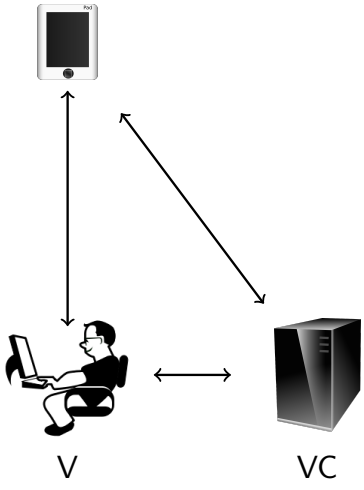
Elliptkõverad ja postkvant-krüptograafia

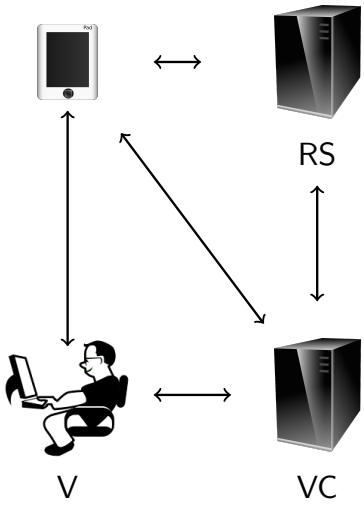
Jan Willemson

28. oktoober 2024

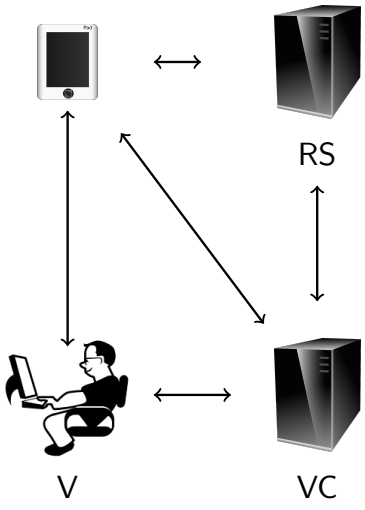
Eesti i-hääletamise protokoll IVXV 2017-. . .

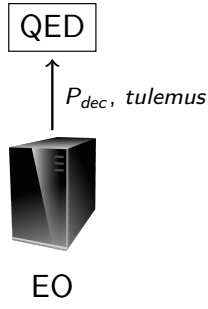


Eesti i-hääletamise protokoll IVXV 2017-. . .

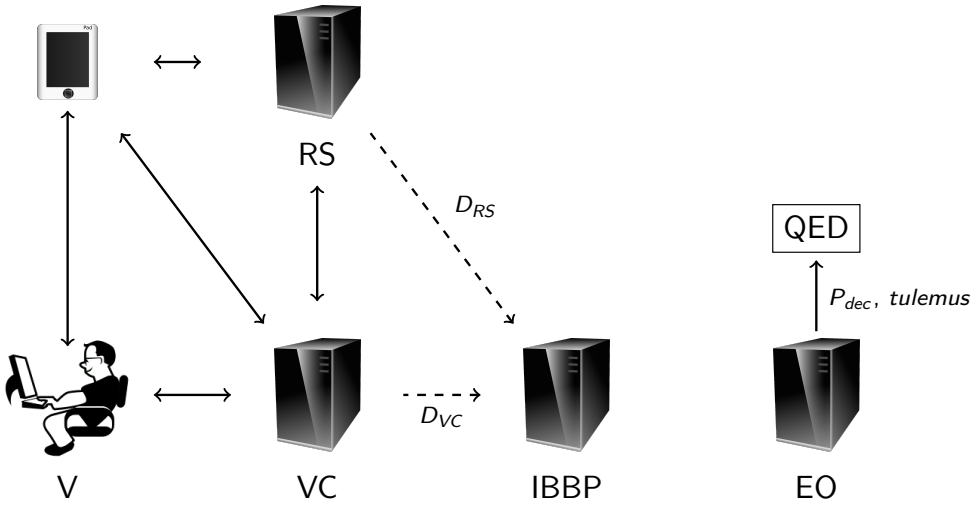


Eesti i-hääletamise protokoll IVXV 2017-. . .

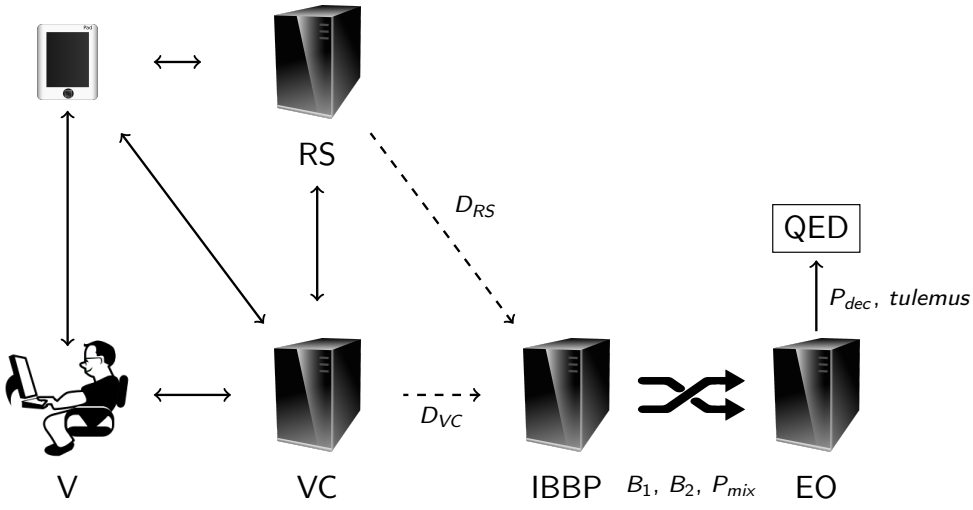




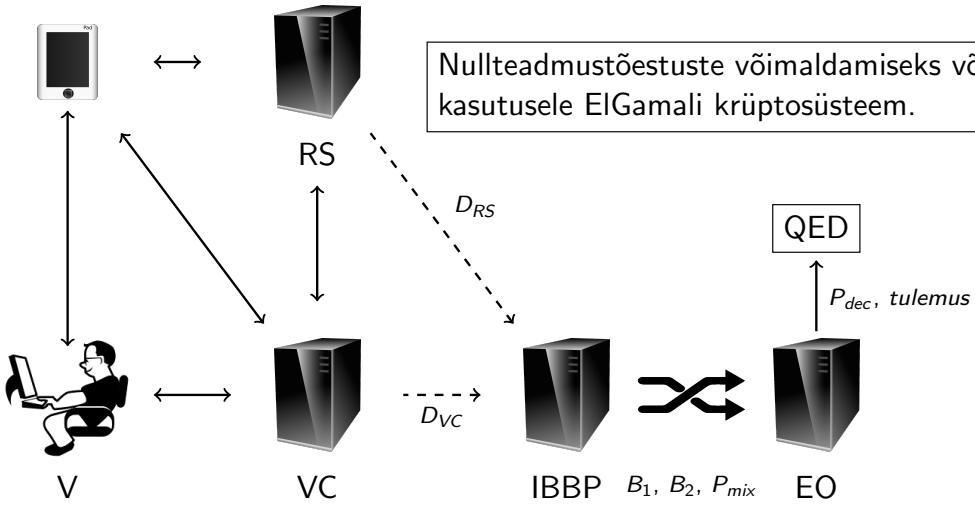
Eesti i-hääletamise protokoll IVXV 2017-...



Eesti i-hääletamise protokoll IVXV 2017-. . .



Eesti i-hääletamise protokoll IVXV 2017-. . .



Natuke matemaatikat

- Praegu kasutab IVXV ElGamali krüptosüsteemi, mis kasutab jäägiga arvutamist modulo 3072-bitine algarv

$$
\begin{aligned}
p = {} & 2^{3072} - 2^{3008} - 1 + 2^{64} \cdot ([2^{2942} \cdot \pi] + 1690314) = \\
= {} & 5809605995369958062791915965639201402176612226902900533702900882779736177890990861472094774477339581147373410185646378 \\
& 3280437298007504700982109244878669350591643715881680475409439816445166327550675016264345563981931866289900712486608193 \\
& 6120511979369398543329703611823291441017187680753645739127785701184989741020751910533335580112110935689745942627184547 \\
& 1397952675959440793493071628394122780510124618488232602464 6
\end{aligned}
$$

Natuke matemaatikat

4987685045886124578424092925842628769970531258450962541951346360515542801716571446536309402160929056108402589366256122257320208286579782186527099114508220065697817719282702453899023996917554619077064568589343801171443042640933867631474357115453714203157300427642870143303638180170530865983075119035294602548205993130657100472736247968841557470259694645777028414843598912963285391839211799747263269307811312988648739934779698277278461586523262128965694428421682461131870976453515250735411634470376999851414834380 7

Probleem: mittestandardsed sedelid

- Kui minu rehkendus on õige, on Eesti i-hääletamise ajaloos olnud 6 mittestandardset sedelit:
  - 2011
  - 2013
  - 2015
  - 2021
  - 2024 (2 tk)
- 2024. aastal jõudis üks mittestandardne sedel ka dekrüpteerimisfaasi.
- Mittestandardse sedeli esitamiseks peab hääletaja kasutama mitteametlikku valijarakendust.

Miks mittestandardsed sedelid pahad on?

- Nende abil saab mõjutusründaja näiteks sundida valijat oma häälest loobuma, kui sedel kehtetuks kuulutatakse.
  - See rünne on ka põhjuseks, miks dekrüpteerimistõestusi P_{dec} ei saa hetkel päris avalikuks teha.
- Teaduskirjanduses on välja pakutud veel mõned ründed:
  - Saladuste lekitamine mittestandardse sedeli abil.
  - Mitme hääle salajasuse leke ühe krüptogrammi kaudu.

Miks mittestandardsed sedelid pahad on?

- Nende abil saab mõjutusründaja näiteks sundida valijat oma häälest loobuma, kui sedel kehtetuks kuulutatakse.
  - See rünne on ka põhjuseks, miks dekrüpteerimistõestusi P_{dec} ei saa hetkel päris avalikuks teha.
- Teaduskirjanduses on välja pakutud veel mõned ründed:
  - Saladuste lekitamine mittestandardse sedeli abil.
  - Mitme hääle salajasuse leke ühe krüptogrammi kaudu.
- Lisamärgetega sedelite abil saab paberhääletamise puhul mõjutusründeid väga lihtsasti korraldada!

Mida teha?

- Häältekogumisserver ei näe krüptogrammi alla ega saa sedeli korrektsust vahetult kontrollida.

Mida teha?

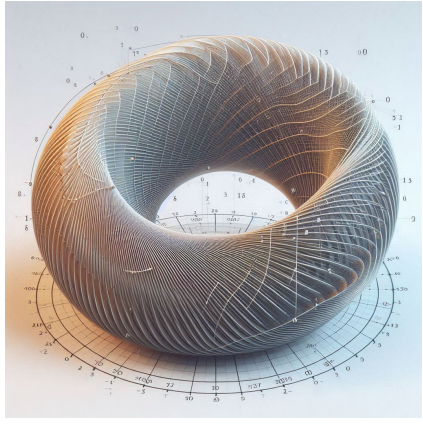
- Häältekogumisserver ei näe krüptogrammi alla ega saa sedeli korrektsust vahetult kontrollida.
- Valijarakendust (sh valija enda kirjutatut!) saab sundida andma **nullteadmustõestust**, et krüptogrammi all on üks standardsetest sedelitest.
  - Erinevalt paberhääletamisest saab mittestandardset sedelit kasutavad ründed i-hääletamise puhul täielikult neutraliseerida!

Mida teha?

- Häältekogumisserver ei näe krüptogrammi alla ega saa sedeli korrektsust vahetult kontrollida.
- Valijarakendust (sh valija enda kirjutatut!) saab sundida andma **nullteadmustõestust**, et krüptogrammi all on üks standardsetest sedelitest.
  - Erinevalt paberhääletamisest saab mittestandardset sedelit kasutavad ründed i-hääletamise puhul täielikult neutraliseerida!
- Võimalikke sedeleid on küll piiratud arvul, kuid siiski üsna palju (tüüpiliselt paarkümmend, maksimaalselt paarsada).
- 3072-bitise ElGamali puhul tuleks tõestused üsna suured ning nende kontroll suhteliselt aeglane.
  - Üks tõestus $\approx$ 30kB.
  - 300000 tõestust $\approx$ 9GB.

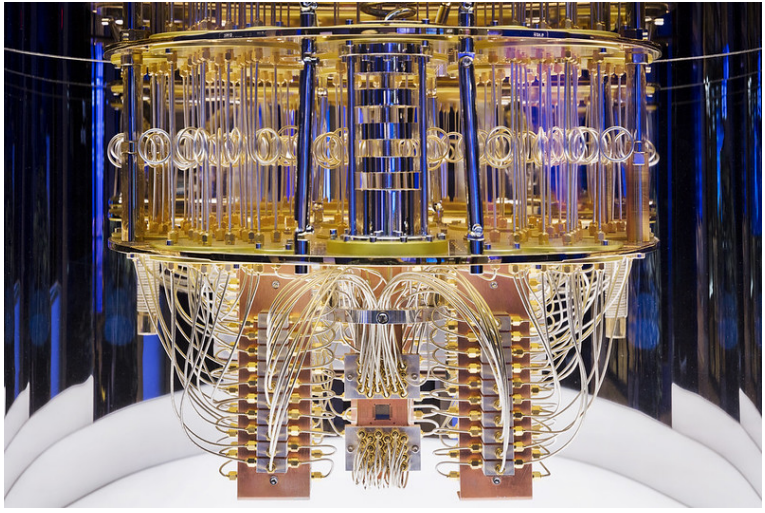
Lahendus: elliptkõverate krüptograafia

- Krüptogrammid ja tõestused tulevad väiksemad
  - Üks tõestus $\approx$ 5kB.
  - 300000 tõestust $\approx$ 1,5GB.
- Arvutamine on kiirem.
- QR-kood tuleb väiksem.
- Eesti ID-kaart ja mobiil-ID kasutavad elliptkõveraid.
- Pärast sedelite nullteadmustõestuste lisamist saab dekrüpteerimistõestused kõigile auditeeritavaks teha.



Pildi autor: DALL-E 3

Kvantarvuti



Pildi allikas: IBM

Mis kvantarvuti ilmudes õieti juhtuks?

- Väga Võimas Kvantarvuti suudaks põhimõtteliselt murda praegust avaliku võtme krüptograafiat.
- See nõuaks endiselt palju ressurssi, hinnanguliselt umbes
  - sadu päevi arvutamiseks ja
  - miljoneid elektriarve maksmiseks,

  aga see oleks kiirem ja odavam kui klassikalise arvutiga.

Mis juhtuks i-hääletamisega?

- Digiallkirjade võltsimine tähendaks miljonitesse ulatuvat kulu iga allkirja kohta.
  - Sellel ründel oleks ülipiiratud mõju, sest ta ei skaleeru.

Mis juhtuks i-hääletamisega?

- Digiallkirjade võltsimine tähendaks miljonitesse ulatuvat kulu iga allkirja kohta.
  - Sellel ründel oleks ülipiiratud mõju, sest ta ei skaleeru.
- Häälte krüpteerimisvõtme murdmine võimaldaks avada korraga kõik hääled.
  - Hääletamistulemuse korrektsus ja terviklus oleks endiselt tagatud.
  - Salajasuse riivet saab kasutada mõjutusrünnetes, nt massiliseks tagakiusamiseks poliitiliste eelistuste pärast.
  - Kui meie inimesed peavad kartma massilist tagakiusamist, on meil ühiskonnas juba suuremaid probleeme.
  - *Salvesta-praegu-dekrüpteeri-hiljem* tüüpi ründed on põhjus, miks krüpteeritud ja signeeritud hääli ei saa avalikuks auditeerimiseks välja anda.

Parem karta kui kahetseda

- 2024. aasta augustis standarditi esimesed postkvant-digiallkirjaskeemid ja niipea, kui eID-rakendused neid tunnistama hakkavad, saame need ka i-hääletamisel kasutusele võtta.
- Krüpteerimisskeemilt nõuame spetsiifilisi omadusi (nt nullteadmustõestuste võimaldamist).
- Standarditud meetodid ei saa neid omadusi ilmselt kunagi pakkuma, seega siinkohal tuleb ise teadust teha.

Tänan!

- Küsimusi?