EVOTEID 2025
INTERNATIONAL CONFERENCE

Removing Insiders' Trust from The Estonian Internet Voting System

(an OSCE/ODIHR point#10 concern)

Shymaa M. Arafat

Associate Professor (Independent, https://github.com/DrShymaa2022)
shar.academic@gmail.com, shymaa.arafat@gmail.com

IVXV trust assumption: *the Vote Collector (VC) & the Registration Service (RS) are not to collude together*.

We propose two alternative solutions:

1- Use different ZKP queries and/or statistical techniques (like RLAs samples) to *check the consistency of multiple sources of information that already exists in the Estonian government*; i.e., digital IDs activity logs like *myID* service.

Verify:

-Count (original votes file) =

Count_Transactions (source=all, destination=IVXV, time=election_interval)

-(original votes file) =

Transactions (source=all, destination=IVXV, time=election_interval)

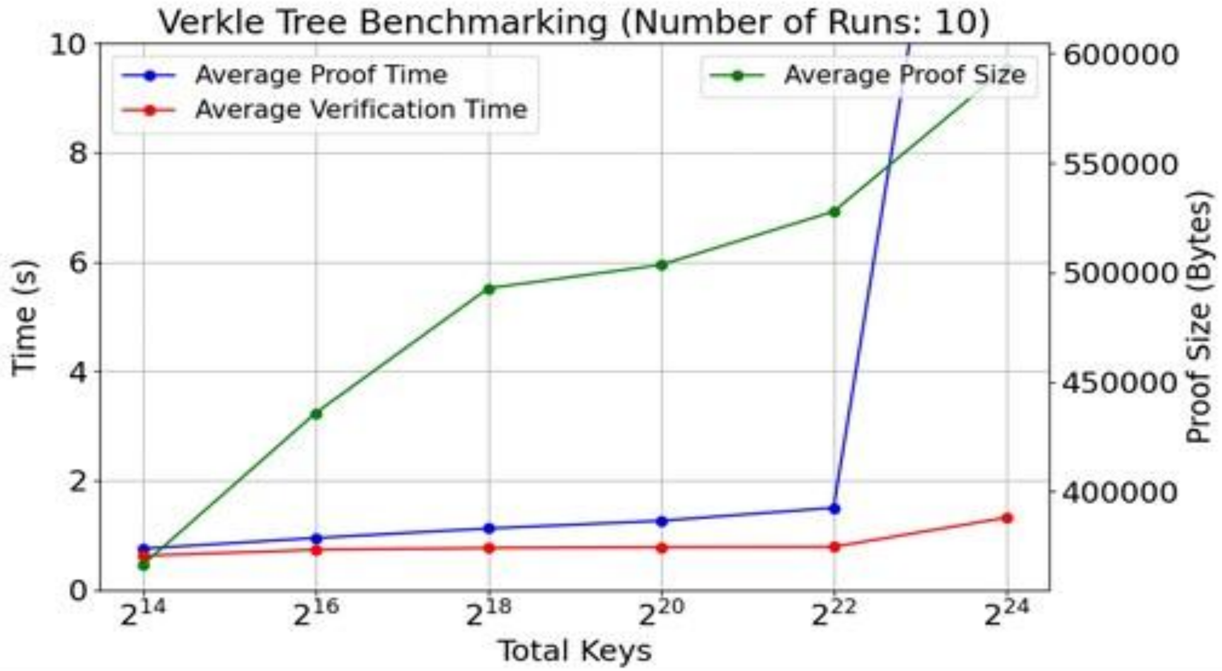
2- *Aggregate votes online in an Authenticated Data Structure that cryptographically proves the number of values* **stored in it (the number of votes in our case); we suggest the use of Verkle Trees**

- $\{VT=VT+H[i] * committed\_vote; i{+}{+};\}$, where the vector H is calculated in the setup phase and τ secrecy is critical
- $H_0= G, H_1=\tau\bullet G, H_2=\tau^2\bullet G, \ldots, H_{p-1}=\tau^{(p-1)}\bullet G$

fast proof generation as benchmarked

~ 1 second for n < 2^{22}~ 4 million

(on Windows Intel i5-4690K, 22GB)


Verkle Tree Benchmarking (Number of Runs: 10)
Average Proof Time
Average Verification Time
Average Proof Size
Time (s)
Proof Size (Bytes)
2^{14}
2^{16}
2^{18}
2^{20}
2^{22}
2^{24}
Total Keys