Description of the Properties that a Secure E-Voting System Should Satisfy

A secure e-voting system should be designed to uphold the following properties:

- *coercion resistance* (CR) [4]: voters cannot prove whether or how they voted, even if they can interact with the adversary while voting;
- *eligibility verifiability* [1,7], which we divide for a more precise analysis into two properties that anyone should be able to verify:
  - EV1: all valid votes have been cast by eligible voters;
  - EV2: all valid votes have been cast by distinct voters.
- *correctness* (CO) [4]: an adversary cannot preempt, alter, or cancel the votes of honest voters;
- *fairness* (FA) [2]: no information about how many votes each candidate has received can be learned until the voting results are published;
- *vote privacy* (VP) [8]: no one is able to know the content of a vote;
- *coercion resistance* (CR) [4]: voters cannot prove whether or how they voted, even if they can interact with the adversary while voting;
- individual verifiability, which is subdivided into:
  - *cast-as-intended verifiability* (CAIV) [3]: the voter can verify that the complete ballot (i.e. containing the intended vote) is correctly computed and cast;
  - *recorded-as-cast verifiability* (RACV) [5]: the voter can verify that the correct ballot is recorded for the tallying;
  - *tallied-as-recorded verifiability* (TARV) [6]: anyone can verify that all and only the recorded votes are tallied, and with the correct procedure;
- *universal verifiability* (UV) [8]: anyone can check that the published result of an election has been correctly computed;
- *eligibility verifiability* [1,7], which we divide for a more precise analysis into:
  - EV1: anyone can verify that all valid votes have been cast by eligible voters;
  - EV2: anyone can verify that all valid votes have been cast by distinct voters.
- *right to vote* (RTV) - eligible voters are able to cast valid vote;
- *successful completion* (SC) - the election process reaches the end, publishing the result of the tallying.

References

1. Cortier, V., Gaudry, P., Glondu, S.: Belenios: a simple private and verifiable electronic voting system. In: Foundations of Security, Protocols, and Equational Reasoning, pp. 214–238. Springer (2019)
2. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

3. Escala, A., Guasch, S., Herranz, J., Morillo, P.: Universal cast-as-intended verifiability. In: International Conference on Financial Cryptography and Data Security. pp. 233–250. Springer (2016). https://doi.org/10.1007/978-3-662-53357-4_16
4. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Towards Trustworthy Elections, Lecture Notes in Computer Science, vol. 6000, pp. 37–63. Springer (2010). https://doi.org/10.1007/978-3-642-12980-3_2
5. Müller, J., Truderung, T.: Caised: A protocol for cast-as-intended verifiability with a second device. In: International Joint Conference on Electronic Voting. pp. 123–139. Springer (2023)
6. Popoveniuc, S., Kelsey, J., Regenscheid, A., Vora, P.: Performance requirements for End-to-End verifiable elections. In: 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 10). USENIX Association, Washington, DC (Aug 2010), https://www.usenix.org/conference/evtwote-10/performance-requirements-end-end-verifiable-elections
7. Smyth, B., Ryan, M., Kremer, S., Kourjieh, M.: Towards automatic analysis of election verifiability properties. In: Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security. pp. 146–163. Springer (2010). https://doi.org/10.1007/978-3-642-16074-5_11
8. U.S. Election Assistance Commission: Voluntary Voting System Guidelines (VVSG) version 2.0 (02 2021), https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines