Pripensoj pri la reta voĉdonsistemo

Paŭlo Ebermann

5–a de junio, 2010

Superrigardo pri la aktuala Reta Voĉdonsistemo de TEJO, problemoj de ĝi kaj propono pri pli sekura varianto.

Enhavo

1 Postuloj pri reta voĉdonsistemo

(De la laborgrupo pri reta voĉdonsistemo dum la Komitatkunveno 2008, akceptita de la Komitato.)

1. Nur la Ĝenerala Sekretario povu gvidi balotojn.
2. Estu distingo inter publikaj kaj sekretaj balotoj.

   Komunaj trajtoj:

   a) La ĜenSek povu vidi je ĉiu tempo, kiu jam voĉdonis en ajna baloto.

   b) Ĉiuj povas vidi la suman rezulton de la baloto post la limdato.

   c) Estas du specoj de sindetenoj: aktiva sindeteno kaj malĉeesto. La ĜenSek sola povu vidi, kiu sindetenis ne donante voĉon. En la kalkulo de la rezulto, ambaŭ specoj de sindetenoj sumiĝas kaj nomiĝas "Sindetenoj".

   Publikaj balotoj: Ĉiu povu vidi, kiu kiel voĉdonis, sed nur post la limdato. Dum la balotado, nenia informo estas publike videbla.

   Sekretaj balotoj: Neniu povu vidi la unuopajn voĉojn de la voĉdonintoj, sed nur la suman rezulton de la baloto.
3. Voĉdonoj ne estu ŝanĝeblaj.

2 Nuna sistemo

Tiu ĉapitro priskribas la sistemo kreita de Tom Juval, trovebla dum julio–septembro 2009 en `http://www.tejo.org/vds/`.

2.1 Datumbazstrukturo

Ĝi havas la jenan datumbazstrukturon, laŭ mia kompreno.

2.1.1 Ĝeneralaĵoj

Tabelo kun nur unu linio.

kiu = 0

kio kalkulilo de la nombro/numero de proponoj (plialtigita en ĉiu "kreuProponon()").

Mi ne scias, por kio oni bezonas tiun tabelon, ĝi ŝajnas superflua.

2.1.2 Uzantoj

Listo de uzanto-kontoj.

uzanto la salutnomo.

pasvorto la pasvorto en klare legebla teksto

flagoj la rajtoj de la uzanto, en bit-kampo:

$1 = 2^0$ Komitatano (havas voĉdonrajton)

$2 = 2^1$ Estrarano (mi ne tute certas

$4 = 2^2$ ĜenSek (rajtas administri)

Homoj sen iuj el tiuj rajtoj estas nomitaj "Aliaj" – tiuj estas observantoj, ekzemple TEJO-Volontulo, komisiitoj, ktp.

Fakte estu nur maksimume unu el tiuj bitoj metita (pro la tabela montrado, kaj la elektoj en la kreilo). Tio signifas, ke la ĜenSek havu ankoraŭ aldonan konton por sia persona uzo.

ekde la dato/tempo de la kreado de la uzanto.

2.1.3 proponoj

Privoĉdonendaĵoj.

id

titolo titolo

enhavo teksto de la propono

flagoj tipo de la voĉdono:

1 = sekreta

0 = publika

ekde komenca dato/tempo

limtempo findato/tempo

jesis nombro de jes-voĉoj ĝis nun.

neis nombro de ne-voĉoj ĝis nun.

sindetenis nombro de sindetenoj ĝis nun.

2.1.4 voĉdonoj

La donitaj voĉoj.

propono

uzanto

voĉo Unu el la sekvaj:

0 = sekreta voĉo

1 = jesis

2 = neis

3 = sindetenis (aktive)

kiam

2.1.5 ŝlosoj

Ŝloso, por garantii, ke maksimume unu uzanto samtempe modifas la tabelojn. Estas unu ŝloso por ĉiu propono.

propono

uzanto la uzanto, kiu nun havas la ŝloson, aŭ "", se neniu havas ŝloson nun.

2.1.6 voĉdonantoj

Liste de la voĉdonrajtigitoj por ĉiu propono. Plenigita dum kreado de propono.

propono

uzanto

2.1.7 nevoĉdonintoj

Listo homoj, kiuj ankoraŭ ne voĉdonis pri iu propono. Plenigita dum kreado de propono. Le enskriboj unuope estas forigota dum "registruVoĉdonon()".

propono

uzanto

3 Urĝa sekureca ŝanĝo

La pasvorto estas stokita en klar-teksto en la datumbazo. Tiel por ĉiu, kiu povas legi la datumbazon, eblas ekscii pasvortojn de uzantoj. Tio estas problema, ĉar oni tiel ne nur povas voĉdoni per ilia konto (kion eblus ankaŭ per manipulado de la datumbazo), sed ofte per tiu pasvorto ankaŭ povas atingi aliajn kontojn de la samaj homoj.

Por eviti tion, necesas anstataŭ la pasvorto p stoki $h(p)$ kun haketfunkcio h – prefere tio estu kriptografie forta haketfunkcio, kaj prefere kun "saltado", do ekzemple uzo de $h(u + p)$, kie u estas la uzantnomo.

Por kontrolo de la pasvorto de uzantoj necesas nur kalkuli la saman funkcion por la entajpita pasvorto, kaj kompari la rezultojn.

Tiel eĉ kun aliro al la datumbazo ne plu eblas eltrovi la pasvorton.

(Se la atakanto povas ŝanĝi la PHP-kodon, li tamen havas eblon ekhavi la pasvortojn de postaj uzantoj, ĉar la uzantoj ja entajpas ĝin. Sed por tio oni bezonas iom pli da krima energio, kaj bonŝancon ke ĝi ne estos trovita.)

4 Aliaj problemoj – rezisto kontraŭ manipuloj

Per la nuna sistemo, principe ĉiu, kiu havas skriban aliron al la datumbazo, povas laŭplaĉe manipuli la voĉdonojn.

En kazo de publikaj voĉdonoj la voĉdonantoj povas poste protesti, se la propra voĉo estas fuŝe registrita (kaj tiam oni povos demandi, ĉu ili fuŝe voĉdonis aŭ estis manipulado), sed en kazo de sekretaj voĉdonoj eĉ ne eblas eltrovi tian manipuladon, se la manipulanto ne estas tro stulta[1].

Do necesas absoluta fido al ĉiu, kiu povas manipuli la datumbazon.

5 Ideoj pri pliaj plisekurigo

La 26an de septembro, dum trajnvojaĝo de Bratislavo al Berlino mi iom pripensis, kiel eblas helpe de kriptografio solvi tiun problemon. (En la trajna varianto de mia ideo mi havis ankaŭ voĉdonojn kun pliaj ebloj ol "jes", "ne", "sindeteno", kiuj utilus por plur-flankaj voĉdonoj. Ĉar tiuj ne estis en la origina sistemo de Tom, mi forlasis ilin nun.) Jen eta priskribo.

5.1 Superrigardo

Principe ni provas eviti ne-aŭtorizitajn ŝanĝojn en la datumoj per tio, ke ĉiuj datumoj estas kriptigitaj kaj/aŭ subskribitaj de la koncernaj personoj. Tian kriptigadon/subskribadon (kaj la malkriptigadon kaj kontrolon de la subskriboj) kompreneble ne la uzantoj mem devas fari, sed la programo faras por ili, uzante ŝlosilojn aŭ stokitajn en la tabeloj, aŭ generitajn el la pasvorto (kaj uzantnomo ktp).

[1] Ekzemple, la sumo de la voĉoj (jes + ne + sindeteno) daŭre restu ĝusta, kaj ne estu unuanimaj rezultoj.

Kelkaj informoj estas stokitaj plur-loke, por ebligi postan komparon kaj kontrolon.

En kazo de publikaj voĉdonoj principe estas sufiĉe facile: Ĉiu voĉdonanto kriptigas sian voĉdonon (kaj subskribon de ĝi) per publika ŝlosilo de la voĉdono, kaj post la fermo de la voĉdono ĉiuj povas per la tiam publigita eks-sekreta ŝlosilo legi kaj kontroli ĉiujn voĉojn.

En kazo de sekretaj voĉdonoj ne eblas, ke uzantoj subskribu sian propran voĉon kontrolebla por ĉiuj (ĉar ja aliaj ne eksciu, kiu voĉis kiel). Por ebligi almenaŭ ioman kontrolon, ni devos certigi, ke ĉiu voĉdoninto povu kontroli, ke sia propra voĉo estas ĝuste kalkulita.

Tial ni stokas la individuajn voĉojn en du lokoj – kaj en loko ligita al la voĉdonanto (kaj tie kriptigite, ke nur li mem povu legi), kaj en loko neligita al la voĉdonanto, kiu (krom en kriptigita parto) ne havas ajnan indikon al tio, kiu voĉdonis.

Post la fermo de la voĉdonoj ĜenSek malfermas la sekretan ŝlosilon, kalkulas la voĉojn, kaj subskribas la rezulton (kun la individuaj nepersonaj voĉoj).

Post tio, la voĉdonintoj povas kontroli, ĉu la propra voĉo estas bone registrita (t.e., ke ne estas diferencoj inter la persona kaj ne-persona voĉo), kaj tion konfirmi (subskribante ankaŭ la kalkulon de ĜenSek).

5.2 Notacio

Por la sekva priskribo (kaj la sistemo poste) ni bezonas la sekvajn funkciojn:

- $h_1(x), h_2(x)$ – kriptografie fortaj haketaj funkcioj, kiuj donas diversajn rezultojn, ekzemple kreitaj el SHA-2. Kiam mi uzas $h(x)$, oni povas uzi ajnan haketan funkcion (sed prefere ĉiam la saman.) [2] [3]

- $\kappa(k,x), \kappa^{-1}(k,y)$ – simitria kriptiga funkcio, kun la kongrua malkriptiga funkcio (kaj ŝlosilo k). Estas
$$x = \kappa^{-1}(k, \kappa(k,x))$$
(En iuj skemoj povas esti $\kappa = \kappa^{-1}$.)

- $\varphi(k^1,x), \psi(k^2,x)$ – asimitria kriptiga funkcio, kun la kongrua malkriptiga funkcio kaj paro de publika kaj sekreta ŝlosilo (k^1,k^2). Devas validi
$$x = \psi(k^2, \varphi(k^1,x)) = \varphi(k^1, \psi(k^2,x)),$$
kaj ke ψ estas malfacile kalkulebla sen koni la ŝlosilon, eĉ se oni konas la alian slosilon. (En iuj skemoj povas esti $\varphi = \psi$.)

- $\sigma(k^2,x), \tau(k^1,x,s)$ – subskribo-funkcio kaj testfunkcio por la subskribo, kun paro de publika kaj sekreta ŝlosilo.[4]

[2] Oni povas ambaŭ funkciojn krei el la sama funkcio h, ekzemple per $h_1(x) := h(\text{"pasvorto"} + x)$, $h_2(x) := h(\text{"ŝlosilo"} + x)$ ktp.

[3] Plia notacio: Kiam ni uzas + en la dua argumento de h_i aŭ σ, ĝi celas ĉeno-kunigon, ne adicion de numeroj. Do tiu + (kaj sekve $h(a+b)$) ne estas komutativa.

[4] Tiujn oni kutime povas konstrui el h_i, φ kaj ψ, ekzemple per $\sigma(k^2,x) := \varphi(k^2, h(x))$, kaj $\tau(k^1,x,s) := (h(x) \stackrel{?}{=} \psi(k^1,s))$.

Se $y = \sigma(k_2, x)$, tiam $\tau(k_1, x, y) =$ jes, kaj kaj ne estas facile (sen koni k_2) trovi $x^* \neq x, y^*$ kun $\tau(k_1, x^*, y^*) =$ jes.

Kiel plian simbolon ni uzu ĜS por la uzanto-konton de la Ĝenerala Sekretario.

5.3 Datumbazstrukturo

5.3.1 Uzantoj

La listo de la uzantoj, kaj informoj pri tiu uzanto. Ĉiu uzanto u havas la jenajn ecojn:

- id_u – identigilo (numero).
- l_u – la salutnomo de la uzanto.
- p_u – la pasvorto.
- $k_u := h_2(p_u + \mathrm{id}_u + l_u)$ – simetria ŝlosilo, nenie stokita sed laŭ bezono kalkulita.
- k_u^1, k_u^2 – paro de ŝlosiloj por asimetria kriptigado. Ili estas kreitaj dum kreado de la uzanto, aŭ pli bone post la unua ensaluto de la uzanto. La uzanto mem ne vere devas koni ĝin, nur la pasvorto por atingi ĝin.
- r_u – la rajtoj de la uzanto, iel ajn kodita. Ekzemple tio povas enhavi la tipon de komitataneco: A/B, C, E, nenio, kaj ankaŭ la rajton ĜenSek-umi.

En la datumbazo ni stokas la jenon:

id id_u

uzantnomo l_u

nomo la plena nomo de la uzanto – ankaŭ foje utilas, sed eble ne necesas.[5]

pasvorto $p_u^* := h_1(p_u + \mathrm{id}_u + l_u)$. Tion ni uzas por kontroli la pasvorton.

publika ŝlosilo k_u^1, la publika ŝlosilo de la uzanto.

sekreta ŝlosilo $\kappa(k_u, k_u^2)$ – la sekreta ŝlosilo en kriptigita (kaj nur de la uzanto mem malkriptebla) formo.

flagoj r_u (la rajtoj de la uzanto)

ekde dato/tempo de la kreado (ĉu bezonata?).

subskribo de uzanto $\sigma(k_u^2, \mathrm{id}_u + l_u + k_u^1 + p_u^*)$ – certigas, ke neniu (krom la uzanto mem) povas ŝanĝi la pasvorton kaj publikan/sekretan ŝlosilon.

subskribo de ĜenSek $\sigma(k_{\hat{\mathrm{G}}\mathrm{S}}^2, \mathrm{id}_u + l_u + r_u)$ certigas, ke neniu (krom ĜenSek) povas ŝanĝi la rajtojn de la uzanto.

Kiam la uzanto ŝanĝas sian pasvorton, necesas rekriptigi la sekretan ŝlosilon.

[5] Se ni havas ĝin, tiam ni inkludu ĝin en unu el la subskriboj sube, depende de tio, ĉu la uzanto mem aŭ la ĜenSek rajtas ŝanĝi ĝin.

5.3.2 Proponoj

La listo de la aferoj, pri kiu oni voĉdonas. por ĉiu propono p, ni havas:

id id_p

titolo tit_p – mallonga titolo

demando d_p – la teksto de la propono

aktivigodato d_p^a

limdato d_p^l

stato ekzemple “dum kreado”, “aktiva”, “fermita” (aŭ korespondaj flagoj).

tipo tip_p ekzemple “publika baloto”, “sekreta baloto”. (Eblus tie ankaŭ distingi aliajn baloto-tipojn, ekzemple voĉdonojn pri la estraro (nur A+B+C), pri komitatanoj C (nur A+B), aliaj temoj (A+B+C+E).)

publika ŝlosilo k_p^1 – speciala publika ŝlosilo por tiu ĉi baloto.

sekreta ŝlosilo $k_p^* = \kappa(k_{\hat{\mathrm{G}}\mathrm{S}}, k_p^2)$ – la kongrua sekreta ŝlosilo, nur uzebla por ĜenSek (kaj estos uzota nur post la fermo)[6]

eks-sekreta ŝlosilo k_p^2 – post la fermo de la baloto ĜenSek publikigas la (eks-)sekretan ŝlosilon, kaj uzas ĝin por kalkuli la voĉojn. Aliaj tiel ankaŭ povas kontroli.

subskribo de ĜenSek $\sigma(k_{\hat{\mathrm{G}}\mathrm{S}}^2, \mathrm{tit}_p + d_p + d_p^l + d_p^a + \mathrm{tip}_p + k_p^1 + k_p^*)$ – por eviti ŝanĝojn post la aktivigo.

memsubskribo $s_p := \sigma(k_p^2, \mathrm{tit}_p + d_p + d_p^l + d_p^a + \mathrm{tip}_p + k_p^1 + k_p^*)$ – por eviti ŝanĝojn post la aktivigo.

voĉoj donitaj simpla kalkulilo por facila superrigardo. Komence 0, estas plialtigita je ĉiu voĉdono.

rezulto (nur post la fermo):

- **jes** $\#_p^{\mathrm{jes}}$ (nombro)
- **ne** $\#_p^{\mathrm{ne}}$ (nombro)
- **sindeteno** $\#_p^{\mathrm{sindeteno}}$ (nombro)
- **dig** $\mathrm{dig}_p := h(\bigoplus_{i \in \mathrm{VN}_p} \mathrm{id}_i + d_i + v_i + m_i)$ – kontrolsumo de ĉiuj rezultoj, por eviti postan ŝanĝon (kune kun la sekva subskribo)
- **subskribo** $s_p^{\mathrm{rez}} = \sigma(k_{\hat{\mathrm{G}}\mathrm{S}}^2, \#_p^{\mathrm{jes}} + \#_p^{\mathrm{ne}} + \#_p^{\mathrm{sindeteno}} + \mathrm{dig}_p)$

[6] Tion bedaŭrinde ne eblas certigi per la nuna maniero, do principe ĜenSek povas trompi, se li samtempe havas aliron al la servilo kaj ioman teknikan sperton. Tiu laŭ mi estas la plej malforta punkto de la sistemo.

5.3.3 voĉdono persona

En tiu tabelo ni stokas por ĉiu rajtigita uzanto u kaj ĉiu propono p la informojn, ĉu li voĉis, kaj kiel. (en kriptigita formo). La tabeleroj estas kreitaj dum kreado/aktivado de la propono, kaj poste ŝanĝita dum la voĉdono.

id $\mathrm{id}_{(u,p)}$

uzanto id_u

propono id_p

por ĜenSek $\varphi(k^1_{\hat{\mathrm{G}}\mathrm{S}}, \boxed{\square})$:

donita $d_{(u,p)}$ – jes/ne-valoro, ĉu jam donis voĉon?
kiu $s \in \{u, p\}$ – kiu kreis tiun parton – voĉdono (u) aŭ propon-kreilo (p)
subskribo $\sigma(k^2_s, \mathrm{id}_u + \mathrm{id}_p + s + d_{u,p})$

Per tio ĜenSek povos kontroli, ĉu la koncerna persono jam voĉdonis.

por publikigo en sekretaj voĉdonoj malplena, en publikaj voĉdonoj $\varphi(k^1_p, \boxed{\square})$:

donita $d_{(u,p)}$ – jes/ne-valoro
voĉo nepersona $\mathrm{id}^*_{(u,p)}$ – ligo al la nepersona voĉo
voĉo $v_{(u,p)}$ – unu el jes/ne/sindeteno/ne voĉis.
propono-dig s_p (por eviti ŝanĝon de la demando post la voĉdono)
kiu $s \in \{u, p\}$ – kiu kreis tiun parton – voĉdono (u) aŭ propon-kreilo (p)
subskribo $\sigma(k^2_s, \mathrm{id}_u + \mathrm{id}_p + s + d_{u,p} + s_p + v_{(u,p)} + \mathrm{id}^*_{(u,p)})$

Tiu parto estos legebla post la fermo de la voĉdono, kiam ĜenSek publikigas la sekretan ŝlosilon de la voĉdono.

por voĉdonanto $\varphi(k^1_u, \boxed{\square})$ (t.e. legebla nur de la voĉdonanto mem):

donita $d_{(u,p)}$ – jes/ne-valoro
voĉo nepersona $\mathrm{id}^*_{(u,p)}$ – ligo al la nepersona voĉo
voĉo $v_{(u,p)}$ – unu el jes/ne/sindeteno/ne voĉis.
propono-dig s_p (por eviti ŝanĝon de la demando post la voĉdono)
kiu $s \in \{u, p\}$ – kiu kreis tiun parton – voĉdono (u) aŭ propon-kreilo (p)
subskribo $\sigma(k^2_s, \mathrm{id}_u + \mathrm{id}_p + s + d_{u,p} + s_p + v_{(u,p)} + \mathrm{id}^*_{(u,p)})$

Tiu restos kaŝita, sed ebligas al la voĉdonanto poste kontroli, ĉu lia voĉo estas ĝuste kalkulita.

kontrolita *(TODO: necesas ankoraŭ ioma priskribo)*

En tiu spaco post la fermo de la voĉdono la uzanto povas meti informojn pri tio, ke (respektive ĉu) lia voĉo estas ĝuste kalkulita.

rezulto-dig dig_p

ĝustas $\hat{g}_{(u,p)}$ – ĉu ĝuste kalkulita? jes/ne/ne kontrolita

subskribo $\sigma(k_p^2, \mathrm{id}_u + \mathrm{id}_p + \mathrm{id}_{(u,p)} + \hat{g}_{(u,p)} + \mathrm{dig}_p)$

5.3.4 voĉdono nepersona

Tiu tabelo enhavas unuopajn voĉojn, sed en formo ne ligita al unuopa voĉdonanto. Ĝiaj elementoj $i \in \mathrm{VN}_p$ estas kreitaj de la propono-kreilo (de propono p) kun $d_i =$ »ne«, kaj poste la voĉdonilo elektas hazarde iun, kiu ankoraŭ havas $d_i =$ »ne«, metas $d_i =$ »jes« kaj plenigas ĝin per informoj. Tiel (en kazo de nepublika voĉdono) ne eblas respuri, kiu voĉis kiel.[7]

Jen post kiam uzanto u voĉis pri propono p:

id $\mathrm{id}_i = \mathrm{id}^*_{(u,p)}$

propono id_p

donita $d_i = d_{(u,p)} =$ »jes« (dum kreado $d_i =$ »ne«)

por publikigo $\varphi(k_p^1, \boxed{\square})$:

> **voĉo** $v_i = v_{(u,p)}$ – jes/ne/sindeteno

Tio estas la voĉo, estos legebla post la fermo de la voĉdono.

por voĉdoninto $m_i := \varphi(k_u^1, \boxed{\square})$:

> **voĉo** $v_i = v_{(u,p)}$ – jes/ne/sindeteno
> **propono-dig** s_p
> **subskribo** $\sigma(k_u^2, \mathrm{id}^*_{(u,p)} + \mathrm{id}_p + d_{(u,p)} + v_{(u,p)} + s_p)$

Tiun la voĉdoninto post la fermo de la voĉdono povos uzi por kontroli sian voĉon.

[7] Se la atakanto dum la tuta tempo observas la datumbazon, li tamen povas ekscii, kiuj voĉoj personaj kaj voĉoj nepersonaj samtempe pleniĝas. Sed mi ne vidas praktikan vojon, kiel eviti tian atakon.

5.3.5 Aliaj tabeloj

Ŝajnas, ke mia propono povus funkcii kun nur tiuj kvar tabeloj.

- La ŝlosoj-tabelo eble ankaŭ utilas, sed anstataŭe oni ankaŭ povus uzi la transakcian funkcion de la datumbaza sistemo (ekzemple `BEGIN TRANSACTION` kaj `COMMIT`, aŭ la pli primitivaj `LOCK TABLES` kaj `UNLOCK TABLES`).
- Se oni volas subteni voĉdonojn kun pluraj elektoj (t.e. pli ol nur "Jes", "Ne", "Sindeteno"), utilus aldoni tabelon por stoki la voĉdoneblojn por ĉiu propono - la voĉo en la voĉdono-tabeloj tiam enhavus referaĵon al tiu tabelo. Necesus ankaŭ adapti la rezulto-kalkuladon kaj kaj la propono-tabelon, por ebligi subskribon de ankaŭ la voĉdonebloj.
- La tabelojn voĉdonanto kaj nevoĉdoninto ni enmetis en nian voĉdono persona-tabelon.

5.4 Funkciado

La plejparton de la funkciado jam estas priskribita ĉe la tabeloj. Jen kelkaj detaloj.

5.4.1 Ĝenerale

Kiam iu uzanto u estas ensalutita, la sistemo konas ties pasvorton p_u^* kaj per tio povas malkriptigi la sekretan ŝlosilon k_u^2. Tiun ni bezonos por nia agado.

Tiu "kono" ĉiam finiĝas, kiam la uzanto elsalutas. (Eble eĉ ni povas uzi HTTP-Authentikado, tiam la sistemo tute ne memoras la pasvorton, sed dum ĉiu voko de paĝo rericevas ĝin. Tiu tamen havas la malavantaĝon ke ne vere eblas malsaluto, kaj la retumilo kutime memoras la pasvorton almenaŭ dum kelka tempo.)

5.4.2 Kreado de proponoj

Tie estas $u = \hat{\mathrm{G}}\mathrm{S}$, do la sistemo konas $k^2_{\hat{\mathrm{G}}\mathrm{S}}$.

1. ĜenSek havas formularon, en kiu eblas enmeti titolon kaj demandon kaj elekti tipon. Ankaŭ aktivigo- kaj limdaton.
2. La sistemo el tio kreas novan propono-datumbazeron p, kun stato 'dum kreado'.
3. La sistemo kreas paron de publika kaj sekreta ŝlosilo (k_p^1 kaj k_p^2) por tiu enketo, metas la publikan ŝlosilon k_p^1 kaj kriptigitan version k_p^* de la sekreta ŝlosilo k_p^2 en la datumbazeron.
4. La sistemo kreas subskribon de tiuj datoj kaj per $k^2_{\hat{\mathrm{G}}\mathrm{S}}$ kaj per la ŝlosilo k_p^2 kaj metas tiujn en la datumbazeron.
5. La sistemo kreas datumbazerojn en la tabeloj voĉdono persona kaj voĉdono nepersona por ĉiu voĉdonrajtigito (tio dependas de la tipo de voĉdono) kaj tiu propono.
6. La sistemo ŝanĝas la staton al "aktiva" aŭ "atendas aktivadon".

5.4.3 Voĉdono

1. Uzanto u elektas proponon p, pri kiu li volas voĉdoni.
2. La sistemo kontrolas,
   a) ĉu la subskriboj de la propono-tabelero p ankoraŭ estas validaj (t.e. neniu manipulis la proponon) (alikaze ni montras erarmesaĝon kaj eble ankaŭ sendu retmesaĝon al iu pri tio);
   b) ĉu la aktuala dato estas inter la aktivigo- kaj limdato por la propono;
   c) ĉu la uzanto rajtas voĉdoni pri tiu propono (depende de la tipo kaj la uzanto-grupo) (alikaze ni nur montras informojn pri la propono, kaj informon ke li ne rajtas); kaj
   ĉ) ĉu la uzanto ankoraŭ ne voĉdonis (t.e. la voĉdono persona de li ankoraŭ ne estas plenigita, per kontrolo de la parto por voĉdonanto) (alikaze ni montras al li, ke kaj kiel li jam voĉdonis).

   Se ĉiuj estas pozitiva, la sistemo montras al li voĉdonilon.
3. La uzanto elektas unu el la ebloj “Jes”, “Ne”, “Sindeteno”.
4. La sistemo havigas al si ŝlosojn por ambaŭ voĉdono-tabeloj.
5. En la tabelo voĉdono nepersona la sistemo elektas unu eron i, kiu ankoraŭ havas $d_i =$ »ne«. Tie ĝi metas $d_i :=$ »jes« kaj enmetas ankoraŭ la informojn por publikigo kaj por voĉdoninto.
6. En la tabelo voĉdono persona la sistemo prenas la eron kun $\mathrm{id}_{(u,p)}$, kaj enmetas la informojn por ĜenSek, por publikigo (en kazo de publika voĉdono) kaj por voĉdonanto.
7. La sistemo plialtigas la kalkulilon voĉoj donitaj en la propono-tabelo.
8. La sistemo liberigas la ŝlosojn por la voĉdono-tabeloj.

5.4.4 Fermo kaj kalkulado

Post kiam la limdato de la propono p pasis, ĜenSek denove eniras, kaj ekas la kalkuladon.

1. ĜenSek klakas »Kalkulu«. (Eble ni anstataŭe povas fari tion aŭtomate kiam ĜenSek unuan fojon ensalutas post la limdato.)
2. La sistemo metas la staton de p al »Fermita«.
3. La sistemo malkriptigas la sekretan ŝlosilon k_p^2 (el k_p^*).
4. La sistemo metas la sekretan ŝlosilon k_p^2 en la propono-tabelon.

5. La sistemo trairas la datumbazerojn de voĉdono nepersona kaj malkriptigas tie la por publikigo-partojn. Ĝi dume kalkulas la voĉojn.

6. (nur en kazo de publika voĉdono) La sistemo trairas la datumbazerojn de voĉdono persona kaj malkriptigas tie la por publikigo-partojn, kaj komparas la valorojn tie kun la partoj en la korespondaj voĉdono nepersona-datumbazeroj. Ĝi ankaŭ kontrolas la subskribon.

7. La sistemo metas la rezulton – $\#_p^{\text{jes}}$, $\#_p^{\text{ne}}$, $\#_p^{\text{sindeteno}}$, kontrolsumon kaj subskribon (de ĜS) de tio en la propono-tabelon.

5.4.5 Kontrolo kaj konfirmo

En sekretaj voĉdonoj ne eblas subskribo de la voĉoj (ĉar ni ja volas eviti, ke eblas eltrovi, kiu voĉis kiel). Do tie ni bezonas mekanismon, ke ĉiu voĉdonanto u povu kontroli kaj konfirmi, ke la propra voĉo estas ĝuste kalkulita. Tio okazas post la kalkulado de la voĉoj kaj publikigo de la rezultoj (por propono p).

1. La uzanto klakas »Kontrolu«. (Eble ankaŭ tion ni povas fari aŭtomate post la ensaluto.)

2. La sistemo prenas k_p^2

3. La sistemo faros paŝon 5 de 5.4.4 denove, kaj komparas la rezultojn kun la enhavo de rezulto.

4. La sistemo rigardas la voĉdono persona por (u, p), malkriptigas la parton por voĉdonanto kaj ekhavas $d_{(u,p)}$, $\text{id}^*_{(u,p)}$, $v_{(u,p)}$, s_p. (Ni dume ankaŭ kontrolas la subskribon.)

5. Ni rigardas la eron el voĉdono nepersona kun $\text{id}^*_{(u,p)}$. Ni tie ankaŭ malkriptigas la parton por voĉdonanto, kontrolas la subskribon kaj komparas la valorojn kun tiuj el la lasta paŝo.

6. Ni komparas la donitan voĉon kun tiu en la ppor publikigo-parto.

7. Se ĉio estas en ordo, ni metas tiun informon en la kontrolita-parton de la voĉo persona-tabelo, kun dig_p kaj subskribo de ambaŭ.

Kiam sufiĉe da homoj kontrolis kaj konfirmis siajn voĉojn (t.e. la kvanto de homoj, kiuj ne kontrolis, estis malpli ol la diferenco inter »Jes« kaj »Ne«), ni povas deklari la rezulton definitiva.