EVOTeID2025
INTERNATIONAL CONFERENCE

Achieving Court Verifiability without Expert Knowledge While Maintaining Coercion Resistance

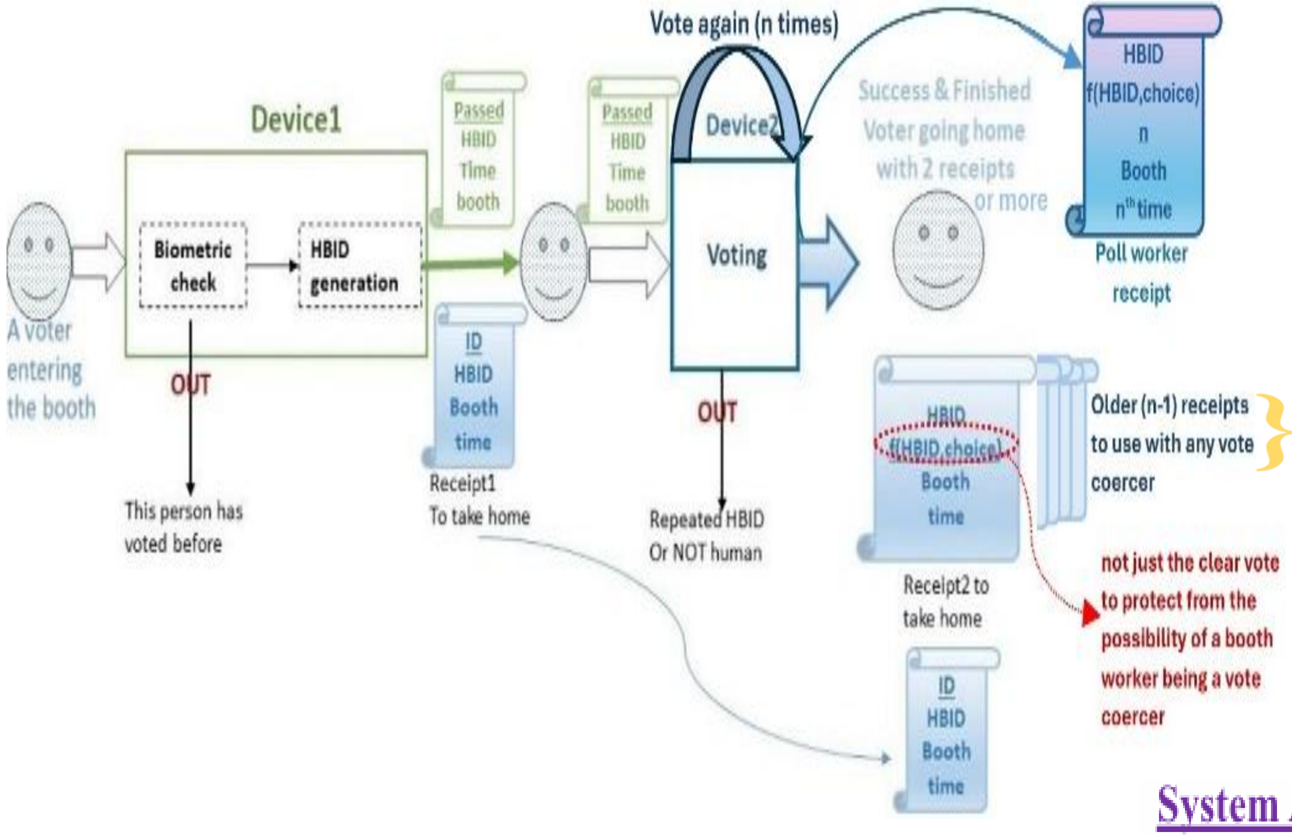
A (2 Devices) and (3+ Receipts) in-booth e-voting system

Shymaa M. Arafat

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

Receipt 1
Receipt 2
Sealing receipt
Poll officer
Voter

Old 2 receipt
Voter
Coercer / Buyer
final
2


Vote again (n times)

A voter entering the booth

Device1

Biometric check

HBID generation

OUT

This person has voted before

Passed HBID Time booth

Passed HBID Time booth

ID HBID Booth time

Receipt1 To take home

Device2

Voting

OUT

Repeated HBID Or NOT human

Success & Finished Voter going home with 2 receipts or more

HBID f(HBID,choice) n Booth n^th time

Poll worker receipt

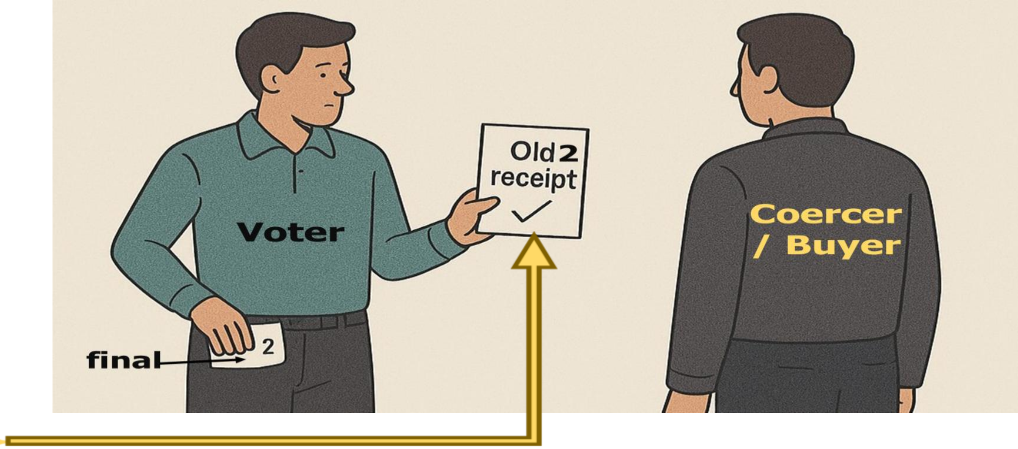
HBID f(HBID,choice) Booth time

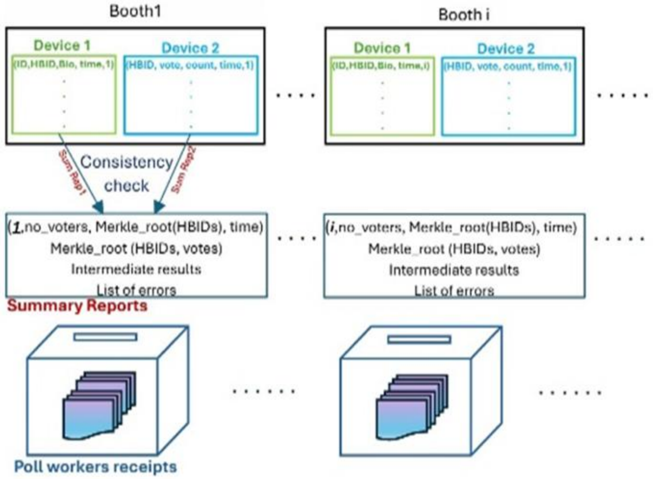
Receipt2 to take home

Older (n-1) receipts to use with any vote coercer

not just the clear vote to protect from the possibility of a booth worker being a vote coercer

ID HBID Booth time




Booth1

Device 1

(ID,HBID,Bio, time,1)

Device 2

(HBID, vote, count, time,1)

Booth i

Device 1

(ID,HBID,Bio, time,i)

Device 2

(HBID, vote, count, time,1)

Sum Rep1

Consistency check

Sum Rep2

(1,no_voters, Merkle_root(HBIDs), time)
Merkle_root (HBIDs, votes)
Intermediate results
List of errors

(i,no_voters, Merkle_root(HBIDs), time)
Merkle_root (HBIDs, votes)
Intermediate results
List of errors

Summary Reports

Poll workers receipts

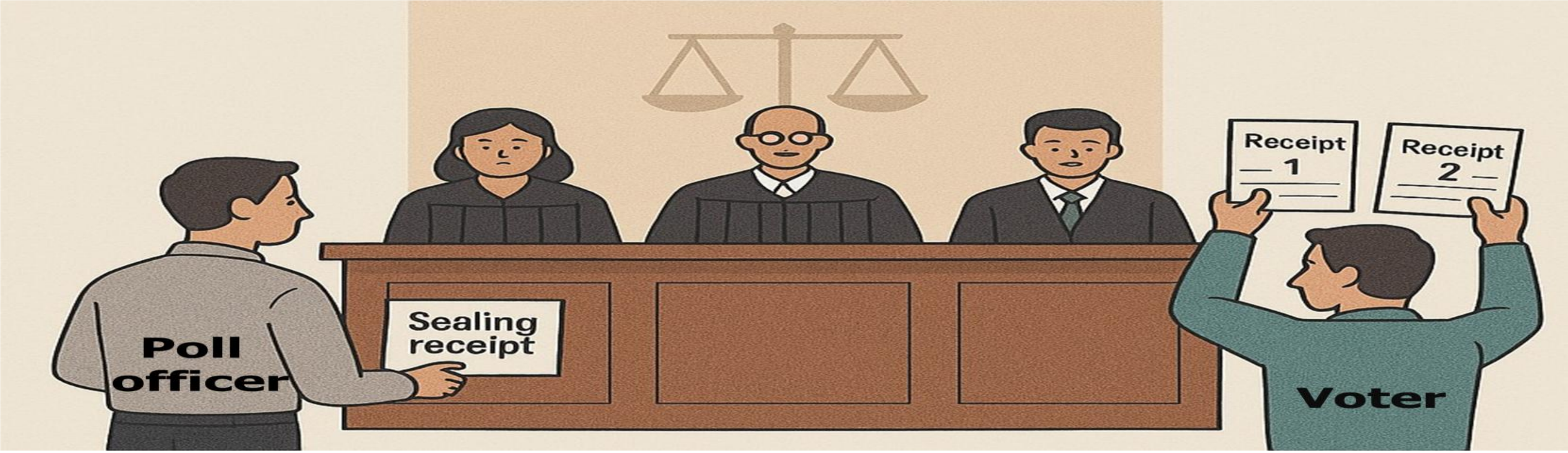
Results on Public Bulletin Board

(Booth, time, vote, no_mult_votes)

.
.
.
.
.
.
.
.

System Assumptions: HBID is unbreakable, receipts cannot be forged, device2 never prints 2 sealing receipts for the same HBID

Malicious Entity	System Defense
Device 2	Benaloh Challange
Device 1 & Device 2	Summary reports, RLAs, consistency checks
Public Bulletin Board (PBB)	Clash attacks and alike not applicable; PBB doesn't know the checking voter (identify with time & booth)
Election Authority (EA)	Trusted in privacy, voters' receipts+summary reports protect integrity
Poll Officers	The linear function + auditors + RLAs



Court Verdict in each possibility

(If a candidate brought a group of voters, RLA ratios could be applied)

Voter EA	*“I can’ find my vote in PBB”*, **OR** *“I didn’t vote, but Non-inclusion Proofs says I did”*
EA submits a sealing receipt and voter’s whole record with signature/authentication supporting their claim	Malicious Voter
No sealing receipt supports EA claim (contradicts or does not exist)	Falsify election in this interval in this booth
EA claims lost receipt	Their Responsibility, rule for voter
EA doesn’t show up in court	Assumed guilty, rule for voter
EA claims “an error in non-inclusion proofs, we agree this voter did not vote”	Perform a manual recount in the specified booth & interval