SoK: Secure E-voting with Everlasting Privacy

Rafieh Mosaheb

SnT, University of Luxembourg, rafieh.mosaheb@uni.lu

Abstract. In this work, we systematically analyze all e-voting protocols designed to provide everlasting privacy. Our main focus is to illustrate their relations and to identify the research problems which have or have not been solved in this area.

Keywords: electronic voting · everlasting privacy · protocol analysis.

1 Introduction

In all elections, it is crucial to ensure that the final election result correctly reflects the votes chosen by the voters. Moreover, voters' individual votes must remain secret so that the final result is not biased by those who are afraid to express their own will freely. In order to guarantee these two fundamental properties, modern *secure* e-voting protocols strive for (end-to-end) verifiability and (vote) privacy. In order to guarantee verifiability, some information about the voters' individual choices needs to be public. Since, at the same time, vote privacy must not be jeopardized, essentially all verifiable e-voting systems used in practice today (e.g., Helios [8] or Belenios [3]) employ the following approach: voters encrypt their votes under the talliers' public key, publish the resulting ciphertexts, and the talliers use their secret key to process these ciphertexts to obtain the final result. Now, the problem is that secrecy of all public-key encryption schemes deployed in these systems (e.g., ElGamal) is based on certain computational hardness assumptions (e.g., decisional Diffie-Hellman) that ensure vote privacy at the time of the election, but not necessarily in the long run. A future adversary, who learns from public data of past elections which ciphertext belongs to which voter, may therefore exploit novel (previously unknown) algorithms or more powerful machines (e.g., quantum computers) to efficiently solve the underlying hardness assumptions and thus break privacy of voters retrospectively. As explained above, such a risk is unacceptable for many real-world elections.

Fortunately, in order to ensure that vote privacy remains preserved in the future, numerous e-voting protocols have been proposed in the academic literature (e.g., [1, 2, 9, 10, 4]). These protocols strive for what is called *everlasting privacy*. This property ensures that privacy is protected *unconditionally* so that even a computationally unbounded adversary is not able to learn how individual voters voted. Most of the e-voting protocols mentioned above actually aim for a weaker notion of everlasting privacy. In fact, these protocols are designed to

guarantee unconditional privacy towards any external adversary who can access all public election data but who is not able to monitor the whole communication network. This relaxed notion of everlasting privacy is called *practical everlasting privacy* [5]. It accurately models the overall threat scenario of a future adversary who knows all public material required to verify an election and who is able to break any computational hardness assumption.

In the next sections, we explain our methodology and then describe our key findings.

2 Methodology

We use the following approach to systematically analyze the state-of-the-art in secure e-voting with everlasting privacy:

1. We study the academic literature to find all relevant existing protocols in this field.
2. We classify existing protocols according to how they (intend to) provide everlasting privacy technically. Moreover, we illuminate how different protocols depend on each other.
3. We analyze which existing protocols are practically efficient and guarantee public verifiability as well as (practical) everlasting privacy under realistic assumptions. To this end, we investigate which protocols actually achieve the properties they were designed for originally, and we critically reflect on the assumptions that existing protocols make.
4. Based on our analysis in the previous steps, we identify which research problems have already been solved and which ones are still open.

We collected 25 existing e-voting protocols designed for secure e-voting with everlasting privacy, however, for the sake of limited space we refer interested readers to the full paper.

3 Our Classification

We propose a classification that captures all existing e-voting protocols aiming for everlasting privacy. We identify two different classes of existing protocols, B-ANON and B-ID. In B-ANON, everlasting privacy reduces to publishing ballots anonymously. On the contrary, in B-ID, where public ballots are identifiable, everlasting privacy is based on the privacy-preserving technique to tally ballots. We argued in the full paper that the general approach taken in B-ID is superior to the one in B-ANON; in short: B-ID $>$ B-ANON. We observe that the two main classes B-ANON and B-ID essentially differ in two aspects: (1) the method used to ensure everlasting privacy as well as the phases when the respective method is applied, and (2) the technique employed to guarantee public verifiability.

4 Solved and problems

4.1 Solved problems

We discover that in both classes, B-ID and B-ANON, there exist reasonable protocols for secure e-voting with everlasting privacy under the respective assumptions made in these classes. For everlasting privacy, all of these protocols consider future adversaries that are not active during an election. We distinguish between those protocols that can handle simple ballot types (e.g., where voters can choose one candidate) and those which can handle arbitrary ballot types (e.g., where voters can rank candidates).

Observation 1 (Simple ballot types) *In B-ID, there exist two secure approaches that can handle simple ballot types: the one based on [1] and the one based on the homomorphic version of [2]. While [2] offers everlasting privacy towards the public (i.e, practical everlasting privacy), [1] additionally offers everlasting privacy towards a threshold of talliers.*

Observation 2 (Arbitrary ballot types) *In B-ID, there exists one secure approach that can handle arbitrary ballot types, the one based on the mix net version of [2]. In B-ANON, there exist two reasonably secure approaches that can handle arbitrary ballot types [3, 4]. These protocols offer practical everlasting privacy.*

All of the approaches mentioned before are sufficiently efficient for large-scale elections. In particular, Belenios [3] has already been deployed in many real-world elections.

4.2 Open problems

The most important open problems are:

1. *Formal protocol analysis:* While the cryptographic components of the promising approaches [1, 2, 4] have been analyzed in-depth, it is an open problem to formally analyze these proposals on the *protocol* level. It is also an open problem to formally analyze everlasting privacy of Belenios [4].
2. *Deployable e-voting system:* While Belenios [3], which is in B-ANON, can be deployed for real-world elections, it is an open problem to develop a full-fledged deployable e-voting system that realizes one of the promising approaches [1, 2] in the superior class B-ID.
3. *Weaker trust for arbitrary ballot types:* All promising approaches that can handle arbitrary ballot types [2, 4, 3] require that all election authorities or all talliers are trusted for everlasting privacy. It is an open problem to mitigate trust on the authorities in terms of everlasting privacy for arbitrary ballot types.
4. *Receipt-freeness:* In all of the promising approaches [1, 2, 4, 3], some evidence is created on the voters' devices that can serve as a proof for how the voter voted. It is an open problem to securely and efficiently improve [1, 2, 4, 3] so that they are free of such receipts.

From our point of view, the first two open problems (formal protocol analysis and development of a deployable system in B-ID) are the most pressing ones. We note that for automated verification, there exist appropriate symbolic definitions to address the first open problem, for example [5] for everlasting privacy and [6] for verifiability/accountability; recent advances [7] facilitate applying these definitions in a joint verification platform.

5 Conclusion

We demonstrated that there exist four promising approaches [1, 2, 4, 3] among the numerous proposals for secure e-voting with everlasting privacy. These solutions offer the potential to guarantee everlasting privacy in real elections. These approaches significantly differ in the assumptions that they need to make for everlasting privacy. While [4, 3] need to assume that voters submit their ballots anonymously, the other two approaches can avoid this often unrealistic assumption. Therefore, [1, 2] are preferable whenever distributing the trustee is feasible.

We identified two important open problems, one of theoretical and the other one of practical nature. First, it is fundamental to formally analyze the security of all promising protocols [1, 2, 4, 3]. Second, it is desirable to realize the two strongest proposals [1, 2] so that they can be deployed to guarantee everlasting privacy of elections in the real world, not only in theory.

References

1. Cramer, R., Franklin, Matthew K., Schoenmakers, B., Yung, M.: Multi-Autority Secret-Ballot Elections with Linear Work. In: EUROCRYPT 1996, pp. 72–83.
2. Cuvelier, E., Pereira, O., Peters, T.: Election Verifiability or Ballot Privacy: Do We Need to Choose?. In: ESORICS 2013, pp. 481–498.
3. Cortier, V., Gaudry, P., Glondu, S.: Belenios: A Simple Private and Verifiable Electronic Voting System. In: Foundations of Security, Protocols, and Equational Reasoning 2019, Springer, pp. 214–238.
4. Locher, P., Haenni, R.: Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. In: VoteID 2015, pp. 74–91.
5. Arapinis, M., Cortier, V., Kremer, S., Ryan, M.: Practical Everlasting Privacy. In: POST 2013, pp. 21–40.
6. Morio, K., Künnemann, R.: Verifying Accountability for Unbounded Sets of Participants. In: 34th IEEE Computer Security Foundations Symposium, CSF 2021, pp. 1–16.
7. Cheval, V., Jacomme, C., Kremer, S., Künnemann, R.: SAPIC+: Protocol Verifiers of the World, Unite!. In: USENIX Security Symposium, 2022.
8. Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX Security 2008, pp. 335–348.
9. Moran, T., Naor, M.: Split-ballot voting: everlasting privacy with distributed trust. In: ACM CCS 2007, pp. 246–255.
10. Buchmann, J., Demirel, D., Van de Graaf, J.: Towards a Publicly-Verifiable Mix-Net Providing Everlasting Privacy. In: FC 2013, Revised Selected Papers, pp. 197–204.