Anonymized version of the Poster (published 2025) with author name and conference details omitted

Achieving Court Verifiability without Expert Knowledge While Maintaining Coercion Resistance

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

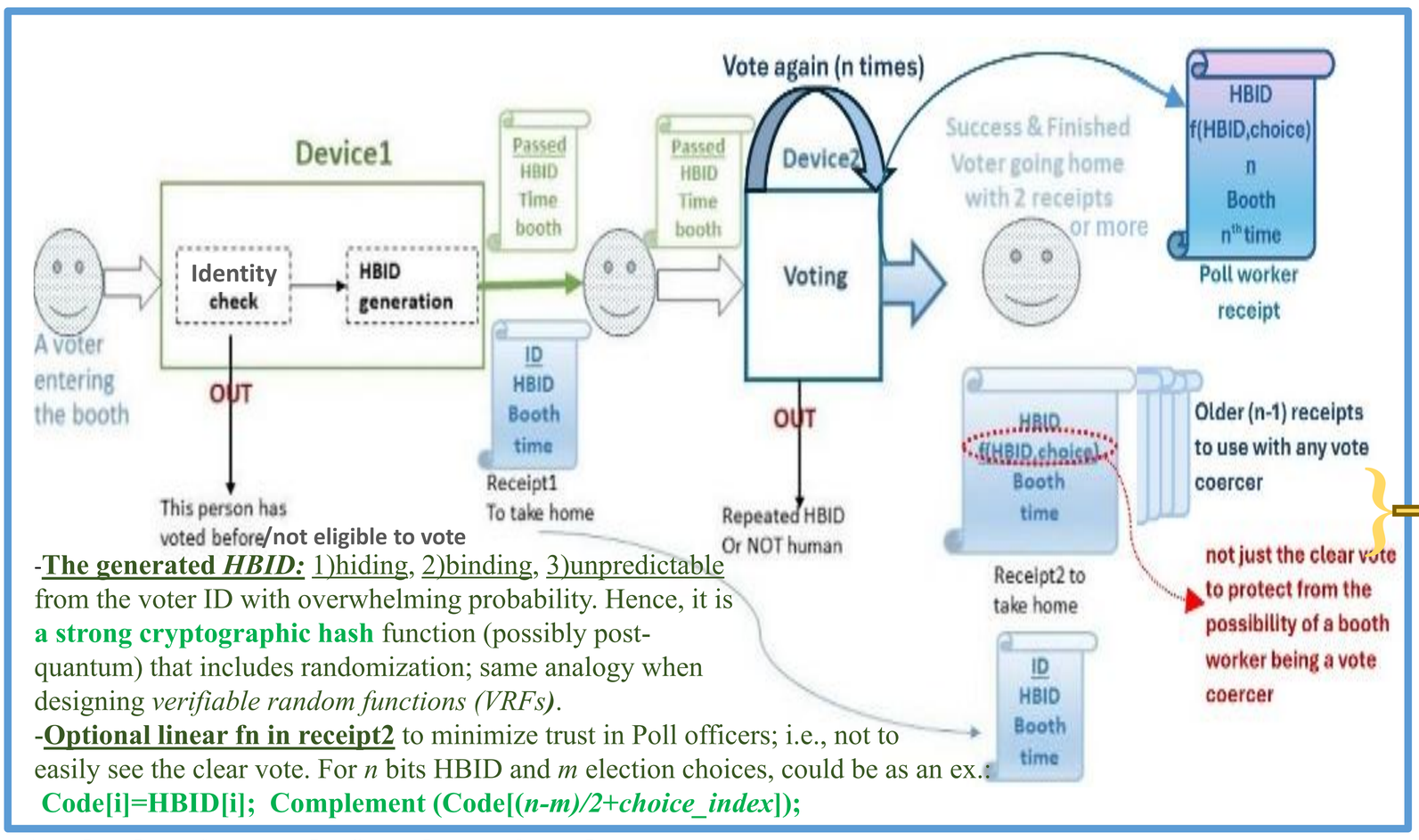
The conference did not publish a book of abstracts for the posters. Hence, the author does not find a problem of publishing the full paper with detailed analysis using the same title

Constitutional German Court finds cryptographic proofs "*somewhat untenable as a verification*" since they require expert testimony

An e-voting system that allow any voter, or a group of voters (ex.: a losing candidate with a group of supporters), to challenge the voting system in court (without expert testimony), and yet remains coercion resistant.

We use printed receipts with tracking codes, then make *Benaloh Challenge* serve 2 purposes: 1)detect malicious devices & 2) deceive vote buyers/ coercers by printing receipts for the trials, while *the sealing receipt* guarantees judges do not fall in the same trick

The proposed system uses 2 devices; the first device authenticates the voter and prints a receipt with a unique cryptographic ID code (*HBID*) for each voter. The second is a voting device that permits successive multiple voting and prints *a receipt for each voting attempt*, then prints *a sealing receipt for poll workers with enough information to identify the voter's final receipt*. We advise to include "*Boycott*" & "*Reject All*" options to avoid absent voting and have a complete protection from coercers. We suggest to *hide the printed vote inside a simple function* as an optional safeguard from coercion by poll workers who will take the distinguishing receipt); although it is supposed to be fast & easy for the average person to get the vote from the simple function in the receipt, it would be time consuming and noticeable if poll workers did it inside the poll station for all voters. We then *publish per booth summary reports every fixed interval* to serve as check points and to be used by RLAs and ZK queries as well. Finally, election *result is published in a Public Bulletin Board as records (booth, time, vote, no of votes)* to anonymize it from adversaries.



-**The generated *HBID:*** 1)hiding, 2)binding, 3)unpredictable from the voter ID with overwhelming probability. Hence, it is **a strong cryptographic hash** function (possibly post-quantum) that includes randomization; same analogy when designing *verifiable random functions (VRFs)*.

-**Optional linear fn in receipt2** to minimize trust in Poll officers; i.e., not to easily see the clear vote. For *n* bits HBID and *m* election choices, could be as an ex.:

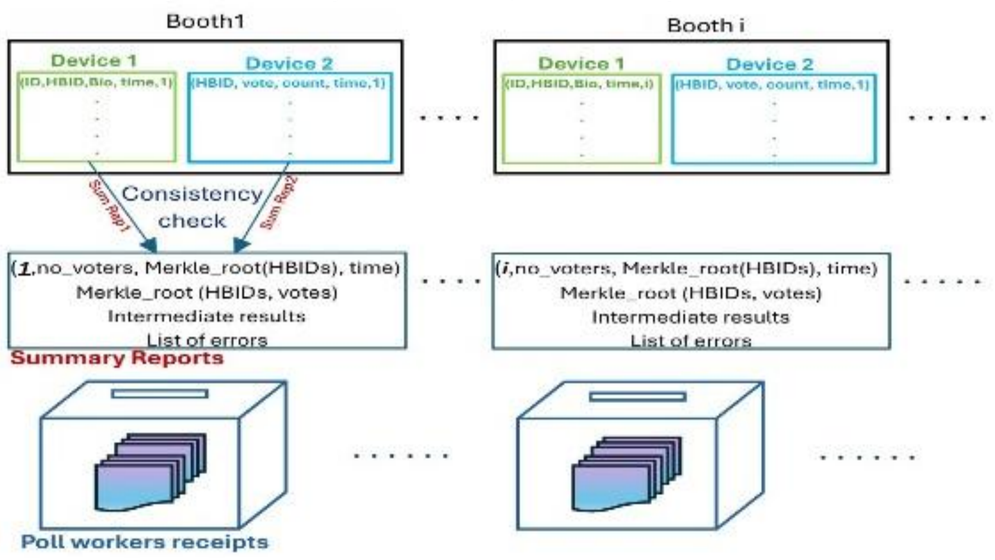
Code[i]=HBID[i]; Complement (Code[(*n-m)/2+choice_index*]);

The vote buyer/coercer has no way of knowing whether it is the final receipt or not *unless colluded with poll officers;* however, such collusion cannot be automated or on large-scale, must be on a vote-by-vote basis.

At check points and after the voting closes:

Each device prints cryptographic checksums of its data for auditors and poll officers to *check consistency of data* from both devices & consolidate them in *a mutually signed* summary report. Risk Limiting Audits (RLAs) can be performed, errors should be listed.

The result is uploaded to a public bulletin board (PBB) as *(booth, time, choice, no of votes)*; voters identify their votes by time & booth, coercers only calculate no. of voters who deceived them as the no. of unmatching receipts.



Results on Public Bulletin Board

(Booth, time, vote, no_mult_votes)
.
.
.
.
.

The court on the other hand can check the Poll worker receipt to know if the voter is lying (submitting an old receipt) or saying the truth.

+ Judges also have *Public Bulletin Board* & *Summary reports* as other sources of information.

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)

EA \ Voter	"*I can't 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