poznáme (zafixujeme) ľubovoľných $n - m$ súradníc vektora $\overrightarrow{x}$, vieme zvyšné súradnice doplniť tak, aby $A \cdot \overrightarrow{x}$ mohlo nadobúdať ľubovoľnú hodnotu a teda mohlo byť ľubovoľným hlasom. Ak by to neplatilo, m stĺpcov A zodpovedajúcich neznámym súradniciam by muselo byť lineárne závislých, čo je v spore s konštrukciou A.

V prípade, že nám popísaná podmienka nestačí, môžeme počet stĺpcov matice A znásobiť číslom q a každej autorite poskytnúť q súradníc $\overrightarrow{s}$. Tím potrebný počet čestných autorít zredukujeme na $\lceil \frac{m}{q} \rceil$.

4.4.4 Registrácia predpripravených hlasov

Zverejňovanie predpripravených hlasov na nástenku vykonáva špeciálny účastník hlasovacieho protokolu – registrátor predpripravených hlasov (ďalej v tejto časti len registrátor). Počas úvodnej fázy sa každý registrátor riadne prihlási a zakladateľ jeho prítomnosť potvrdí v zozname účastníkov. Súhlasom s účasťou registrátora v hlasovacom procese mu všetky autority dávajú povolenie vykonávať nižšie popísanú činnosť. Očakáva sa, že zariadenie plniace úlohu registrátora sa bude nachádzať na verejne viditeľnom mieste.

Popisovanie vlastného pripradenia kandidátov na predpripravenom hlasom k reálnym kandidátom je komplikované a zdĺhavé. Namiesto toho môžeme použiť nasledovnú konvenciu. Hlasujúci si pri registrácii hlasu môže zvoliť číslo p. Kandidátov na predprivanenom hlase (alternatívne riadky matice A) p-krát cyklicky zrotujeme v kladnom smere (z poslednej pozície posúvame na prvú). Následne sa kandidáti priamočiaro priradia podľa indexov. Prevyšujúci kandidáti na predpripravenom hlase sa priradia poslednému reálnemu kandidátovi. Poznajúc túto konvenciu, môže softvér predpripravujúci hlas vypočítať správne p pre hlasovanie za konkrétnu pozíciu kandidáta (štandardne

označenú písmenami anglickej abecedy) a vytlačiť túto informáciu v čitateľnej podobe. Pri registrácii hlasu potom stačí hlasujúcemu porozumieť jednoduchej informácii tvaru *Ak chcete hlasovať za možnosť C stlačte 5.*

Pri samotnej registrácii príde hlasujúci k registrátorovi a načíta grafickú informáciu obsahujúcu identifikátor predpripraveného hlasu na nástenke. Registrátor overí existenciu a korektnosť hlasu a zobrazí hlasujúcemu možnosť voľby p v rozsahu 1, ..., (p_k). Hlasujúci nahliadne do súkromnej predtlačenej permutácie a zvolí požadovanú možnosť. Registrátor zverejní tieto informácie na nástenke. Následne hlasujúci rozdá informácie obsahujúce s_i a t_i autoritám podľa jeho vôle, tie ich načítajú, prešifrujú a zverejnia. U týchto autorít si zároveň môže overiť, či je na nástenke naozaj zapísané p, ktoré si zvolil. Hlasujúci musí dohliadnuť na to, aby všetky jeho s_i boli korektne načítané. Všetky papierové informácie okrem identifikátora hlasu musia aj po skončení hlasovania zostať v tajnosti.

4.4.5 Prešifrovacia autorita

Odovzdávanie informácií jednotlivým účastníkom hlasovania môže byť nepraktické a zdĺhavé. V niektorých prípadoch môže dávať zmysel oslabiť dôvernost v prospech pohodlnosti. Uvažujme autoritu, ktorá by vykonávala celé prešifrovanie. Autorita by mala úplnú informáciu o hlase a teda by vedela prešifrovať pôvodný hlas, bez zbytočných transformácií. Informácie by však stále zostali aj na nástenke a teda by autorita hlas nevedela zmeniť.

Prešifrovacia autorita môže existovať ako nezávislá samostatná online služba, ktorá uchová dôverné informácie od momentu predprípravy hlasu až do momentu, kedy je registrátorom požiadaná o prešifrovanie. Keďže informácie o zvolenej možnosti a tajomstvá o hlase sú uložené na rôznych miestach a spravované rozdielnymi účastníkmi, bude si porušenie dôvernosti vyžadovať aktívne kroky zo strany autority. Takéto chovanie možno aspoň právne ošetriť – hlasujúci by mal s poskytovateľom služby zmluvu. Hlasovanie bez zariadenia však zjednodušíme na jeden sken a stlačenie jedného tlačítka.

4.5 Podporné mechanizmy

Existujú pomerne jednoduché mechanizmy, ktoré dokážu urýchliť hlasovací proces výmenou za menšie riziká. Jedným takýmto mechanizmom je špeciálny účastník hlasovania nazvaný kalkulátor. Kalkulátor počíta a zverejňuje informácie, ktoré sú verejne odvoditeľné. Zariadenia s menším výpočtovým výkonom, potom tieto informácie počítať nemusia, prípadne ich môžu začať s ich kontrolov až v dobe, kedy neprebiehajú ďalšie výpočty. Vo vlastnom záujme by si však zariadenie malo aspoň dodatočne všetky informácie dooverovať.

Pokiaľ sa na nástenke objaví správne podpísaná nekorektná správa, nastane konfrontácia a hlasovanie sa musí reštartovať. Nástenka však môže aspoň čiastočne kontrolovať informácie v správe a v prípade, že sú nekorektné, správu odmietnuť. Vie tak zabrániť zbytočným konfliktom. Navyše, pokiaľ si nástenka s kalkulátorom navzájom dôverujú, môže ho nástenka využiť na úplnú kontrolu informácií pred tým, než ich zverejní.

5 Formalizácia

Našim cieľom bude formálne zadefinovať priebeh hlasovacieho protokolu navrhnutého v predchádzajúcej kapitole a následne dokázať, prípadne odôvodniť, niektoré jeho vlastnosti. Najskôr si predstavíme konštrukcie, ktoré bude protokol využívať, dostatočne si ich predstavíme a vyslovíme predpoklady o ich rozhraní a vlastnostiach. Väčšina konštrukcií bude štandardných a čitateľ sa o nich môže dozvedieť viac napríklad v práci [4], konštrukcie v časti 5.1.3 sú pôvodné. Neskôr si popíšeme, ako vyzerajú jednotlivé správy a nakoniec dokážeme jednotlivé tvrdenia o protokole. Protokol je všeobecne známy, avšak doplnený. Formalizácia protokolu je pôvodná.

5.1 Východiskové konštrukcie

5.1.1 Šifrovanie

Na utajenie hlasov budeme používať šifrovaciu schému, ktorú navrhol ElGamal. Schéma je homomorfická a umožňuje konštrukciu spoločného verejného kľúča [11]. Fungovanie schémy nebudeme formálne definovať ani dokazovať, nakoľko sa odkazujeme na niekoľko prác, ktoré sa jej venujú. Uvedieme však aspoň základný popis, nakoľko je dôležitý pre pochopenie fungovania protokolu.

Nech G je pevne určená multiplikatívna cyklická grupa a nech g je jej generátor rádu r. Potom pre náhodne zvolené celé x, také že $0 < x < r$, je x súkromným kľúčom a $h = g^x$ k nemu prislúchajúcim verejným kľúčom. Výpočet x za pomoci h je inštanciou problému diskrétneho logaritmu o ktorom sa vo všeobecnosti predpokladá, že pre vhodné G nie je efektívne riešiteľný.

Ak chceme zašifrovať správu $m \in G$, najskôr zvolíme náhodné celé y, také že $0 < y < r$, a skonštruujeme dvojicu $(c_1, c_2) = (g^y, mh^y)$, ktorá je zašifrovaným textom. Prijímateľ potom s pomocou súkromného kľúča vypočíta $c_2(c_1^x)^{-1} = mh^y(g^{yx})^{-1} = mg^{xy}(g^{yx})^{-1} = m$ a teda pôvodnú správu. Zistenie správy bez znalosti x alebo y je tiež redukovateľné na diskrétny logaritmus.

Ak po zložkách vynásobíme tým istým kľúčom zašifrované správy $(g^{y_1}, m_1h^{y_1})$ a $(g^{y_2}, m_2h^{y_2})$, dostaneme dvojicu $(g^{y_1+y_2}, m_1m_2h^{y_1+y_2})$, ktorá je validný zašifrovaný text

pre správu $m_1 m_2$. Indukciou potom ukážeme, že ak zašifrovanú správu m po zložkách umocníme na k-tu, dostaneme validne zašifrovanú m^k.

Predpokladajme ďalej, že grupa G je Schnorrova [18]. Rád r generátora g je teda prvočíslo a $N_r = \{0, 1, 2, \ldots r-1\}$ je pole. Prvok $n \in N_r$ môžeme zakódovať ako správu $m = g^n$ [9], pričom pre súčin správ platí $m_1 m_2 = g^{n_1+n_2}$. Podobne $m^k = g^{kn}$. Násobením a umocňovaním zašifrovaných textov teda sčítavať a násobiť pôvodné zakódované prvky N_r, čo nám umožní manipuláciu s hlasmi bez nutnosti odšifrovania.

Iná vhodná predstava, je vnímať všetky možné zašifrovania $(g^y, g^n h^y)$ prvkov poľa N_r ako vektorový priestor, pričom násobenie po zložkách je sčítanie vektorov a umocňovanie po zložkách na konštantu je násobenie vektorov touto konštantou. Keďže modulus N_r je rádom generátora g, všetky operácie sú uzatvorené. Odšifrovanie je potom homomorfizmus do jednorozmerného priestoru nad N_r. Je teda zjavné, že akékoľvek operácie nad zašifrovanými správami sa homomorfizmom prenesú na odšifrovanú hodnotu.

Posledná užitočná konštrukcia je násobenie verejných kľúčov. Správu zašifrovanú pomocou súčinu dvoch verejných kľúčov $(g^y, m h_1^y h_2^y)$ možno odšifrovať postupným výpočtom $(g^y)_1^x$ a $(g^y)_2^x$, ktoré nazveme čiastočné odšifrovania, a následným predelením výrazu $m h_1^y h_2^y$ čiastočnými odšifrovaniami.

Zistené skutočnosti si teraz sformalizujeme do rozhrania, ktoré budeme v ďalšom texte používať.

Predpoklad 5.1.1. *Existuje šifrovacia schéma ElGamal s procedúrami*

- $Generate() \to (PK, SK)$
- $Combine(PKs) \to PK$
- $Encrypt(PK, n \in N_r) \to C$
- $DecryptShare(SK, C) \to d$
- $Decrypt(D, C) \to n \in N_r$

, predikátom

- $Matches(PK, SK)$

a operáciou $(\cdot)$ definovanou na zašifrovaných hodnotách takými, že:

- $Matches(Generate())$
- $Combine(\{PK\}) = PK$
- *je extrémne výpočtovo náročné zistiť hodnotu SK príslušnú k danému PK*
- *bez znalosti SK príslušného k PK je extrémne výpočtovo náročné zistiť hodnotu m z výsledku $Encrypt(PK, m)$.*
- *je extrémne výpočtovo náročné zistiť hodnotu vstupného SK z výstupu DecryptShare a to aj v prípade slobodnej voľby zvyšných parametrov.*
- *znalosť menej ako všetkých hodnôt SK_i príslušných k daným PK_i, nezmení náročnosť výpočtu SK príslušného k výsledku $Combine(\{PK_i\})$*
- *pokiaľ*

- $Matches(PK_i, SK_i)$ *pre* $i \in I$
- $PK := Combine(\{PK_i \mid i \in I\})$
- $C_j := Encrypt(PK, m_j)$ *pre* $j \in J$,

tak

$$\sum_{j \in J} m_j = Decrypt(\{DecryptShare(SK_i, \prod_{j \in J} C_j) \mid i \in I\}, C)$$

Pri hlasovaní teda najskôr vynásobíme všetky verejné kľúče autorít, potom každý hlasujúci vytvorí pre každého kandidáta jeden hlas tak, aby všetky obsahovali práve jednu jednotku a zvyšné nuly. Následne zašifrované hlasy sčítame a súčty bezpečne odšifrujeme bez straty anonymity. Výsledky sú v tvare g^l, kde l je počet hlasov, ktoré dotyčný kandidát získal. Keďže toto číslo je pomerne malé, vieme ho efektívne zistiť odskúšaním všetkých možností. Je však potrebné dokázať, že sme pri jednotlivých krokoch postupovali správne.

5.1.2 Bezznalostné dôkazy

Pri bezznalostných dôkazoch budeme používať iba všeobecne známe protokoly, ktoré nebudeme do hĺbky rozoberať. Pôvodné interaktívne dôkazy môžeme Fiat-Shamirovou konštrukciou [12] upraviť do formy, kedy stačí ku správe priložiť výpočty založené na hešoch už existujúcich hodnôt. Predídeme tak zbytočnej komunikácii a umožníme ich všeobecnú overiteľnosť. Všetky spomenuté konštrukcie si čitateľ môže naštudovať buď priamo v zdrojových prácach alebo menej formálne v článku [4].

Na dôkaz znalosti súkromného kľúča prislúchajúceho ku konkrétnemu verejnému môžeme použiť Schnorrov protokol [18]. Dôkaz je dôležitý najmä preto, aby potenciálny útočník nemohol ako svoj verejný kľúč prezentovať účelovo zvolené číslo.

Predpoklad 5.1.2. *Existuje predikát Schnorr a metóda, ktorou je za pomoci SK príslušného k danému PK možné získať dôkaz p taký, aby platilo* $Schnorr(p, PK)$. *Zároveň je extrémne výpočtovo náročné získať p bez znalosti SK a znalosť p nezmení náročnosť výpočtu SK.*

Na dôkaz správneho čiastočného odšifrovania použijeme Chaum-Pedersenov protokol [6]. Tento protokol možno tiež použiť na dôkaz, že sme zašifrovali jednu konkrétnu hodnotu. S Cramer-Damgård-Schoenmakersovou konštrukciou alternatívy [8] ho následne vieme rozšíriť na dôkaz, že sme zašifrovali jednu z malej množiny hodnôt.

Predpoklad 5.1.3. *Existuje predikát OneOf a metóda, ktorou je popri konštrukcii* $C := Encrypt(PK, m)$ *pre danú* $M \supseteq \{m\}$ *možné získať dôkaz p taký, aby platilo* $OneOf(p, PK, C, M)$. *Zároveň je extrémne výpočtovo náročné získať p pokiaľ* $m \notin M$ *a v prípade* $|M| > 1$ *znalosť p nezmení náročnosť výpočtu m.*

Predpoklad 5.1.4. *Existuje predikát ValidDecryption a metóda, ktorou je popri konštrukcii* $d := DecryptShare(SK, C)$ *možné získať dôkaz* p *taký, aby platilo* $ValidDecryption(p, PK, c$ *Zároveň je extrémne výpočtovo náročné získať* p *pokiaľ* $d \neq DecryptShare(SK, C)$ *a znalosť* p *nezmení náročnosť výpočtu* SK*.*

5.1.3 Prešifrovanie

V nasledujúcom texte nadviažeme na časť 4.4.3 vysvetlením detailov prešifrovania. Pre lepšiu orientáciu čitateľa následne ešte raz popíšeme aj celý proces preprípravy hlasov.

Predpokladajme, že hlasujúci bez zariadenia zverejnil zašifrovanú správu $(c_1, c_{2,orig}) = (g^y, mh^y_{orig})$. Hodnotu y zverejnil jednej autorite, ktorej úlohou bude zašifrovať hodnotu pre verejný kľúč h_{new}. Budeme od nej vyžadovať aby použila tú istú hodnotu y. Bude teda musieť zverejniť zašifrovanú správu v tvare $(c_1, c_{2,new})$ pre nejaké $c_{2,new} \in G$. Nech $m_{new} = c_{2,new}h^{-y}_{new}$. Prešifrovanie je správne práve vtedy, keď $m = m_{new}$. Každý však môže skonštruovať aj tretiu zašifrovanú správu

$$(c_1, c_{2,orig}c^{-1}_{2,new}) = (g^y, mm^{-1}_{new}(h_{orig}h^{-1}_{new})^y)$$

, ktorá je zašifrovaním hodnoty mm^{-1}_{new} pri verejnom kľúči $h_{orig}h^{-1}_{new}$. Správnosť prešifrovania potom možno dokázať bezznalostným dôkazom, že $(c_1, c_{2,orig}c^{-1}_{2,new})$ je zašifrovaná $1 = g^0$.

Tvrdenie 5.1.5. *Pokiaľ autor správy* $C_1 = (a_1, b_1)$ *zašifrovanej kľúčom* PK_1 *poskytne inému užívateľovi tajomstvá, ktoré sa dozvedel pri šifrovaní, je tento užívateľ schopný zgenerovať správu* $C_2 = (a_2, b_2)$ *zašifrovanú kľúčom* PK_2 *a bezznalostný dôkaz* p *faktu, že* C_1 *a* C_2 *sú šiframi tej istej správy. Dôkaz je možné overiť súčasnou platnosťou* $a_1 = a_2$ *a* $OneOf(p, PK_1 \cdot PK_2^{-1}, (a_1, b_1b_2^{-1}), \{0\})$*.*

Pri vytváraní predpripraveného hlasu autor zverejní zašifrované hodnoty $s_1, s_2, \ldots s_n$, $h_1, h_2, \ldots h_m$, všetky z N_r, maticu A takú, že $A \cdot \overrightarrow{s} = \overrightarrow{h}$, a surjektívne priradenie $\pi : \{1 \ldots m\} \to K$. Niektoré z týchto hodnôt môžu byť fixné a dokonca sme aj uviedli ich hodnoty. Ďalej zverejní dôkaz, že $\overrightarrow{h}$ je platný hlas pre m kandidátov. Pri hlasovaní rozdá jednotlivé s_i medzi n autorít aj s tajomstvami, ktoré získal pri ich obstarávaní. Autority s_i prešifrujú a teda je možné vďaka homomorfickosti skonštruovať prešifrovaný hlas. Ten sa započíta ku správnym kadidátom podľa π.

Všetky kroky sú overiteľné a teda si každý môže byť istý, že sa započítal správny hlas. Pokiaľ navyše platí, že každých n stĺpcov A je lineárne nezávislých, na zistenie akejkoľvek informácie o hlase treba poznať viac ako $n - m$ z hodnôt s_i. Na zachovanie dôvernosti nám teda stačí m autorít, ktoré nevyzradia zistenú hodnotu y.

5.1.4 Autentifikácia

Na autorizáciu jednotlivých správ budeme potrebovať podpisovú schému. Keďže existujú všeobecne známe, používané a otestované riešenia tohto problému, implementáciou sa zaoberať nebudeme. Jedným z možných riešení je použiť schému RSA [16].

Predpoklad 5.1.6. *Existuje podpisová schéma SignatureScheme taká, že skonštruovať podpis bez znalosti súkromného kľúča je extrémne výpočtovo náročné.*

Implementáciu autorizácie účastníkov sme sa rozhodli z protokolu vynechať. Vyslovíme teda iba predpoklad o nevyhnutnom rozhraní na jej používanie:

Predpoklad 5.1.7. *Existuje predikát IsAuthenticated a metóda, ktorou môže jedine účastník hlasovania u obdržať token t taký, že platí*

$$IsAuthenticated(t, u, PSK_u)$$

, kde PSK_u je ľubovoľný verejný kľúč podpisovej schémy SignatureScheme, ktorý si účastník počas obstarávania t zvolil.

5.1.5 Nástenka

Formalizácia nástenky by priniesla zbytočnú priestorovú zložitosť a repetitívnosť. Budeme preto predpokladať, že existuje ideálna nástenka, ktorá prijíma všetky správy, zobrazuje každú prijatú správu v pôvodnom znení a zároveň poskytuje aktuálny zoznam všetkých správ týkajúcich sa konkrétneho hlasovania. Každej správe zároveň priradí unikátnu časovú pečiatku.

Ako vynútiť väčšinu z tohto správania sme si popísali v časti 4.2.2. Pri poskytovaní aktuálneho zoznamu môže reálna nástenka tento zoznam podpísať spolu s časom, v ktorom bol aktuálny. Prípadná snaha o utajenie správy bude potom napadnuteľná (v prípade podvodu má autor správy podpis časovej pečiatky a autor zoznamu má podpis údajne kompletného zoznamu z neskoršej dobe bez inkriminovanej správy). V prípade presného časového stretu dvoch požiadaviek možno unikátnosť časovej pečiatky zabezpečiť losom.

5.2 Typy správ

Platné hlasovanie bude definované ako množina správ zverejnených na nástenke. Každá správa bude jednoznačne identifikovaná typom a zoznamom parametrov. Typ určuje štruktúru správy, počet parametrov, typ autora a charakter obsiahnutých informácií. Parametre viažu tieto informácie s konkrétnymi entitami. Samozrejme, nemôžeme zabrániť tomu, aby sa na nástenke objavilo viac správ s rovankým typom aj hodnotami parametrov.

Na referencovanie správ budeme používať konvenciu známu z mnohých imperatívnych jazykov, kde typ správy zreťazíme s n-ticou parametrov. Správu typu *TEST* s parametrami a a b teda definujeme ako $TEST(a, b)$ a jej konkrétnu inštanciu ako $TEST(42, 47)$.

Každá správa nesie sériu lokálnych informácií zaujímavých iba v kontexte správy samotnej a sériu globálnych informácií, ktoré budú využívané v nadväzujúcich správach a pri výpočte výsledku. Globálne informácie sú vždy indexované parametrami a teda dve rôzne správy nemôžu poskytovať ten istý globálny parameter. Okrem toho správa obsahuje aj zoznam správ, na ktoré nadväzuje, zvaných prerekvizity.

Definícia 5.2.1. *Správa je objekt vytvorený a zverejnený účastníkom volebného procesu, ktorý obsahuje:*

- *signatúru pozostávajúcu z typu a zoznamu parametrov*
- *zoznam globálnych hodnôt*
- *zoznam lokálnych hodnôt*
- *zoznam iných správ nazývaných prerekvizity*
- *identifikátor autora*
- *podpis autora*
- *unikátnu časovú pečiatku zverejnenia*

5.2.1 Úvodná fáza protokolu

Autorom prvej správy je zakladateľ, ktorý zverejní zoznam kandidátov. Okrem toho zverejní aj podpisový kľúč. Keďže však iba tlmočí verejne známe rozhodnutia, ktoré musia byť dodatočne schválené ďalšími účastníkmi a navyše je ako autor pozvánok k hlasovaniu dopátrateľný, nie je potrebná autentifikácia zakladateľa.

Predpoklad 5.2.1. *Existuje zakladateľ volebného protokolu označený ako creator.*

Definícia 5.2.2. *Štruktúra správy typu HELLO() je nasledovná:*

- *autorom je creator*
- *obsahuje práve tieto globálne hodnoty:*
  - $PSK_{creator}$ *– verejný podpisový kľúč zakladateľa*
  - $\mathcal{K}$ *– množina kandidátov*
- *obsahuje práve tieto lokálne hodnoty:*
  - t *– obdržaný autorizačný token*
- *nemá žiadne prerekvizity*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $IsAuthenticated(t, creator, PSK_v)$

Na správu odpovedajú jednotliví účastníci, ktorí majú záujem zúčastniť sa hlasovania. Zverejnia svoj verejný podpisový kľúč, doklad o tom, že boli autentifikovaný, a v prípade, že sú to autority, aj verejný šifrovací kľúč.

Definícia 5.2.3. *Štruktúra správy typu $VOTER(v)$ je nasledovná:*

- *autorom je hodnota parametra v*
- *obsahuje práve tieto globálne hodnoty:*
  - *PSK_v – verejný podpisový kľúč identity v*
- *obsahuje práve tieto lokálne hodnoty:*
  - *t – obdržaný autorizačný token*
- *prerekvizity majú nasledovné hodnoty:*
  - *$HELLO()$*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- *$IsAuthenticated(t, v, PSK_v)$*

Definícia 5.2.4. *Štruktúra správy typu $AUTHORITY(a)$ je nasledovná:*

- *autorom je hodnota parametra a*
- *obsahuje práve tieto globálne hodnoty:*
  - *PSK_a – verejný podpisový kľúč identity a*
  - *PK_a – verejný šifrovací kľúc autority a*
- *obsahuje práve tieto lokálne hodnoty:*
  - *t – obdržaný autorizačný token*
  - *p – dôkaz znalosti súkromného kľúča pre PK_a*
- *prerekvizity majú nasledovné hodnoty:*
  - *$HELLO()$*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- *$IsAuthenticated(t, a, PSK_a)$*
- *$Schnorr(p, PK_a)$*

Definícia 5.2.5. *Štruktúra správy typu $REGISTRAR(r)$ je nasledovná:*

- *autorom je hodnota parametra r*
- *obsahuje práve tieto globálne hodnoty:*
  - *PSK_r – verejný podpisový kľúč identity r*
- *obsahuje práve tieto lokálne hodnoty:*
  - *t – obdržaný autorizačný token*
- *prerekvizity majú nasledovné hodnoty:*
  - *$HELLO()$*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- *$IsAuthenticated(t, r, PSK_r)$*

Keď sa zakladateľ rozhodne, že už sa prihlásili všetci potenciálni účastníci, vyberie, ktorí účastníci by mali byť akceptovaní (napríklad na základe diskusie cez audiovizuálny kanál) a zverejní ich zoznamy. Autority musia s týmto zoznamom explicitne súhlasiť.

Definícia 5.2.6. *Štruktúra správy typu START() je nasledovná:*

- *autorom je creator*
- *obsahuje práve tieto globálne hodnoty:*
  - U_V *– zoznam zapojených voličov*
  - U_R *– zoznam zapojených registrátorov predpripravených hlasov*
  - U_A *– zoznam zapojených autorít*
- *neobsahuje žiadne lokálne hodnoty*
- *prerekvizity majú nasledovné hodnoty:*
  - $HELLO()$
  - $VOTER(v)$ *pre všetky* $v \in U_V$
  - $REGISTRAR(r)$ *pre všetky* $r \in U_R$
  - $AUTHORITY(a)$ *pre všetky* $a \in U_A$

Na správy tohto typu nie sú kladené žiadne sémantické podmienky.

Definícia 5.2.7. *Štruktúra správy typu* $STARTED(a)$ *je nasledovná:*

- *autorom je hodnota parametra a*
- *neobsahuje žiadne globálne hodnoty*
- *neobsahuje žiadne lokálne hodnoty*
- *prerekvizity majú nasledovné hodnoty:*
  - $START()$
  - $AUTHORITY(a)$

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $a \in U_A$

Po úspešnom úvode je možné vypočítať verejný kľúč.

Definícia 5.2.8. *Spoločný verejný kľúč je výraz* $PK = Combine(\{PK_a \mid a \in U_A\})$

5.2.2 Hlasovanie

Hlasovanie účastníkov so zariadením prebehne po tom, čo všetky zvolené autority odsúhlasia zoznam účastníkov. Stačí práve jedna správa od každého voliča.

Definícia 5.2.9. *Štruktúra správy typu* $VOTE(v)$ *je nasledovná:*

- *autorom je hodnota parametra v*
- *obsahuje práve tieto globálne hodnoty:*
  - $V_{v,k}$ *pre všetky* $k \in \mathcal{K}$ *– zašifrovaný hlas za konkrétneho kandidáta*
- *obsahuje práve tieto lokálne hodnoty:*

  - p_k *pre všetky* $k \in \mathcal{K}$ *– dôkazy správnosti hlasu za konkrétneho kandidáta*
  - p *– dôkaz správnosti súčtu hlasov*
- *prerekvizity majú nasledovné hodnoty:*
  - $START()$
  - $VOTER(v)$
  - $STARTED(a)$ *pre všetky* $a \in U_A$

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $v \in U_V$
- $OneOf(p_k, PK, V_{v,k}, \{0,1\})$ *pre všetky* $k \in \mathcal{K}$
- $OneOf(p, PK, \prod_{k \in \mathcal{K}} V_{v,k}, \{1\})$

5.2.3 Predpripravené hlasy

Predpripravený hlas nemá žiadne prerekvizity a teda sa na nástenke môže zverejniť v ľubovoľnom čase. Za súčasť komunikácie patriacej k hlasovaniu ho však začneme považovať až v momente, kedy sa použije.

Definícia 5.2.10. *Štruktúra správy typu* $PREPARE(e)$ *je nasledovná:*

- *autorom je hodnota parametra* e
- *obsahuje práve tieto globálne hodnoty:*
  - PSK_e *– verejný podpisový kľúč identity* e
  - PK_e *– verejný šifrovací kľúč použitý pre tento hlas*
  - n_e *– počet tajomstiev predpripraveného hlasu*
  - m_e *– počet kandidátov predpripraveného hlasu*
  - $V'_{e,k}$ *pre všetky* $k \in \{1..m_e\}$ *– zašifrované časti hlasu*
  - $s'_{e,i}$ *pre všetky* $i \in \{1..n_e\}$ *– zašifrované tajomstvá hlasu*
- *obsahuje práve tieto lokálne hodnoty:*
  - t *– obdržaný autorizačný token*
  - q *– bezznalostný dôkaz znalosti súkromného kľúča pre* PK_e
  - p_k *pre všetky* $k \in \{1..m_e\}$ *– dôkaz správnosti hlasu za konkrétneho kandidáta*
  - p *– bezznalostný dôkaz správnosti súčtu hlasu*
- *nemá žiadne prerekvizity*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $m_e \leq n_e$
- $IsAuthenticated(t, e, PSK_e)$
- $Schnorr(e, PK_e)$
- $OneOf(p_k, PK, V'_{v,k}, \{0,1\})$ *pre všetky* $k \in \{1..m_e\}$
- $OneOf(p, PK, \prod_{k \in \{1..m_e\}} V'_{v,k}, \{1\})$
- $V'_{e,k} = \prod_{i \in \{1..n_e\}} (s'_{e,i})^{a_{k,i}}$ *pre všetky* $k \in \{1..m_e\}$

Samotná registrácia začína pri registračnom zariadení. Kvôli jednoduchosti predpokladajme, že zariadenie preloží na konvenčnej dohode (uvedenej v časti 4.4.4) založené číslo p na priradenie π. Kvôli jednoduchosti neuvažujeme možnosť prešifrovacej autority. Jej dotefinovanie je však len technickým cvičením.

Definícia 5.2.11. *Štruktúra správy typu REGISTER(e) je nasledovná:*

- *autorom je hodnota r_e*
- *obsahuje práve tieto globálne hodnoty:*
  - *r_e – registrátor použitý na regsitráciu predpripraveného hlasu identity e*
  - *π_e – priradenie $\{1..m_e\} \to \mathcal{K}$*
- *neobsahuje žiadne lokálne hodnoty*
- *prerekvizity majú nasledovné hodnoty:*
  - *START()*
  - *STARTED(a) pre všetky $a \in U_A$*
  - *REGISTRAR(r_e)*
  - *PREPARED(e)*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $r \in U_R$

Nasleduje rozdelenie tajomstiev medzi autority a prešifrovanie správy.

Definícia 5.2.12. *Štruktúra správy typu REENCRYPT(e, i) je nasledovná:*

- *autorom je hodnota $a'_{e,i}$*
- *obsahuje práve tieto globálne hodnoty:*
  - *$a'_{e,i}$ – autorita použitá na prešifrovanie $s_{e,i}$*
  - *$s_{e,i}$ – prešifrovaná hodnota tajomstva*
- *obsahuje práve tieto lokálne hodnoty:*
  - *p – bezznalostný dôkaz správneho prešifrovania*
- *prerekvizity majú nasledovné hodnoty:*
  - *REGISTER(e)*
  - *STARTED$(a'_{e,i})$*

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $a'_{e,i} \in U_R$
- $(x, y) = s_{e,i} \wedge (x', y') = s_{e,i} \wedge x = x' \wedge \mathit{OneOf}(p, PK_e \cdot PK^{-1}, (x, y'y^{-1}), \{0\})$

Je možné, že počas registrácie tajomstiev u autorít nastane problém (napríklad strata čiastočnej informácie). Preto má registračné zariadenie možnosť pri ukončovaní svojej činnosti určiť, ktoré predpripravené hlasy majú byť vo výsledku započítané. Ak je hlasujúci vylúčený neprávom, možno sa na situáciu pozerať, ako keby jeho účasť bola odmietnutá všeobecne – svoje práva si musí vymáhať mimo protokolu.

U hlasujúcich, ktorých hlasy majú byť použité musíme počkať na registráciu všetkých tajomstiev.

Definícia 5.2.13. *Štruktúra správy typu CLOSED(r) je nasledovná:*

- *autorom je hodnota parametra r*
- *obsahuje práve tieto globálne hodnoty:*
  - E_r *– zoznam akceptovaných kandidátov*
- *neobsahuje žiadne lokálne hodnoty.*
- *prerekvizity majú nasledovné hodnoty:*
  - $START()$
  - $REGISTRAR(r)$
  - $REGISTER(e)$ *pre všetky* $e \in E_r$
  - $REENCRYPT(e, i)$ *pre všetky* $e \in E_r$ *a* $i \in \{1..n_e\}$

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $r \in U_R$
- $r_e = r$ *pre všetky* $e \in E_r$

5.2.4 Sčítanie

Sčítanie hlasov je podobne jednoduché ako hlasovanie. Stačí aby každá autorita spočítala a čiastočne odšifrovala súčty pre kandidátov a zverejnila informácie. Výsledok bude následne verejne dopočítateľný a ako sa nám podarí ukázať, aj overiteľný.

Definícia 5.2.14. *Zašifrovaný súčet hlasov pre kandidáta* $k \in \mathcal{K}$ *je výraz*

$$S'_k = \prod_{v \in U_V} V_{v,k} \cdot \prod_{r \in U_R} \prod_{e \in E_r} \prod_{l \in \{1..m_e\} \wedge \pi_e(l) = k} \prod_{i \in \{1..n_e\}} (s'_{e,i})^{a_{l,i}}$$

Definícia 5.2.15. *Štruktúra správy typu DECRYPT(a) je nasledovná:*

- *autorom je hodnota parametra v*
- *obsahuje práve tieto globálne hodnoty:*
  - $d_{a,k}$ *pre všetky* $k \in \mathcal{K}$ *– odšifrovaný podiel autority a z hodnoty* S'_k
- *obsahuje práve tieto lokálne hodnoty:*
  - p_k *pre všetky* $k \in \mathcal{K}$ *– dôkaz správnosti odšifrovania*
- *prerekvizity majú nasledovné hodnoty:*
  - $STARTED(a)$
  - $VOTE(v)$ *pre všetky* $v \in U_V$
  - $CLOSED(r)$ *pre všetky* $r \in U_R$

Navyše, správy tohto typu musia spĺňať nasledovné sémantické podmienky:

- $a \in U_A$
- $ValidDecryption(p_k, S'_k, PK_k, d_{a,k})$ *pre všetky* $k \in \mathcal{K}$

Definícia 5.2.16. *Súčet hlasov pre kandidáta* $k \in \mathcal{K}$ *je výraz*

$$S_k = Decrypt(\{d_{a,k} \mid a \in U_A\}, S'_k)$$

5.3 Vlastnosti správ

Postupne budeme iterovať definíciami z predchádzajúcej sekcie a dokazovať o nich čoraz silnejšie tvrdenia. Začneme však definíciou korektnej správy.

Definícia 5.3.1. *Hlasovanie je ľubovoľná množina zverejnených správ.*

Definícia 5.3.2. *Správa je korektná v danom hlasovaní ak spĺňa všetky nasledovné podmienky:*

- *jej typ je zadefinovaný a má správny počet parametrov*
- *neexistuje skôr zverejnená správa rovnakej signatúry v danom hlasovaní*
- *má typom stanovenú štruktúru*
- *všetky jej prerekvizity sú zverejnené skôr a sú korektné*
- *spĺňa typom stanovené sémantické podmienky*
- *je podpísaná verejným podpisovým kľúčom jej autora*

Fakt, že sme korektnosť zadefinovali, ešte neznamená, že ju vieme rozhodovať alebo že vôbec existuje. Typové definície používali mnoho premenných, ktoré nemusia mať určené hodnoty. Treba sa teda pozrieť na tieto premenné a ich dostupnosť.

Definícia 5.3.3. *Relácia x je prechodcom y je reflexívno-tranzitívnym uzáverom relácie x je prerekvizitou y*

Definícia 5.3.4. *Hovoríme, že správa vidí hodnotu, pokiaľ je to lokálna hodnota obsiahnutá v danej správe alebo globálna hodnota obsiahnutá v niektorom z predchodcov správy.*

Tvrdenie 5.3.1. *Ak je správa korektná, vidí každú hodnotu najviac raz.*

Dôkaz. Môžeme ľahko overiť, že každá typová definícia používa inú sadu globálnych premenných, každá globálna premenná je indexovaná aspoň parametrami a žiadne lokálne premenné nie sú v konflikte so žiadnymi globálnymi. Konflikt dvoch globálnych premenných by teda znamenal rovnakú signatúru, čo je u korektných správ vylúčené. □

Tvrdenie 5.3.2. *Ak je správa korektná, vidí každú hodnotu použitú v jej definícii.*

Dôkaz. Pri dôkaze treba postupovať opatrne. Postupne iterujme cez všetky zadefinované typy v poradí ich definície. Ak máme korektnú správu, ktorá je tohto typu, môžeme začať postupne budovať množinu viditeľných hodnôt. Začneme tými, ktoré nie su závislé na iných a postupne pridávame nové hodnoty a identifikujeme prerekvizity, ktoré sú skorších typov a teda trvdenie pre ne už platí. Čitateľ sa môže presvedčiť, že týmto postupom sa dopracuje ku nadmnožine všetkých použitých hodnôt, pri všetkých typových definíciách. Treba ešte upozorniť, že symboly PK, S'_k a S_k označujú celé výrazy, ktoré musia byť substituované. □

Tvrdenie 5.3.3. *Vieme rozhodovať korektnosť správ.*

Dôkaz. Prechádzajme správy v poradí, v akom boli zverejnené. Pri každej správe overme jej typ a počet parametrov. Overme tiež, že všetky jej prerekvizity sú korektné (musia byť skôr zverejnené, teda sme ich už rozhodli) a vybudujme z nich základnú množinu viditeľných hodnôt. Pridajme do tejto množiny aj hodnoty zadefinované v správe. Podľa predchádzajúceho tvrdenia by teraz v tejto množine mali byť všetky hodnoty použité v typovej definícii. Ak to tak nie je, správa je nekorektná. Ak to tak je, môžeme overiť všetky podmienky korektnosti. □

Podarilo sa nám teda nájsť postup ako správy validovať a teda vieme rozlíšiť korektné hlasovanie. Zamyslime sa teraz na existenciou takéhoto hlasovania ako aj nad jeho vlastnosťami.

Definícia 5.3.5. *Množinu všetkých korektných hlasov v hlasovaní nazveme korektné hlasovanie.*

Definícia 5.3.6. *Korektné hlasovanie je kompletné, ak obsahuje správu $START()$ a na základe hodnôt v tejto správe aj všetky správy typu:*

- $DECRYPT(a)$ *pre všetky* $a \in U_A$
- $VOTE(v)$ *pre všetky* $v \in U_V$
- $CLOSED(r)$ *pre všetky* $r \in U_R$

Tvrdenie 5.3.4. *Z korektného hlasovania vieme vyhodnotiť súčet hlasov S_k pre každého kandidáta $k \in \mathcal{K}$.*

Dôkaz. Stačí overiť, že všetky použité hodnoty sú dosiahnuteľné so správ uvedených definícii korektnosti. □

Tvrdenie 5.3.5. *Korektné hlasovanie môže vzniknúť.*

Dôkaz. Ak budú správy pribúdať v súlade s navrhnutým protokolom, problém s prerekvizitami nenastane. Zaujímavé je však overiť, či autori správ dokážu zabezpečiť sémantické podmienky. Splniteľnosť väčšiny z nich sme podložili tvrdeniami v prvej časti tejto kapitoly. Zvyšok sú podmienky na parametre vymedzujúce účastníkov hlasovania, ktoré možno splniť triviálne. □

Tvrdenie 5.3.6. *Korektné hlasovanie môže vzniknúť.*

Dôkaz. Ak budú správy pribúdať v súlade s navrhnutým protokolom, problém s prerekvizitami nenastane. Zaujímavé je však overiť, či autori správ dokážu zabezpečiť sémantické podmienky. Splniteľnosť väčšiny z nich sme podložili tvrdeniami v prvej časti tejto kapitoly. Zvyšok sú podmienky na parametre vymedzujúce účastníkov hlasovania, ktoré možno splniť triviálne. □

Tvrdenie 5.3.7. *Porušenie všeobecnej overiteľnosti, individuálnej overiteľnosti aj overiteľnosti správnosti kompletného hlasovania je extrémne výpočtovo náročné.*

Tvrdenie 5.3.8. *Porušenie dôvernosti kompletného hlasovania voči hlasujúcemu so zariadením je extrémne výpočtovo náročné alebo si vyžaduje kooperáciu všetkých autorít.*

Tvrdenie 5.3.9. *Porušenie dôvernosti kompletného hlasovania voči hlasujúcemu bez zariadenia je extrémne výpočtovo náročné alebo si vyžaduje kooperáciu všetkých autorít alebo si vyžduje kooperáciu aspoň $n_e - m_e$ z tých autorít, ktoré obdržali jeho tajomstvá.*

Dôkazy posledných troch tvrdení možno konštruovať sporom. Predpokladajme, že vlastnosť je porušená ale zároveň nie je splnená žiadna z uvedených príčin. Postupne tak preiterujeme všetkými zasiahnutými správami až sa dostaneme ku poslednej možnej príčine, ktorá tiež splnená nebude. Ako argumentačné nástroje by nám mali slúžiť predpoklady z prvej časti a ako ukazovateľ smeru, vysokoúrovňové myšlienky, ktoré sme počas návrhu protokolu vyslovili. Podrobné dôkazy sú však príliš technické a náročné a teda ich vynecháme.

Formalizácia protokolu neobsahuje nástroje na argumentovanie o jeho robustnosti a teda tvrdenia vyslovovať nebudeme.

6 Výsledky

Úlohou tejto kapitoly je zhromaždiť poznatky, ktoré autor nadobudol počas svojej práce, ako aj zopár výsledkov, ku ktorým sa dopracoval. Postupovať budeme chronologicky od zistení pri rozbore, cez protokol až po pokus o implementáciu.

6.1 Hlasovanie v reálnom čase ako slabo pokrytá oblasť

Už pri rozbore modelových situácií sa nám podarilo identifikovať značný rozdiel medzi požadovaným modelom hlasovania a tým, ktorý je bežne skúmaný. Na rozdiel od veľkoplošného hlasovania počas dlhšieho obdobia, kde je najväčšou výzvou počet hlasujúcich alebo ochrana pred pravdepodobne veľkým tlakom korupciu, sme totiž potrebovali hlasovanie v reálnom čase s dôrazom na rýchlosť a jednoduchosť.

Jedným z dôvodov, prečo malé hlasovania nie sú skúmané, môže byť nutná hardvérová vybavenosť hlasujúcich, ktorá bola donedávna ťažko zabezpečiteľná. V dnešnej dobe sa táto situácia mení a teda téma sa stáva aktuálnejšou. Stále si však treba dávať pozor na skutočnosť, že nie každý člen skupiny vlastní vhodné zariadenia a že pri práci s vlastnými zariadeniami môže nastať veľké množstvo problémov.

Našli sme teda slabo pokrytú oblasť, ktorá má široké praktické uplatnenie a ponúka nám inú sadu výziev než klasické elektronické voľby. Aj keď sme niektoré najkritickejšie problémy vyriešili, stále je tu obrovský na zlepšovanie, najmä v oblasti nedokázateľnosti.

6.2 Protokol

Na základe vyšpecifikovaných podmienok sa nám úspešne podarilo navrhnúť dôverný a overiteľný protokol pre hlasovania v reálnom čase s malým počtom hlasujúcich. Na rozdiel od zaužívaných techník pri návrhoch protokolov sme do úvahy brali aj implementačné detaily a dostupné zdroje. Dosiahli sme tak niekoľko zaujímavých odlišností.

Protokol je navrhnutý na pre beh na osobných zariadeniach hlasujúcich, okrem ktorých vyžaduje už iba jednu ďalšiu entitu, nástenku. Vplyv nástenky na hlasovanie

je pomerne malý a jediný útok, ktorého je schopná, je sabotáž. Toto ponechá celý vplyv v rukách hlasujúcich a potenciálne zvýši dôveru laického používateľa.

Hlasovať je možné aj bez vlastného zariadenia. Hlas sa predpripraví v ľubovoľnom čase pred začiatkom hlasovania a následne sa rozdistribuuje medzi niekoľko účastníkov. Títo potom získajú kolektívnu informáciu o zvolenom kandidátovi, overiteľnosť však zostane rovnaká. Alternatívne možno dôverné informácie presunúť na externú službu a súkromie si upraviť právnou cestou. Týmto spôsobom získame jednoduché hlasovanie bez zariadenia, kde si na jeden krok možno predpripraviť ľubovoľné množstvo hlasov a potom jedným krokom kedykoľvek zahlasovať.

Na druhej strane, navrhnutý protokol účastníkom zariadeniam plný dôkaz o zvolenom kandidátovi, ktorým môžu presvedčiť potenciálneho útočníka. Nedokázateľnosť je jedna z najviac skúmaných oblastí v súčastnosti a naša práca ju vylúčila už pri určovaní podmienok. Protokol si tiež vyžaduje online účasť všetkých hlasujúcich počas celého procesu a má nezanedbateľné výpočtové nároky. Poslednou značnou nevýhodou oproti štandardným prácam je nutnosť vopred špecifikovanej konečnej množiny kandidátov.

Aj keď veľká časť protokolu vznikla úpravou a prispôsobením existujúcich riešení, niektoré prvky a mnohé detaily však autor považuje za vlastnú tvorivú činnosť. Okrem samotného návrhu je protokol aj podrobne formálne zadefinovaný, čo by malo uľahčiť jeho implementáciu.

6.3 Implementácia

Súčasťou práce bol aj pokus o implementáciu protokolu, ktorý, bohužiaľ, skončil neúspešne. Existujúci kód však pokrýva aspoň niektoré časti protokolu, existuje robustný a pomerne stručný architektonický návrh finálneho produktu a autor dokáže posúdiť pripravenosť webovej platformy na kryptografické výpočty. Zdrojový kód možno nájsť na adrese `https://github.com/syslo/nestvoting`, architektúra je stručne popísaná v Prílohe A.

Za nedokončením implementácie stáli dva významné dôvody. Prvým bola architektúra, ktorá bola príliš komplikovaná pre jednoduchú verziu systému demonštrujúcu funkčnosť protokolu, pretože počítala s integráciou s externými službami. Druhým bolo dlhé, náročné a podrobné skúmanie možností súčasnej platformy v implementácii funkcionalít ako je aritemtika veľkých čísel, kryptograficky bezpečné zdroje náhody či RSA šifrovanie. Čas bol strávený najmä porovnávaním existujúcich riešení, a odhaľovaním zle zdokumentovaného chovania.

Vo všeobecnosti možno tvrdiť, že aj keď webová platforma ešte nie je úplne pripravená na kryptografické aplikácie, pomerne rýchlo sa k tomu blíži. Špecifikuje sa celý nový modul *Crypto*, ktorý poskytne všetky štandardné kryptografické konštrukcie. Pre

náš protokol je taktiež dôležitá aritmetika veľkých čísel, nakoľko ElGamal šifrovanie treba implementovať osobitne. Tá však v súčastnosti nie je natívne podporovaná a teda musí byť vykonávaná pomalým, emulovaným spôsobom. Toto by bol pravdepodobne najväčší výkonnostný problém pri dokončenej aplikácii.

Aj keď je súčasný kód nekompletný, autor mu venoval veľké množstvo času a intelektuálneho úsila, dodržiavajúc najlepšie vývojové praktiky v konkrétnych technologických oblastiach. Súčasný stav kódu považuje za veľmi dobrý a pripravený na nadviazanie.

Záver

V práci sme podrobne spracovali tému hlasovaní v malých skupinách ľudí. Prešli sme kompletným procesom, od rozboru reálnych situácií, cez modelovú situáciu, návrh a formalizáciu protokolu až k pokusu o implementáciu. Využili sme jednak existujúce konštrukcie, ktoré však skombinovali s vlastnými riešeniami, miestami teoreticky zaujímavými, a dospeli sme k návrhu, ktorý je pripravený na implementáciu, prípadne pokračovanie v existujúcej implementácii.

Pri rozbore sme zobrali do úvahy všetky dôležité požiadavky zo zadania a pokúsili sa pokryť čo najširšie spektrum hlasovacích situácií pri súčasnom zachovaní kompaktnej a dobre definovateľnej modelovej situácie. Vzali sme tiež do úvahy ústupky voči aktuálnemu trendu, najmä v oblasti nedokázateľnosti hlasovania.

Podrobne sme sa venovali dôležitým návrhovým rozhodnutiam, najmä pri redukcii autorít a hlasovaní bez zariadenia. Okrem finálneho najlepšieho riešenia sme spomenuli niekoľko ďalších, skorších riešení, ktorých myšlienky môžu byť použité pri riešení podobných problémov. Za spomenutie napríklad stojí permutácia kandidátov, ktorá sa zverejní až po odhlasovaní, ako aj dvojité hlasovanie a následné zverejnenie jedného z hlasov. V kapitole sme tiež uviedli niekoľko možných konštrukcií, ktoré dokážu protokol ďalej zefektívniť (napr. kalkulátor).

Možno tvrdiť, že hlavný problém, hlasovanie bez vlastného zariadenia, sme vyriešili hneď dvoma spôsobmi. Dostatočne bezpečným, ale koordinačne komplikovaným rozdávaním čiastočných informácií iným účastníkom hlasovania, ako aj pohodlným použitím prešifrovacej autority, dôvernosť ktorej je upravená právne. Hlasujúci sa teda môže sám rozhodnúť medzi dôvernosťou, pohodlnosťou a dôverou v autoritu.

V ďalšej časti sa pokúšame o formalizáciu protokolu. Nami navrhnutý originálny prístup nám umožňuje štruktúrovanejším spôsobom overiť naše tvrdenia o protokole ako aj poskytuje detailný prepis protokolu vhodný pre implementáciu. O tú sme sa pokúsili, pričom sme sa dopracovali k stručnej, ale premyslenej architektúre, čiastočnému kódu a zisteniu, že webová platforma nie je na kryptografické programovanie ešte úplne pripravená.

Keďže hlasovania malého rozsahu sú relatívne nepreskúmané, možností, ako nadviazať na túto prácu, je veľa. Jednou z možností je vychádzať z rovnakých modelových

situácií a pokúsiť sa navrhnúť alternatívny hlasovací protokol, ktorý bude následne porovnateľný s našim. Protokol samotný má tiež priestor na rozširovanie, napríklad cestou k nedokladovateľnosti alebo k vpisovaniu kandidátov. Asi najpriamočiarejšia možnosť, viac praktická, ako vedecká, je pokračovať v samotnej implementácii.

Hlavnú časť zadania, návrh a teoretické zdôvodnenie volebného systému, sa nám podarilo splniť spolu s množstvom ďalších zaujímavých výsledkov a preto, aj napriek nedokončenej implementácii, možno prácu považovať za úspešnú.

Literatúra

[1] Ben Adida. Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335–348, 2008.

[2] Josh Benaloh. Simple verifiable elections. *EVT*, 6:5–5, 2006.

[3] Josh Daniel Cohen Benaloh. Verifiable secret-ballot elections. 1987.

[4] David Bernhard and Bogdan Warinschi. Cryptographic voting—a gentle introduction. In *Foundations of Security Analysis and Design VII*, pages 167–211. Springer, 2014.

[5] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak sponge function family main document. *Submission to NIST (Round 2)*, 3:30, 2009.

[6] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In *Annual International Cryptology Conference*, pages 89–105. Springer, 1992.

[7] Josh D Cohen and Michael J Fischer. *A robust and verifiable cryptographically secure election scheme*. Yale University. Department of Computer Science, 1985.

[8] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Annual International Cryptology Conference*, pages 174–187. Springer, 1994.

[9] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. *Transactions on Emerging Telecommunications Technologies*, 8(5):481–490, 1997.

[10] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[11] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[12] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

[13] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In *Advances in Cryptology—AUSCRYPT'92*, pages 244–251. Springer, 1993.

[14] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[15] Emmanouil Magkos, Mike Burmester, and Vassilis Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In *Towards The E-Society*, pages 683–693. Springer, 2002.

[16] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[17] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme. In *Advances in Cryptology—EUROCRYPT'95*, pages 393–403. Springer, 1995.

[18] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174, 1991.

Príloha A: Architektúra systému Nestvoting

Systém Nestvoting je pokus o implementáciu protokolu navrhnutého v tejto práci. Jeho aktuálne zdrojové kódy sú zverejnené na adrese `https://github.com/syslo/nestvoting`. Keďže systém nie je dokončený, táto príloha dokumentuje návrh finálnej podoby projektu, ktorá si prešla niekoľkými iteráciami úprav.

Komponenty

špecifikácia skupiny

Každá hlasovacia skupina má svoje vlastné pravidlá. Tieto informácie sú súčasťou jednoduchého konfiguračného súboru s názvom špecifikácia skupiny. Skupina je jednoznačne identifikovaná pomocou URL, na ktorej je zverejnená, a autenticita informácií je zabezpečená pomocou SSL. Obsahuje:

- používanú nástenku – URL a verejný kľúč
- možnosti autentifikácie a dáta k nim prislúchajúce (napríklad URL a verejný kľúč autoritatívneho autentifikátora)
- názov, maximálny počet členov, zákaz hlasovania bez zariadenia, ...

aplikácia

Najkritickejšia časť systému, vykonáva protokol v mene hlasujúceho. Je preto dôležité aby bola štandardizovaná, podpísaná a nebolo nutné ju modifikovať. Dostupná môže byť z mnohých zdrojov, užívateľ by mal byť schopný jednoducho verifikovať je pravosť. Rôzne zdroje môžu mať iné konfiguračné súbory, tie však nesmú ovplyvniť priebeh hlasovania. Je to webová aplikácia, ktorá však beží a všetky informácie si ukladá lokálne.

Keďže môže obsluhovať viacero špecifikácií skupín a hlasovaní v nich, musí obsahovať históriu a manažment týchto entít. Možnosti manažmentu vedia byť konfiguro-

vateľné. Tiež by malo byť jednoduché vytvoriť odkaz, ktorý otvorí priamo konkrétnu obrazovku aplikácie, prípadne hlasovanie.

Počas hlasovania by mala byť aplikácia čo najviac nápomocná, môže zobrazovať aktuálny stav procesu, účastníkov, na ktorých sa momentálne čaká, prípadne nápovedu k riešeniu vzniknutých problémov.

nástenka

Dostupný server, ktorý je pomerne ľahko, ideálne aj automaticky škálovateľný. Umožňuje vytvárať hlasovania pre rôzne špecifikácie skupín a pridávať do nich správy a následne ich zverejní pre celý svet. Bonusom môže byť možnosť verejných hlasovaní pre ľahšie pripojenie sa alebo aspoň čiastočná kontrola korektnosti správ.

autentifikátor

Jedna z možností autentifikácie. Server, ktorého adresa aj identifikácia sa nachádzajú v špecifikácii skupiny. Aplikácia presmeruje účastníka spolu s jeho vygenerovaným dočasným verejným podpisovým kľúčom na stránku autentifikátora. Účastník vykoná autentifikačný úkon, autentifikátor ho overí a v prípade úspechu o tom zverejní na nástenke správu. Tým sa zvaliduje účastníkov verejný podpisový kľúč.

Konštrukcie a Technológie

stavový automat pre protokol

Na protokol možno nahliadať ako na stavový automat, ktorý postupne spracováva správy či udalosti (užívateľ zahlasoval) a občas generuje nové. Stav je však pomerne komplikovaný objekt. Okrem fázy hlasovania, môže obsahovať aj súkromné kľúče, globálne hodnoty získané z protokolu, jednotlivé správy či vypočítané pomocné dáta. Týmto oddelíme logiku protokolu od riadiacej logiky aplikácie, užívateľského rozhrania či detailov sieťovej komunikácie.

Clojure

Clojure je funkcionálny programovací jazyk z rodiny LISP, ktorý je možné kompilovať do Javy ako aj do JavaScriptu. Webovú platformu môžeme využiť na aplikáciu, Javu zase na servery. Platformovo závislý kód je možné pre jednotlivé jazyky oddeliť. Vo funkcionálnom kóde sa lepšie argumentuje o správnosti a vďaka perfektnému systému makier nám navyše umožní navrhnúť prehľadný deklaratívny zápis samotného protokolu. Najmä kvôli týmto skutočnostiam bol Clojure zvolený za hlavný jazyk projektu.

knižnica

Protokol a funkcie operujúce nad rozhraním jednotlivých komponentov by mali byť súčasťou štandardnej knižnice, ktorá umožní záujemcom implementovať nástenky s vlastnou logikou kontroly, vlastné autorizátory či aplikácie slúžiace na rozbor hlasovaní. Aj keď by to nemal byť primárny cieľ, je dobré na to pri implementácii myslieť.