Volilne sheme

Janez Starc

17.3.2010

1 Uvod

Skozi leta so se volitve organizirale na različne načine. V večini primerov se danes glasove oddajajo na papirju. Ker pa bi radi čim bolj avtomatizirali volitve in pri tem ne bi izgubili na varnosti so se pojavile drugačne oblike volitev. Ponekod uporabljajo (na samem volišču) elektronske naprave ali pa volilci luknjajo kartice in tako oddajo svojo glasovnico. To omogoča hitrejše in bolj zanesljivo štetje.

Danes je Internet že tako močno razvit, da se je pojavila možnost, glasovanja preko Interneta. Številni volilci bi volili veliko bolj pogosto, če bi imeli možnost voliti kjerkoli že so; še posebej tisti, ki so med volitvami v tujini. Poleg tega bi bile take volitve cenejše, hitrejše in udobnejše. Zato bi volitve lahko izvedli pogosteje. Državljani, občani, člani društva, oziroma volilni upravičenci bolj aktivno sodelovali pri odločitvah. To bi pripomoglo k demokratizaciji ustanove v kateri potekajo volitve.

Vendar ima uporaba informacijske tehnologije za izvedbo volitev tudi slabosti. Predvsem je težko stoodstotno zagotoviti varnost na takšnih volitvah. Kajti računalniki volilcev so lahko nezaščiteni oziroma okuženi. Tako bi lahko nepridipravi vdrli v tak računalnik in onemogočili volilcu, da voli oziroma sami oddali svoj glasovnico. Že na tradicionalnih prihaja do napak in poneverb. Z uporabo Interneta pa bi lahko prišlo do prevare na najvišji ravni, ki bi jo lahko zagrešil že en heker. Lahko bi povzročil, da bi se izugubile vse glasovnice, ali pa bi lahko celo tako priredil rezultatate, da bi zmagala njegova odločitev. Prak tako bi lahko hrošč v programski kodi programa za volitve popolnoma pokvaril volitve. Zato je treba biti še posebej previden pri načrtovanju takih volitev. Uporaba kriptografije je zato bistvena za izvedbo elektronskih volitev.

2 Model volitev

Elektronske volitve morajo potekati podobno kot tradicionalne volitve na papirju. Volilna komisija skrbi za pošteno izvedbo volitev. Najprej zbere podatke o volilnih upravičencih in jih obvesti o volitvah. Preden volilec lahko glasuje, ga volilna komisija najprej identificira. Nato sme voliti samo enkrat in to v tajnosti. Ko se čas za oddajanje glasovnic izteče, volilna komisija prešteje glasovnice in objavi rezultate volitev.

Udeleženci na volitvah so volilci in volilne komisije (če pa govorimo o posameznikih so to člani volilne komisije). V našem modelu si jih predstavljamo kot deterministične Turingove stroje. Torej v zglednem času ne morejo rešiti problem diskretnega logaritma, razcepiti veliko praštevilo na prafaktorje, rešiti NP-poln problem, itd. Volilci želijo volilni postopek opraviti čim hitreje, zato naj bo postopek oddaje glasovnic čim preprostejši. Poleg tega naj volilec opravlja čim manj računanja. Volilec se lahko vzdrži glasovanja, če želi. Predpostavljamo tudi, da si lahko spravi neko informacijo na varno mesto, ki je znana samo njemu. Volilna komisija pa ima na voljo veliko računske moči in veliko prostora, kjer lahko varno spravijo podatke.

2.1 Tipi glasovanja

Glaosovi so lahko različnih, tipov odvisno od vprašanja. Poznamo:

- Za/proti glasovanje. Volilčev glas je za določeno trditev oziroma proti. Za glasovanje je potreben samo en bit: 1 - za in 0 - proti.
- $1 - L$ glasovanje. Tukaj ima volilec L možnosti na izbiro in izbere natanko eno. Oddan glas je številka med 1 in L. Primer: Volitve za predsednika, kjer izbiramo enega izmed L kandidatov
- $K - L$ glasovanje. Volilec izbere k elementov iz množice L možnosti. Vrstni red možnosti ni pomemben. Oddan glas je K-terka $(v_1, \ldots, v_K)$.
- $K - L$ urejeno glasovanje. Podobno je kot $K - L$ glasovanje, le da je oddan glas urejena K-terka $(v_1, \ldots, v_k)$. V tem primeru ponavadi kandidat na prvem mestu dobi največ točk. Kandidat na zadnjem mestu pa najmanj točk.
- $1 - K - L$ glasovanje. Volilec izbere eno množico izmed danih. Nato iz te možnosti izbere K elementov. Glas je $K + 1$-terka $(i, a_1, \ldots, a_k)$, kjer so $a_1, \ldots, a_k$ elementi i-te množice. Primer: ko najprej izbiramo neko listo (stranko), nato pa še kandidate iz te liste.

- tekstovno glasovanje. Volilec sam sestavi odgovor in ga napiše. Glas je niz z omejeno maksimalno dolžino.

V resničnem svetu je zelo tvegano zaupati volitve samo eni osebi, kajti ta oseba lahko z lahkoto zlorabi svoj položaj in poneveri rezultate. Zato volitve raje zaupamo skupini ljudi, ki težje poneverijo volitve. V našem primeru bomo predpostavljali, da organizira volitve N članov volilne komisije. Od tega pa jih je največ T nepoštenih, ki bi želeli spremeniti dejanski izid volitev.

2.2 Komunikacijski elementi

Nekatere sheme zahtevajo posebne komunikacijske elemente za izvedbo volitev:

- **Elektronska oglasna deska** (bulletin board) je javna oglasna deska, kjer ima vsak udeleženec možnost objaviti kar želi. Vsak lahko to prebere. Nobeden pa ne more tega spremeniti oziroma izbrisati. Na elektronsko oglasno desko lahko gledamo, kot na javni kanal s spominom.

- **Zasebni kanali** so kanali po katerih si lahko dva udeleženca pošiljata skrivno informacijo, tako da nobena druga oseba ne more prisluškovati kanalu. Torej nobeden ne more videti, oziroma spremeniti informacije, ki gre po kanalu. Tega se ne da implementirati s kriptografskimi tehnikami.

- **Anonimni kanali** (anonymous channel) so kanali, ki zagotavljajo anonimnost pošiljatelja. Torej prejemnik sporčila ne ve, kdo pošilja sporočilo in nihče ne more povezati nekega udeleženca s sporočilom. Tak kanal je lahko javen in se ga lahko kriptografsko implementira [1].

2.3 Faze volilnega procesa

Volilni proces je razdeljen na več različnih faz:

- **Inicializacija.** Kriptografski ključi in različni sistemski parametri so zgenerirani.

- **Registracija.** Volilni upravičenci prejmejo zasebne ključe na varen način in so registrirani ter dodani na listo vseh volilcev.

- **Glasovanje.** Volilci pošljejo glasovnice uradnikom.

- **Preštevanje glasov.** Uradniki izračunajo (preštejejo) glasovnice po volilnem protokolu.

- **Preverjanje.** Volilna komisija preveri, če so vse faze potekale po protokolu, če so glasovi pravilno prešteti, itd. Ta postopek lahko poteka vzporedno z volitvami. Preverja se lahko tudi še po tem, ko so rezultati že objavljeni.

2.4 Zahteve volilnih shem

Volilna shema mora izpolnjevati čim več zahtev, da bi jo lahko uporabili v praksi. V tem razdelku so naštete nekatere od teh zahtev:

- **Upravičenost.** Volilne upravičence mora volilna komisija registrirati in identificirati. Samo oni lahko oddajo glasove. Nobeden ne more glasovati dvakrat.

- **Zasebnost.** Nobeni skupini udeležencev (tudi volilni komisiji), ki ne vsebuje volilca samega, ne sme biti znana nobena informacija o povezavi med volicem in njegovo glasovnico, tudi če opazujejo vso komunikacijo med volilcem in komisijo. To se lahko doseže na 3 načine:

  - Preprosto je videti glasovnico, ampak jo je nemogoče povezati z volilcem.
  - Nemogoče ali vsaj računsko prezahtevno je videti glasovnico, vendar je preprosto identificirati volilca.
  - Videti glasovnico, kot tudi identificirati volilca, je oboje nemogoče oziroma računsko prezahtevno

- **Invidualna preverljivost.** Vsak volilec lahko preveri, če je bil njegov glas res upoštevan.

- **Univerzalna preverljivost.** Vsak udeleženec ali pasivni opazovalec lahko preveri, če so bile volitve poštene. Lahko tudi sam prešteje glasove.

- **Poštenost.** Noben udeleženec ne more izvedeti nobene informacije o (delnem) izidu preden se glasovanje ne konča, ker bi lahko s temi informacijami vplival na tiste, ki še niso glasovali.

- **Robustnost.** Napačno obnašanje neke zmerno velike skupine se lahko tolerira. Torej takšno združenje ne more pokvariti volitev. Vsakega goljufa pa se takoj odkrije.

- **Časovna zahtevnost.** Shema ne sme biti preveč časovno zahtevna; v tem smislu, da ne ovira volilca, da hitro odda svoj glas. Volilna komisija pa ne sme predolgo izračunavati rezultatov.

Nekatere volilne sheme imajo močnejše oblike zasebnosti, kot je:

- **Nedokazljivost.** Volilec ne more na noben način nikomur dokazati, da je volil na določen način. Tako se prepreči, da bi volilec glasoval, kakor mu je nekdo zaukazal. Niti ne more prodati svojega glasu, ker kupcu glasu ne more dokazati, da je v resnici glasoval, kakor mu je kupec zaukazal. Ponavadi lahko volilec kupovalcu glasov izda nekatere varnostne parametre. Ta pa lahko s temi preveri, kako je volilec glasoval; na enak način kot volilec preveri, če je njegov glas upoštevan. Če je shema nedokazljiva teh varnostnih parametrov ni.

Vendar so volilci še vedno lahko prisiljeni, da ne oddajo svoje glasovnice, ali pa, da kdo glasuje namesto njih. Še močnejša zahteva, ki prepreči take napade je:

- **Odpornost proti prisiljevanju.** Shema je odporna proti prisiljevanju, če lahko dopustimo, da napadalec prisili volilca, da glasuje na zahtevan način, da se vzdrži glasovanja, ali da mu celo izda svoje zasebne ključe. Kljub temu pa se napadalec nikakor ne more prepričati, če je volilec, res naredil stroril, kar mu je ukazal.

Ena od od najbolj zahtevnih lastnosti volilne sheme je zasebnost. Če ne bi zahtevali zasebnosti, ne bi bilo težko skonstruirati volilno shemo z ostalimi lastnostmi (upravičenost, invidualna preverljivost,...). (Seveda če ne zahtevamo zasebnosti prav tako ne moremo zahtevati nedokazljivost, odpornost proti priseljevanju). Shema brez zasebnosti je zelo preprosta: vsak volilec bi svoj glas zapisal na svoj del elektronske oglasne deske. Tako bi vsak lahko prebral njegov glas in seštel vse glasove.

Do sedaj je znanih malo načinov za zagotavljane zasebnosti, kajti vsaka informacija o povezavi med volicem in njegovim glasom mora biti nedostopna vsem (tudi volilni komisiji), če tudi spremljajo vso komunikacijo, ki teče po javnih kanalih. Eden od načinov dovoljuje, da lahko vidimo, kako je nekdo glasoval, ampak ne moremo vedeti kdo je to bil. Za ta način potrebujemo anonimni kanal. Pri drugem načinu pa je nemogoče ali vsaj računsko pretežko videti, kako je nekdo dejansko glasoval, vendar pa vemo kdo je oddal to (zakodirano) glasovnico.

3 Kriptografski pripomočki

V tem razdelku so predstavljeni kriftografski pripomočki, na katerih temeljijo sheme prikazane v naslednjem poglavju.

3.1 Javno preverljiva shema za deljenje skrivnosti

Javno preverljiva shema za deljenje skrivnosti je shema za deljenje skrivnosti, ki omogča preverjanje, ali je, tisti ki deli skrivnost - delilec, pravilno razdelil dele med prejemnike (katerakoli množica $t+1$ prejemnikov bo prejela isto skrivnost). Omogoča tudi, da se ugotovi ali je kateri od prejemnikov (članov volilne komisije) poneveril svoj del. Ta shema je del Schoenmakerjeve sheme [3].

Začetek. Izbere se grupo Z_p in generatorja G, g. Prejemnik A_j izbere svoj zasebni ključ z_j in objavi svoj javni ključ $h_j = g^{z_j}$. Delilec želi deliti deliti skrivnost g^s med prejemnike.

Razdelitev posameznih delov. Delilec izbere naključni polinom stopnje t v Z_p:

$$p(x) = \sum_{k=0}^{t-1} \alpha_k x^k$$

kjer $\alpha_0 = s$ in $\alpha_1, \ldots, \alpha_t \in Z_p$. Delilec objavi $C_k = G^{\alpha_k}$, $0 \leq k \leq t$, kot tudi zašifrirane dele $H_j = h_j^{p(j)}$, $j = 1, 2, \ldots N$. Polinom pa ostane tajen. Delilec dokaže, da so zašifrirani deli konsistenti: Naj bo $X_j = \prod_{k=0}^{t} C_k^{j^k} = G^{\sum_{k=0}^{t} \alpha_k j^k} = G^{p(j)}$, delilec z uporabo neinteraktivnga dokaza iz razdelka 3.3.1 dokaže, da:

$$\log_G X_j = \log_{h_j} H_j$$

za vsak $j = 1, 2, \ldots, N$

Rekonstrukcija rešitve. Prejemnik A_j odšifrira svoj del $S_j = g^{p(j)}$ tako da izračuna $S_j = H_j^{1/z_j}$. A_j prav tako dokaže, da $\log_G X_j = -\log_{H_j} S_j$ (spet s pomočjo dokaza iz razdelka 3.3.1). Predpostvimo, da je $t+1$ prejemnikom A_j, $j \in A$ uspelo pridobiti pravilne vrednosti S_j, $j \in A$. Skrivnost je g^s rekonstruirana z Langragevo interpolacijo

$$\prod_{j \in A} S_j^{\lambda_{j,A}} = \prod_{j \in A} g^{p(j)\lambda_{j,A}} = g^{\sum_{j \in A} p(j)\lambda_{j,A}} = g^{p(0)} = g^s$$

kjer so $\lambda_{j,A} = \prod_{l \in A - \{l\}} \frac{l}{l-j}$ Lagrangevi koeficienti.

3.2 Homomorfno šifriranje

Naj bo P prostor čistopisov in C prostor zašifriranih besedil, tako da je P grupa nad operacijo $\oplus$ in C grupa nad operacijo $\otimes$. Naj bo E primer verjetnostnega kriptosistem, ki je določen z javnim in zasebnim ključem. Naj bo $E_r(m)$ zašifrirano sporočilo, r pa naključni parameter primera E (r je naključnost uporabljena pri šifriranju).

Verjetnostni kriptosistema je $(\oplus, \otimes) - homomorfen$, če za vsak primer E kriptosistema velja, da za $c_1 = E_{r1}(m1)$ in $c_2 = E_{r2}(m2)$ obstaja r, tako da

$$c_1 \otimes c_2 = E_r(m1 \oplus m2)$$

Naprimer, ElGamalov kriptosistem je homomorfen. Tukaj vzamememo za $P = Z_p$ in za C je množico parov $C = \{(a, b)|a, b \in Z_p\}$. Operacija $\oplus$ je množenje po modulu p. Za binarno operacijo $\otimes$ pa lahko vzamemo množenje po modulu p po komponentah. Dva čistopisa m_0, m_1 sta zašifrirana v

$$\begin{aligned} E_{k_0}(m_0) &= (g^{k_0}, h^{k_0} m_0) \\ E_{k_1}(m_1) &= (g^{k_1}, h^{k_1} m_1) \end{aligned}$$

kjer sta k_0 in k_1 naključna.

Velja

$$E_{k_0}(m_0)E_{k_1}(m_1) = (g^{k_0}g^{k_1}, h^{k_0}h^{k_1}m_0m_1) = (g^k, h^k m_0 m_1) = E_k(m_0m_1)$$

za $k = k_0 + k_1$.

Torej v ElGamalovem kriptosistemu dobimo zmnožek dveh zašifriranih sporočil, če zmnožimo ti dve sporočili in jih zašifriramo.

3.3 Interaktivni dokazi

V tem poglavju so predstavljeni interaktivni dokazi, ki se jih uporablja v volilnih shemah. Ti dokazi temeljjo na problem ElGamalovem kriptosistemu. Podobni dokazi obstajajo za ostale kriptosisteme.

3.3.1 Enakost diskretnih logaritmov

V tem razdelku je predstavljen protokol, ki pokaže enakost dveh diskretnih logaritmov. Tisti, ki dokazuje (poimenujmo ga David) ima četvorko (g, h, x, y), $g, h, x, y \in Z_p$ in mora dokazati, da pozna $\alpha \in Z_p$, tako da velja: $x = g^\alpha$ in $y = h^\alpha$. Varnostne lastnosti so predstavljene v [4].

David najprej izbere $w \in Z_p$ in izračuna $a = g^w$ in $b = h^w$ ter jih pošlje prejemniku (poimenujmo ga Peter). Nato Peter izbere izziv $c \in Z_p$ in ga

pošlje nazaj Davidu. Ta izračuna $r = w + \alpha c$ in pošlje r Petru. Sedaj Peter preveri ali velja $g^r = ax^c$ in $h^r = by^c$. Če enakosti veljata, je David dokazal Petru, da $\log_g x = \log_h y$ in da pozna α.

Za naključna c, r lahko David ukane Petra, tako da pošlje $a = g^r x^{-c}$ in $b = h^r y^{-c}$. Vendar pošlje David prej a in b, kot Peter c. In če David ne pozna α, ne more poslati takega r-ja, da bi ukanil Petra.

Ne-interaktivna verzija. Z manjšo modifikacijo, lahko zgornji dokaz spremenimo v ne-interaktivnega. David ponovi vse izračune, le da si c izračuna sam: $c = H(a||b||x||y)$, kjer je H varna zgoščevalna funkcija. David shrani kot del dokaza tudi c in r. Peter nato preveri če David res pozna α, tako da izračuna, če velja $c = H(g^r x^{-c}||h^r y^{-c}||x||y)$

3.3.2 Dokaz ponovnega šifriranja

Tisti, ki dokazuje (David), mora dokazati tistemu, ki preverja (Peter), da je eden izmed zašifriranih sporočil $(x_1, y_1), (x_2, y_2), \ldots, (x_L, y_L)$ ponovno zašifrirano sporočilo (x, y). Sporočilo m je zašifrirano z ElGamalovim kriptosistemom, da dobimo (x, y). Vzamimo, da je (x_t, y_t) ponovo šifriranje (x, y), tako da $(x_t, y_t) = (xg^v, yh^v)$.

Protokol

1. David naključno izbere vektorja $d = (d_1, \ldots, d_L)$, r= $(r_1, \ldots, r_L)$ naključnih števil $d_i, r_i \in Z_p, i = 1, \ldots, L$

2. David izračuna $w = vd_t + r_t$

3. David izračuna vektorja $a = (a_1, \ldots, a_L), b = (b_1, \ldots, b_L)$ in jih pošlje Petru:
$$\begin{aligned} a_i &= (\tfrac{x_i}{x})^{d_i} g^{r_i} \\ b_i &= (\tfrac{y_i}{y})^{d_i} h^{r_i} \end{aligned}$$

4. Peter mu odgovori z naključnim izzivom $c \in Z_p$

5. David ponovno izračuna
$$\begin{aligned} d_t &= c - \textstyle\sum_{j \neq t} d_j \\ r_t &= w - vd_t \end{aligned}$$
in pošlje spremenjena vektorja d in r Petru

6. Peter preveri, če velja

$$\begin{aligned} c &= d_1 + \ldots + d_L \\ a_i &= (\tfrac{x_i}{x})^{d_i} g^{r_i} \\ b_i &= (\tfrac{y_i}{y})^{d_i} h^{r_i} \end{aligned}$$

Če zgornje enakosti veljajo, potem je David uspešno izvedel dokaz. Potem ko David pošlje vrednosti a_i, b_i Petru, ne more več spreminjati vrednosti d_i in r_i za vse $i = 1, \ldots, L$ razen za $i = t$. Vrednosti a_t in b_t prisilijo Davida, da ne more spreminjati vrednosti $w = vd_t + r_t$, kajti $a_t = g^{vd_t + r_t}$ in $b_t = h^{vd_t + r_t}$. Ker David pozna v, lahko še zmeraj spremeni d_t in r_t. Zato pa mu Peter pošlje izziv c, tako da bo vsota elementov vektorja d ravno to naključno število c. Pravzaprav David nastavi vrednosti d_t in r_t, tako da zadoščajo zahtevam ($c = d_1 + \ldots + d_L$ in $w = vd_t + r_t$). Ta zmožnost Davida prepriča Petra, da je eden izmed L zašifriranih parov zares ponovno šifriranje (x, y). Drugače ne bi mogel prilagoditi vrednosti d_t, r_t vsoti c. Dokaz preprosto spremenimo v neiteraktivenga (podobno kot v prejšnem dokazu), tako da si David s pomočjo zgoščevalne funkcije sam izračuna c.

3.3.3 L možnosti diskretnega logaritma

Za zašifrirano sporočilo $(x, y) = E(m)$ (v ElGamalovem kriptosistemu), skušamo dokazati, da je m eden izmed L možnih sporočil $G_1, \ldots, G_L$. Pri tem ne želimo razkriti ničesar o sporočilu m, razen tega, da pripada množici $G = \{G_1, \ldots, G_L\}$. Predpostavljamo, da ne poznamo diskretnih logaritmov (z bazama g in h) elementov iz G. Cilj je dokazati da velja:

$$\log_g x = \log_h(y/G_1) \vee \log_g x = \log_h(y/G_2) \vee \ldots \vee \log_g x = \log_h(y/G_L)$$

Dovolj je že, da dokažemo, da je eden izmed

$$\begin{aligned} (x_1, y_1) &= (x, y/G_1) \\ (x_2, y_2) &= (x, y/G_2) \\ &\vdots \\ (x_L, y_L) &= (x, y/G_L) \end{aligned}$$

ponovno šifriranje $(1, 1)$. To lahko dokžemo s pomočjo dokaza iz prejšnega razdelka.

4 Volilne sheme

V tem razdelku so opisane tri vrste različnih volilnih shem. Vsaka vrsta ima nekatere zaželene zahteve, ki jih druga nima. Nato so opisani modeli konkretnih shem.

4.1 Sheme z anonimnim kanalom

V fazi registracije volilec dobi žeton, ki mu daje pravico, da voli v volilni fazi. Volilec ne more sam izdelati žetona, ampak samo v sodelovanju z volilno komisijo. Ta pomaga volilcu izdelati žeton samo enkrat (volilec lahko dobi samo en žeton), vendar na koncu ne vedo, kako ta žeton izgleda. Vsak pa lahko preveri, če je žeton veljaven. To se omogoči z slepimi podpisi. V volilni fazi volilec odda glasovnico, ki vsebuje žeton in njegovo odločitev preko anonimnega kanala volilni komisiji. Tipa ne bodo sprejeli neveljavnega ali že uporabljenega žetona. To zagotavlja, da lahko volijo, samo tisti, ki so upravičeni do tega in to največ enkrat. Vsak volilec mora imeti drugačen žeton. Žeton je lahko sestavljen iz česarkoli: skrite volilčeve identitete(npr. hash vrednost), naključnih številk, zakodiranega glasu, oznake volitev, itd. Edina omejitev je, da naj bi bilo težko, oziroma nemogoče izvedeti iz žetona karkoli o volilčevi identiteti. Nobeden ne more ugotoviti povezave med volilcem in njegovo odločitvijo, ker gre glasovnica po anonimnem kanalu in se iz žetona ne da razbrati voličeve identite. S tem je dosežena zasebnost.

4.2 Sheme z homomorfnim šifriranjem

Pri teh shemah, volilec pošlje zašifriran glasovnico po javnem kanalu, ponavadi na elektronsko oglasno desko. Glasovnico lahko odšifrira katerakoli množica, v kateri je vsaj $t + 1$ uradnikov. Nobena množica, ki pa vsebuje t ali manj uradnikov pa ne more odšifrirati glasovnice. To se naredi na dva načina:

- pragovni javni kriptosistem se uporabi za šifriranje glasovnic (ključ za odšifriranje si deli katerakoli množica $t + 1$ uradnikov). Tak sistem je naprimer ElGamalov kriptosistem.
- vsak uradnik ima svoj lasten kriptosistem. Volilec deli skrivnost (glasovnico) med N uradniki z uporabo $(t + 1, N)$ sheme za deljenje skrivnosti (npr. Shamirjeva shema). Volilec pošlje vsakemu uradniku samo del skrivnosti (glasovnice).

To prepreči majhni skupini uradnikov, da bi zlorabila svoj položaj in tako kršila predpostavko o zasebnosti volilca. Šifrirana metoda za šifriranje glasov

je homomorfna: zmnožek zašifrinih glasov je enak zašifrirani vsoti glasov. V primeru pragovnega javnega kriptosistema se zašifrirani glasovi zmnoži. Volilna komisija odšifrira ta zmnožek in tako dobi izid volitev. V drugem primeru pa vsak član volilne komisije zmnoži zašfrirane dele. Končna vsota pa se lahko izračuna, s pomočjo $t+1$ delnih vsot članov volilne komisije.

Kadar se uporablja za/proti glasovanje (kjer pomeni 1 glas za in 0 glas proti) je stvar preprosta, kajti skupna vsota je enaka številu volilcev, ki so glasovali da. Ker poznamo število vseh volicev, ki so glasovali, lahko hitro ugotovimo število volilcev ki so glasovali proti. Za ostale tipe glasovanj pa moramo biti nekoliko bolj iznajdljivi. Naprimer pri $1-L$ glasovanju, zakodiramo i-to možnost ($1 \leq i \leq L$) kot M^{i-1} (kjer je M število vseh volilcev, ki so glasovali). Vsota vseh glasov bo $S_1 = a_1 + a_2 M + a_3 M^2 \ldots + a_L M^{L-1}$, kjer je a_i število volilcev, ki so izbrali i-to možnost. Koeficiente a_i je možno iterativno izračunat: $a_i = S_i \pmod M, S_{i+1} = (S_i - a_i)/M$, kjer je S_1 vsota vseh glasov. Volilna komisija naj bo sposobna ločiti med veljavnimi in neveljavnimi glasovi in izločiti neveljavne. Kajti en neveljaven glas popolnoma spremeni izid glasovanja. Od volilca se zahteva, da dokaže ali je njegov glas v pravilni obliki (npr. 0 ali 1), ne da bi razkril kako je glasoval. To naredi s pomočjo dokaza brez razkritja znanja.

Ponavadi sheme z homomorfnim šifriranjem niso nedokazljive: Naprimer, da je voličev glas V in zašifriran glas je C. Potem volilec pošlje V na elektronsko oglasno desko, torej C vsi poznajo. Denimo, da je napadalec zahteva od volilca, da izbere W, ki ni enak V. Napadalec lahko kasneje zahteva od volilca, da mu pokaže, kako je zakodiral W v C. To pa volilec ponavadi ne more narediti. Zato take sheme ponavadi niso nedokazljive.

4.3 Sheme z mešanjem glasov

.

Če vzamemo naprimer $1-L$ glasovanje. Volilna komisija vzame seznam, na katerem je vseh L možnosti in ga premeša in s tem ustvarijo končni seznam. To naredijo na naslednji način:

Prvi uradnik vzame seznam ga naključno premeša in zašifrira vsak glas posebej. Kako je premešal glasove pokaže samo volilcu in nikomur drugemu. Zaradi varnosti uradnik pošlje permutacijo volilcu preko varnega kanala. Ustvarjen seznam, ki vsebuje ponovno šifrirane in premešane glasove je objavljen in predan naslednjemu članu. Če nekdo vidi originalen in nov seznam, ne more vedeti na kakšen način so glasovi premešani, razen če mu te permutacije ne zaupa ta član volilne komisije. Nato seznam prevzame naslednji član in ponovno naključno premeša, ponovno zašifrira glasove, pokaže permutacijo volilcu in objavi seznam. To se zaporedoma dela dokler zadnji uradnik ne

objavi končnega seznama. Samo volilec ve na katerem mestu na končnem seznamu je vsak element iz originalnega seznama. Volilec iz končnega seznama preprosto izbere svoj glas in ga napiše na elektronsko oglasno desko. Če je uporabljeno homomorfno šifriranje, potem se glasovi zmnožijo. Uradniki pa potem skupaj dešifrirajo zmnožek, da dobijo skupno vsoto glasov. Ker napadalec ne more prisluškovati varnemu kanalu, se lahko volilec napadalcu zmisli kakšna je bila permutacija začetnega seznama, tako da ugodi napadalcu. Zato volilec ne more dokazati, kako je volil. Take sheme so nedokazljive.

4.4 Radwinova shema

Ta shema je bila napisana v [2]. V tej shemi potrebujemo samo enega člana volilne komisije, ki lahko opravlja vsa dela (registracija, štetje). Seveda je bolje če imamo več članov volilne komisije, kajti potem je varnost večja. Shema ima lastnost, da učinkovito ugotovi, če je kdo glasoval dvakrat. Za varno izvedbo potrebujemo še anonimni kanal, ki omoga, da lahko volilec večkrat pošilja in še zmeraj ostane anonimen. Poleg tega potrebujemo še funkciji f in g, ki sta brez trčenj.

Registracija V fazi registracije uradniki ustvarijo in objavijo javni RSA ključ (n, e) in varnostni parameter k. Potem ko se volilec Viktor identificira kot volilni upravičenec volilni komisiji, oboji interaktivno izdelajo numerični psevdonim (žeton). Pri tem Viktor uporabi neko število, s katerim se identificira npr. EMŠO. Naj bo to število ID in naj bosta f in g dvoargumentni funkciji brez trčenj. To pomeni, da je računsko prezahtevno poiskati dveh vhodov za tako funkcijo, ki se preslikata v isto točko.

Da pridobi psevdonim, Viktor naredi naslednjo izmenjavo z volilno komisijo:

1. Viktor izbere števila a_i, c_i, d_i in r_i, $i = 1, 2, \ldots, 2k$ naključno iz Z_n
2. Nato izračuna $B_i = r_i^e f(x_i, y_i)$, kjer je $x_i = g(a_i, c_i)$, $y_i = g(a_i \oplus ID, d_i)$ in pošlje B_i , $i = 1, 2 \ldots 2k$
3. Volilna komisija izbere naključno podmnožico z k elementi iz $R = \{1, 2, \ldots, 2k\}$ in zahteva od Viktorja, da pokaže števila a_i, c_i, d_i, r_i za vsak $i \in R$.
4. Volilna komisija preveri če velja $B_i = r_i^e f(g(a_i, c_i), g(a_i \oplus ID, d_i))$ za vsak $i \in R$. Če je preverjanje uspešno, se predpostavi, da je tudi drugih k B_i-jev pravilnih, če preverjanje ni uspešno volilna komisija razveljavi registracijo.

5. Volilna komisija podpiše ostale B_i elemente $i \notin R$, tako da izračuna $S_i = B_i^d, i \notin R$, kjer je d zasebni ključ in pošlje Viktorju $S = \prod_{i \notin R} S_i$. Opazimo, da $S_i = B_i^d = (r_i^e f(x_i, y_i))^d = r_i^{ed} f(x_i, y_i)^d = r_i f(x_i, y_i)^d$, torej je $S = \prod_{i \notin R} r_i f(x_i, y_i)^d$.

6. Na koncu Viktor izračuna svoj psevdonim kot $P = \prod_{i \notin R} f(x_i, y_i)$ in njegov podpis $SP = \frac{S}{\prod^{i \notin R} r^i} = \prod_{i \notin R} r_i f(x_i, y_i)^d$.

Števila a_i, c_i, d_i in r_i, $i \in R$ niso več potrebna, zato zaradi preprostosti označimo preostale elemente $a_i, c_i, d_i, i \notin R$ z $a_1, c_1, d_1, \ldots, a_l, c_l, d_l$.

Volilna faza

1. Viktor izbere njegov glas v in izdela glasovnico $(v||P||SP)$ in jo zašifrira z javnim ključem volilne komisije (e, n) in pošlje $(v||P||SP)^e \pmod n$ preko anonimnega kanala.

2. Volilna komisija odšifrira sporočilo in preveri podpis SP za psevsonim P.

3. Volilna komisija pošlje nazaj Vikrtorju naključen binaren vektor $Z = (z1, \ldots, zk)$ dolžine k.

4. Volilec odgovori z T, ki vsebuje l trojk, ki deloma razkrijejo psevdonim. Če $z_k = 0$, potek je k-ta trojka (a_k, c_k, y_k). Če pa $z_k = 1$, potem je k-ta trojka $(x_k, a_k \oplus ID, d_k)$. To pomeni da, je za vsak k eden izmed argumentov funkcije f razkrit, drugega pa se lahko izračuna s funkcijo g, tako da za vhod vzamemo preostala elementa trojke.

5. Volilna komisija izračuna, če se Viktorjeve trojke ujemajo z psevdonimom P, ki ga je prej poslal. Če je test psevdonima P uspel, volilna komisija ni prejela od Viktorja še ene glasovnice s psevdonimom P in ta glasovnica je veljavna. Torej volilna komisija upošteva Viktorjev glas v.

Če pa je eden od volilcev dvakrat uporabil psevdonim P, potem lahko volilna komisija z visoko verjetnostjo izve identiteto tega volilca. Ko je volilec poslal psevdonim prvič (drugič), je prejel vektor Z1 (Z2) in tako deloma razkril psevdonim P. Z veliko verjetnostjo, se vektorja Z1 in Z2 razlikujeta na vsaj enem mestu k. To pa pomeni da je volilec poslal obe možni trojki. Tako ima volilna komisija na voljo vse podatke, da izračuna ID in tako razkrije identiteto volilca.

Preštevanje glasov Volilna komisija razglasi rezultate, tako da objavi seznam poslanih glasovnic, ki vsebuje $(v||P||SP)^e$ psevdonime P, SP, vektorje Z in trojke T in glasove v.

Upravičenost Volilec ne more sam izdelati žetona, ker potrebuje podpis volilne komisije. Komisija pa mu dovoli, da samo enkrat izdela podpis. Če volilec poskuša dvakrat voliti, lahko volilna komisija z visoko verjetnostjo razkrije njegovo identiteto. Upravičenost je dosegljiva samo, če je volilna komisija poštena.

Zasebnnost Po koncu faze registracije volilna komisija ne ve ničesar o psevdonimu volilca. Volilec razkrije samo eno polovico B_k-jev volilni komisiji, ki niso uporabljeni v psevdonimu. Ker sta funkciji f in g brez trčenj, volilec ne more zgenerirati nobenih drugih $a'_i, b'_i, c'_i, d'_i, r'_i$, tako da

$$B_i = (r'_i)f(g(a'_i, c'_i), g(b'_i, d'_i))$$

Tako volilna komisija zagotovi, da je psevdonim pravilno skonstruiran (volilec je vključil svoj ID). Ker izhod funkcije f izgleda naključen (prav tako zmnožek izhodov f), izgleda psevdonim naključen. Povezavo med identiteto volilca in njegovim psevdonimom je zaščitena s slepimi podpisi. Volilčeva identiteta je zaščitena, razen če uporabi svoj psevdonim dvakrat. Identitete pošiljatelja se ne da ugotoviti, ker je bila poslana po anonimnem kanalu. Ko volilec prvič uporabi psevdonim, sicer deloma razkrije njegovo strukturo volilni komisiji. Volilec razkrije samo takšno trojko $(x_i, a_i \oplus ID, d_i)$, ki je bila uporabljena pri izdelavi psevdonima. Ker sta funkciji f in g brez trčenj in ker v tem primeru volilna komisija ne pozna c_i, ne more iz teh podatkov izračunati ID. Podobno velja, če volilec pošlje drugo vrsto trojke pri $(z_i = 0)$. Če pa volilec poskuša drugič uporabiti svoj psevdonim potem se lahko informacija, ki jo je razkril prvič in drugič združi in se ugotovi ID volilca.

Preverljivost Volilec lahko preveri, če je njegova glasovnica objavljena na seznamu, ker pozna svoj psevdonim in podpis. Če volilec ne najde svojega psevdonima na seznamu, potem lahko protestira, tako da dokaže, da je poslal veljavno glasovnico in, da je bil njegov odziv na izziv volilne komisije korekten. Vendar s tem razkrije volilni komisiji, kako je glasoval. S tem je dosežena invidualna preverljivost. Univerzalna preverljivost ni dosežena, ker lahko volilna komisija glasuje namesto tistih, ki so niso glasovali, ali pa nekaterim volilcem zagotovi več žetonov.

Nedokazljivost Shema ni nedokazljiva, ker lahko napadalec od volilca zahteva števila a_i, c_i, d_i, r_i, ki jih je zgeneriral v fazi registracije. S pomočjo teh in objavljenih podatkov, pa lahko pridobi volilčevo identiteto in glasovnico.

4.5 Schonmakerjeva shema

V tej shemi volilec deli svoj glas med člane volilne komisije s pomočjo javno preverljive sheme za deljenje skrivnosti, ki je prikazana razdelku 3.1. Shema je bila opisana v [3].

Začetna faza Najprej se nastavi shemo za deljenje skrivnosti. Objavi se generatorja $g, G \in Z_p$ in javne ključe $h_j = g^{z_j}$ posameznih članov volilne komisije.

Volilna faza Volilec V_i izbere svoj glas $v_i \in \{0, 1\}$ in naključno število $s_i \in Z_p$. Nato razdeli skrivnosti g^{s_i} med člane volilne komisije in objavi vrednost $U_i = g^{s_i+v_i}$. Poleg tega mora pokazati, da $v_i \in \{0, 1\}$. Dokazati mora, da

$$\log_G C_0 = \log_g U_i \vee \log_G(GC_0) = \log_g U_i$$

Kjer velja $C_0 = G^{s_i}$, To dokaže z dokazom iz razdelka 3.3.3

Preštevanje glasov Predpostvimo, da so volilci $V_i, i = 1, \ldots, m$ veljavno oddali svoje glasovnice. Najprej so zbrani vsi zašifrirani deli:

$$H_j^* = \prod_i H_{ij} = \prod_i h_j^{p_i(j)} = h_j^{\sum_i p_i(j)}$$

Nato vsak od članov volilne komisije Aj uporabi protokol za rekonstrukcijo svojega dela iz razdelka 3.1. Zaradi homomorfnega šifriranja dobijo: $g^{\sum_i p_i(0)} = g^{\sum_i s_i}$. Potem se izračuna $\prod_i U_i = g^{\sum_i s_i+v_i}$ in nato še

$$g^{\sum_i s_i+v_i-\sum_i s_i} = g^{\sum_i v_i} = g^T = W$$

Končno število glasov T ŽA", se izračuna iterativno, tako da $O(M)$ krat modularno množimo, kjer je M število vseh volilcev: $g^1, g^2, \ldots$ dokler ne dobimo W.

Izpolnjene zahteve

- **Upravičenost.** Samo volilni upravičenci lahko pišejo po elektronski oglasni deski. Volilec ne more oddati neveljavne glasovnice in ne more dvakrat glasovati, ker more podati dokaz, da je njegov glas pravilne oblike.

- **Zasebnost, Robustnost.** Nobena množica največ t članov volilne komisije ne more pokvariti volitev. Zaradi sheme za deljenje skrivnosti je dosežena tudi zasebnost.

- **Univerzalna preverljivost.** Vsakdo lahko preveri, ali je volilčev glas veljaven. Shema za deljenje skrivnosti prepreči, da bi volilec narobe razdelil posamezne dele članom volilne komisije. Vsakdo lahko zmnoži šifrirane glasove j-tega člana volilne komisije in vsakdo lahko preveri, če je ta član pravilno dešifriral vsoto posameznih delov. Prav tako pa lahko vsakdo izračuna končni izid volitev iz objavljenih vsot posameznih članov.

- **Nedokazljivost.** Ta shema ni dokazljiva. Kajti napadalec lahko zahteva, da volilec razkrije svojo skrivnost s_i in tako ugotovi kako je volilec glasoval.

5 Elektronske volilne sheme v resničnem svetu

5.1 Zakaj voliti elektronsko?

Največja prednost volitev preko Interneta je predvsem udobnost za volilca. Kakorkoli že blizu je volilcu volišče, najbolj udobno je voliti doma preko računalnika. Najlažje za volilce bi bilo odpreti brskalnik, odpreti stran z volitvami, obkljukati svojo željo in pritisniti na gumb "Voli!". Danes po svetu je trend upadanja volilni udeležbe. Tak način bi morda spodbudil tiste volilce, ki se ponavadi ne udeležujejo volitev, da se jih udeležil.

Na dolgi rok bi take volitve verjetno zmanjšale stroške za izvedbo volitev, kajti za fizične volitve je potrebno veliko denarja za ljudi, ki delajo na voliščih. Lahko se tudi zgodi, da narobe preštejejo glasovnice. To naj ne bi predstavljajo večje napake, kajti ponavadi se zmotijo naključno in ne vedno v prid nekemu kandidatu. Zato je vpliv na končne rezultate naključen. Poleg tega se na elektronski način veliko hitreje in bolj zanesljivo prešteje glasove, kot pri štetju papirnatih glasovnic na roko. Vendar morajo biti ti glasovi pravilno pretvorjeni v elektronsko obliko, ker nam nič ne pomaga še enkrat prešteti vse glasove, kajti računalnik bo vrnil vedno isti rezultat. Zato je ena od zamisli, da se ob tem, ko volilec voli, tudi natisne glasovnico na papir.

Poznamo več različnih oblik elektronskih volitev:

- *Elektronske volitve na fizičnem volišču.* Ponavadi na volišča pripeljejo računalnike z zasloni na dotik, na katerih volilec odda svoj glas. Identifikacija volilca poteka na tradicionalen način.

- *Volitve v javnih kioskih.* V tem primeru volilna komisija pripelje kioske (stroje podobne kot v prejšni točki) na javna mesta, kjer se ljudje velikokrat zadržujejo (nakupovalna središča itd.). To se lahko organizira tudi na bankomatih oziroma na podobnih napravah, katerih je veliko v vsakem okolju. Ta način je bolj prikladen za volilce, vendar ta mesta niso pod neposrednim nadzorom volilne komisije. Tako mora identifikacija potekati na nek drug, prav tako varen način.

- *Volitve z oddaljenim dostopom.* Volilec od doma, iz službe, itd. odda glas iz svojega računalnika. Tu volilna komisija nima nadzora niti nad identifikacijo volilca, niti nad napravo s katero volilec oddaja svoj glas. Ta način je najbolj ranljiv za kakšne prevare, a je hkrati tudi najbolj udoben za volilca.

5.2 Varnost volitev z oddaljenim dostopom

Če bi bili organizatorji volitev popolni, bi bile volitve z navadnimi papirnatimi glasovnicami najbolj varne. Če pa želimo organizirati volitve na elektronski način, obstaja več različnih tveganj, da izid volitev ni pristen. Tveganja obstajo na voličevi napravi, na napravi volilne komisije, kot tudi na povezavi med njima.

Danes je na večini računalnikov naložen operacijski sistem Microsoft Windows. Ta sistem je bil načrtovan tako, da bi bil do uporabnika čim bolj prijazen, ne pa za tako občutljive naloge kot so izvedba volitev preko Interneta. Ta operacijski sistem ima veliko varnostnih lukenj. To pridoma izkoriščajo izdelovalci različnih virusov, hroščev in trojanskih konjev. Danes naj bi bilo 20% računlnikov okuženih z virusom [5]. Skratka izdelovalci sistema za volitve z oddaljenim dostopom nimajo nobenenga zagotovila, da so domači računalniki volilcev varni.

Zagotavljanje varnosti na povezavi med volilčevimi domačimi računalniki in centralnim strežnikom je tudi problematična, čeprav pametna raba javne kriptografije zagotavlja določeno stopnjo varnosti komunikacijskih kanalov. SSL (Secure Sockets Layer) in TLS(Transport Layer Security) sta protokola, ki jih uporabljajo brskalniki, da bi zagotovili varne komunikacijske kanale za internetno bančništvo itd. Protokola preprečita t.i. napad moža na sredini. Na žalaost pa je ta tehnologija ranljiva pred drugimi vrstami napadov kot so: napad z onemogočanjem storitve, spoofing itd. Čeprav je internetno bančništvo danes dokaj varno, je zagotavljanje varnosti volitev z oddaljenim dostopom težji problem zaradi dveh razlogov. V internetnem bančništvu se točno ve,

kdo je izvajalec transakcije in kakšna je vrednost transakcije. Pri volitvah pa med volilcem in njegovo glasovnico ne sme biti nobene povezave. Drugi razlog je, da če pride pri bančni transakciji do kakršnekoli napake, se jo lahko kasneje popravi. Če pa pride do napake pri volitvah, se jo popravi težje, sploh po razglasitvi rezultatov.

5.3 Družbeni vidik

Internet je danes že zelo razvit, vendar ga več uporabljajo predvsem nekatere družbene skupine.(mladi, premožnejši, meščani, izobraženi, ...) Zaradi možnosti udobnega voljenja z oddaljenim dostopom, bi se te skupine bolj množično udeleževale volitev. Ostale skupine pa se bi težje spopadle s to tehnologijo in bi se manj udeleževale volitev. Torej rezultat volitev ne bi v takšni meri odražal volje družbenih skupin, ki ne uporabljajo Interneta.

5.4 Dosedanje elektronske volitve

Prve Internetne volitve na državni ravni so bile organizirane v švicarskem kantonu Ženeva. V začetku leta 2003 so imeli prebivalci Ženeve možnost, da volijo preko Interneta [6]. Švicarji volijo bolj pogosto kot ostali drugje po svetu. Predvsem imajo več referendumov, tipično 4 do 6 na leto. Tak sistem neposredne demokracije nalaga volilni komisiji, da je volilni postopek, čim preprostejši in udobnejši. 85 odstotokov programske opreme volilnega sistema je odprtokodne. Zato je sistem transparenten in se drži Kerckhoffovega načela. Že leta 1995 so dali prebivalcem možnost, da oddajo svoj glas po pošti. To je dvignilo volilno udeležbo za 20%. Sistem internetnega glasovanja se je začel v Genevi razvijati leta 2000 in je razširitev glasovanja po pošti. Nobeden od teh dveh sistemov pa ne preprečuje kupovanja glasov in vplivanja na izbiro. V Švici se zanašajo na družbeno-kulturne norme in uveljavljene pravne mehanizme, da se zaščitijo pred takimi nevarnostimi.

Elektronske volitve so se pojavile že v zadnejem desetletju prešnega stoletja. Vendar to niso bile volitve preko Interneta, ampak elektronska oddaja glasovnice na samem volišču. V nekaterih državah poznajo samo tak sistem volitev. Naprimer v Braziliji imajo več kot 400.000 naprav za elektronske volitve. Nekaj manjših poskusov volitev preko Interneta so organizirale predvsem zasebne organizacije v poznih devetdesetih.

Sprva je bil namen takih volitev zagotoviti državljanom, ki so v tujini zagotoviti možnost udeležbe volitev. Ameriška vojska je leta 2000 želela zagotoviti vojakom daleč od domovnine, da volijo preko Interneta. Na koncu se je tega načina poslužilo 82 vojakov. Projekt je stal 6.2 milijona dolarjev. Kar je več kot 70.000 dolarjev na osebo [7]. Kjub temu pa niso uspeli zagotoviti ključnih varnostnih principov. Kljub tem napakam se je ta projekt razvil v sistem SERVE (Secure Electronic Registrtion and Voting Experiment), da bi služil širšim množicam na splošnih volitvah leta 2004, a so ga zaradi prevelikih varnostnih tveganj odpovedali. Prvi večji poskus političnih volitev pa je organizirala Demokratska stranka iz Arizone marca leta 2000. Približno 42 odstotkov od 85970 volicev se je odločilo, da odda svojo glasovnico preko Interneta [8]. Vendar so imele te volitve nekaj težav: sistem je odpovedal za nekaj časa, nekatere identifikacijske številke volicev so bile izgubljene in telefonska zveza s klicnim centrom za pomoč je bila preveč obremenjena, kajti veliko volilcev je imelo težave. Čeprav so Američani znani po uporabi naprednih tehnologij za volitve, imajo v preteklosti kar nekaj težav pri elektronskih volitvah. Leta 2000 na predseniških volitvah na Floridi, leta 2004 na predseniških volitvah v Ohiu (obakrat zmagal George W. Bush) so se pojavile nekatere težave zaradi katerih nekateri dvomijo v legitimnost teh volitev [10]. Tudi leta 2007 se je zgodila neprijetnost, ko je bilo kar 18.000 elektronskih glasovnic praznih [9]. Zato se še dolgo po tem ni vedelo, kdo bo zasedel sedež v Kongresu.

Različne oblike elektronskih volitev z oddaljenim dostopom (preko telefona, Interneta in SMSov) so izpeljali v Angliji leta 2002 in 2003 [11]. Tudi drugod po Evropi (Franciji, Nemčiji in Švedski) so bili uspešni poiskusi Internetnih volitev v okviru projekta CyberVote, ki ga je organizirala Evropska komisija. Namen je bil razviti varen prototip za elektronske volitve preko mobitelov in Interneta [11]. Projekt pa se ni razvil v nič večjega. Pravi pionirji na področju internetnih volitev pa so Estonci, leta 2005 so dali možnost volilcev, da lahko med drugim glasujejo tudi preko Interneta. Nekatere menijo, da so to prve prave internetne volitve, kajti bile so organizirane na nacionalni ravni. Od takrat naprej lahko Litvanci volijo preko Interneta. Leta 2009 na lokalnih volitvah je preko Interneta glasovalo približno več kot 100.000 državljanov, kar je okoli 10 odstkov vseh volilni upravičencov [12].

Nekatere države so zelo naklonjene elektronskim volitvam in ustanvljajo projekte s katerimi želijo zagotoviti varne volitve preko Interneta naprimer Norveška. Na drugi strani pa so države, ki želijo ukiniti elektronske volitve kot naprimer Italija. V Nemčiji pa je celo vrhovno

sodišče razsodilo, da je bila uporaba elektronskih volitev leta 2005 protiustavna [13].

6 Zaključek

V zadnjih letih je bilo na razvoju elektronskih volilnih shem narejenega veliko napredka, predvsem na teoretičnem delu. Spoznali smo sheme z anonimnim kanalom, s homorfnim šifriranjem in z mešanjem glasov. Vsaka od teh vrst ima svoje prednosti žal pa tudi slabosti. Pri shemah z anonimnim kanalom je potrebno implementirati anonimni kanal, ki ima pomankljivost, da za vsak bit, ki ga želimo poslati po anonimnem kanalu, moramo poslati 10^5 bitov po javenm kanalu [1]. Sheme s homomorfnim šifriranjem ponavadi niso nedokazljive. Sheme z mešanjem glasov zahtevajo varni kanal med volilcem in volilno komisijo. Obstajo tudi sheme, ki so mešanice teh shem in imajo manj slabosti. Vendar zaenkrat še ne obstaja popolna shema, ki bi izpolnila vseh zahteve.

Po drugi starni je danes v realnosti težko narediti volilno shemo, ki bi ustrezala vsem zahtevam varnosti. Volitve so zelo občutljiva stvar, ki zahteva predvsem varnost. Ker danes računalniki še niso dovolj varni, da bi služili kot posrednik med volicem in volilno komisijo, volitve preko Interneta še niso razširjene po svetu. Tudi volitve na računalnikih na fizičnem volišču niso idealne in so v preteklosti povzročale veliko preglavic. Organizatorji volitev morajo narediti kompromis med varnostjo in udobnostjo volitev; med tradicionalnostjo in digitalizacijo. Prav gotovo pa bi pa varna shema za volitve z oddaljenim dostopom prispevala k demokratizaciji družbe, kajti ljudje bi se lahko bolj pogosto odločali izraziti svojo voljo.

Literatura

[1] David L. Chaum. Untraceable electronic mail, return address, and digital pseudonym. Communication of ACM 24, Feb 1981.

[2] Michael J. Radwin. An untraceable, universally verifiable voting scheme. 1995.

[3] Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. Advances in Cryptology - CRYPTO, 1666 of Lecture Notes in Computer Science:148– 164, 1999.

[4] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. Advances in Cryptology - EUROCRYPT, 1997.

[5] Paul Roberts. Your PC May Be Less Secure Than You Think. IDG News Service. 2004.

http://www.pcworld.com/article/118311/your_pc_may_be_less_secure_than_you_think.html

[6] Bruce Schneier. Internet Voting. Crypto-Gram. 2001.

http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b4

[7] John Dunbar. Internet Voting Project Cost Pentagon $73,809 Per Vote. 2001.

http://projects.publicintegrity.org/telecom/report.aspx?aid=297

[8] Lalita Acharya Science and Technology Division. Internet Voting. September 2003.

http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-e/PRB0306-e.pdf

[9] Kim Zetter. House Seat Hangs by a Byte. November 2007. http://www.wired.com/science/discoveries/news/2007/01/72452

[10] Open Rights Group. Electronic Voting. A challenge to democracy? January 2007.

http://www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf

[11] Countries with e-voting projects.

http://aceproject.org/ace-en/focus/e-voting/countries

[12] Internet Voting in Estonia.

http://www.vvk.ee/index.php?id=11178

[13] No e-voting in Germany. March 2009.

http://www.edri.org/edri-gram/number7.5/no-evoting-germany