EVOTEID 2025 INTERNATIONAL CONFERENCE
Tenth International Joint Conference on Electronic Voting
1-3 October 2025 - Nancy, France

Achieving Court Verifiability without Expert Knowledge While Maintaining Coercion Resistance

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

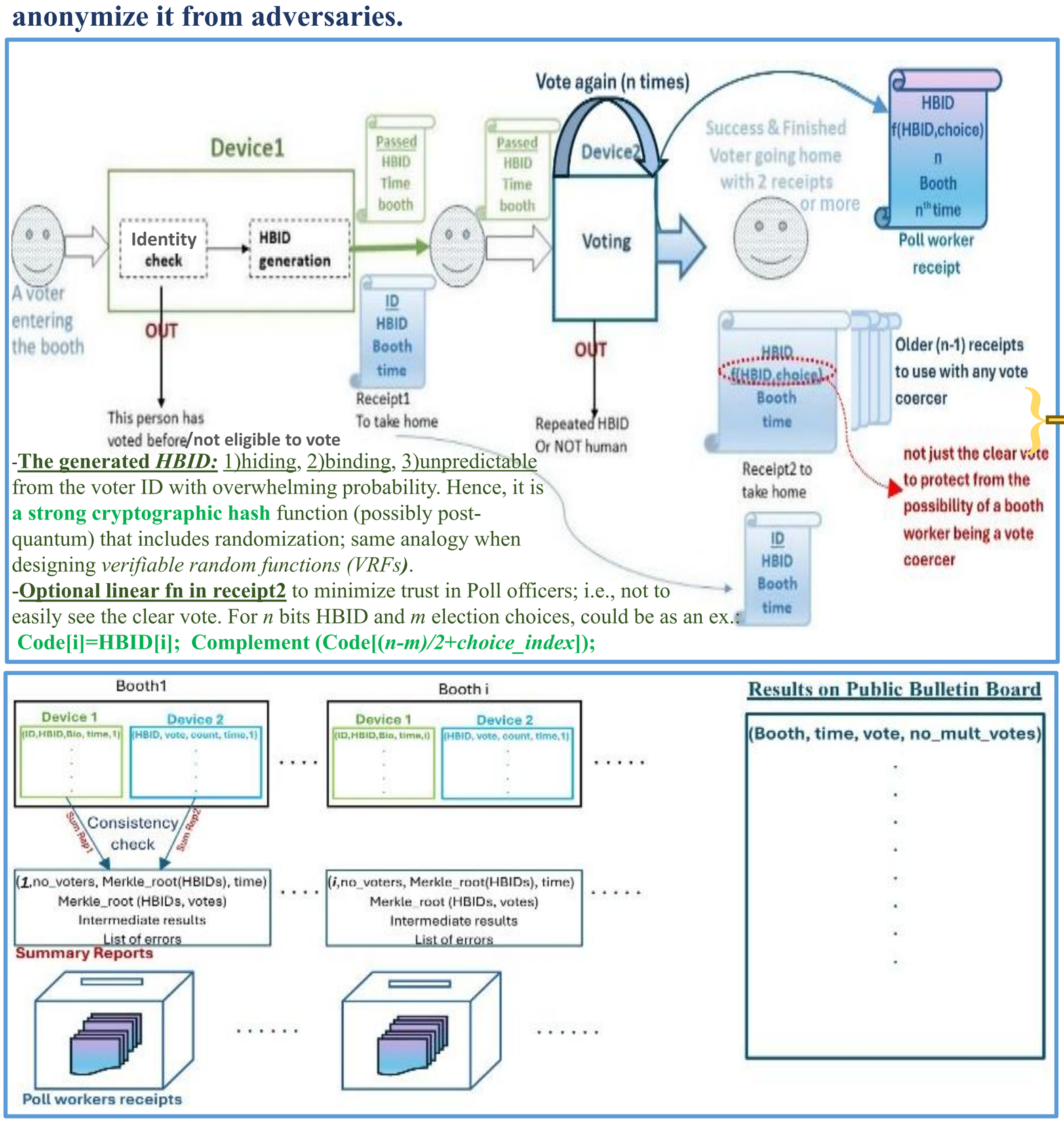
Shymaa M. Arafat
Associate Professor (Independent, https://github.com/DrShymaa2022)
shar.academic@gmail.com, shymaa.arafat@gmail.com

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 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.

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.

At check points and after the voting closes:

1. **Each device prints cryptographic checksums of its data for auditors and poll officers to *check the consistency of data from both devices and consolidate them in a summary report*. Then all of them *sign the summary report either manually in a public document or by their public keys to a public Blockchain* containing (booth ID, date & time of session, no of voters, no of votes,...); the number of voters should be also checked against handwritten signatures totals. Risk Limiting Audits (RLAs) can be performed by cryptographically verifying the correct corresponding data of sampled poll workers receipts in both devices. If errors were found, they should be listed.**
2. **Poll workers deliver memory cards from both devices and the sealing receipts box to the election authority.**
3. **The election authority aggregates all memory cards in a voting server which will conduct more consistency checks on the whole data.**
4. **When the voting server completes the counts, the election result is uploaded to a public bulletin board in the form *(booth, time, choice, no_of_votes)*; since it is impossible for 2 votes to have the same exact time and booth, any voter can identify his/her vote in the Public Bulletin Board, while adversaries can at maximum figure the ratio of those who deceived them when not finding the exact time in the receipts they took.**

Cite as:
Shymaa M. Arafat, "*Achieving Court Verifiability without an Expert Knowledge while Maintaining Coercion Resistance*", E-Vote-ID 2025, Track-4 Posters and Demos, 10th International Conference on Electronic Voting, 1-3 Oct 2025, Nancy France.

See the paper preprint with all the references in:
https://github.com/DrShymaa2022/articles_papers/blob/main/courtverify_EVoteID_final.pdf