**Boundaries of privacy in E2E verifiable e-voting systems**

Tamara Finogina[[1]](#footnote-1),\*, Author 2[[2]](#footnote-2)

**Conference Topic**: Frontier Technologies

**Keywords**: security, E2E verifiability, privacy, e-voting

**ABSTRACT**

Voter privacy implies that a voter is capable of casting his own vote secretly and freely without letting others' parties, namely an adversary, to learn some information about his preferences or interfere in it. On the other hand, the end-to-end verifiability notion states that the voter can obtain a receipt at the end of the ballot casting procedure that is used for verifying that his vote was (1) cast as intended, (2) recorded as cast, and (3) tallied as recorded. Furthermore, anyone should be able to verify that the election procedure is executed properly.

Intuitively, the security property that an E2E verifiability intends to capture is the ability to *trace* a ballot back to the corresponding receipt and therefore to the voter who cast it. On the contrary, privacy means that no one, ideally not even election authority, is able to get some information about voter’s intent or link a voter with his ballot. It can be observed, that privacy and E2E verifiability requirements contradict each other at some point. Therefore, there should exist the maximum level of privacy that is possible to achieve in any E2E verifiable e-voting system.

We used the E2E verifiability definition given by Kiayias et al. As for privacy, we considered a case when all voters are corrupted but an adversary is still unable to break privacy, denotes as strict privacy. We formally define strict voter privacy via a Voter Privacy game that is played between an adversary *A* and a challenger *C* and takes as input a security parameter and returns 1 or 0 depending on whether the adversary wins. According to the game rules, an adversary is allowed to define an election parameters, act on behalf of all voters and corrupted entities. ding on whether the adversary wins. Also, A is allowed to corrupt some entities. The choice of the corrupted parties splits the Voter Privacy game into two different scenarios. All meaningful cases of collusion fall into two scenarios: (1) Election Authority and Trustee are hones and (2) Voting Support Device is honest. During the game the challenger plays the role of honest parties and returns to the adversary simulated and real view in order defined by a coin *a* (If *a=0*, the challenger returns *(simulated\_view,real\_view)* and *(real\_view,simulated\_view)* otherwise). A challenger flips the coin *a* only once, before interaction with an adversary. Note that the result of the game heavily depends on an efficiency of the simulator that is used by the challenger for producing a simulated view.

We proved that strict privacy is the weakest level of privacy that contradicts end-to-end verifiability.

[1] Yehuda Lindell. How To Simulate It - A Tutorial on the Simulation Proof Technique. [IACR Cryptology ePrint Archive 2016](http://dblp.uni-trier.de/db/journals/iacr/iacr2016.html#Lindell16): 46 (2016)

[2] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. End-to-end verifiable elections in the standard model. In EUROCRYPT, pages 468–498. Springer, 2015.

[3] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pages 352–363. ACM, 2015.

**Thomas’s edits**

**Conference Topic**: Big Data

**Keywords**: e-voting security, E2E verifiability, privacy-preserving data processing

In an electronic voting (e-voting) execution, the voters engage in an interaction with the system by providing sensitive data such as their vote preference, authentication passwords, or personal data used for election auditing. All collected data should be processed in a way that election integrity and voter privacy are preserved at the best possible level. In scenarios that e-voting runs at a national level data processing scales at the order of millions, whereas any security breach may lead to a massive and disastrous effect. Consequently, formal analysis and provable security of e-voting systems has been in the centre of related literature.

*Voter privacy* suggests that voters are capable of casting their votes secretly and freely without letting adversarial parties to learn any information about their preferences. On the other hand, integrity is traditionally captured by *the end-to-end (E2E) verifiability* notion states that the voter can obtain a receipt at the end of the ballot casting procedure that is used for verifying that his vote was (1) cast as intended, (2) recorded as cast, and (3) tallied as recorded. Furthermore, anyone should be able to verify that the election procedure is executed properly. It has been observed that voter privacy and E2E verifiability requirements inherently contradict each other at some point. Therefore, there should exist the maximum level of privacy that is possible to achieve in any E2E verifiable e-voting system.

In this work, we perform a thorough and formal study on “locating” the critical contradiction point in the voter privacy-E2E verifiability tradeoff. As part of our analysis, we introduce a strong privacy definition where voters are corrupted but an adversary is still unable to break privacy, denoted as *strict privacy*. We formally define strict voter privacy via a Voter Privacy game that is played between an adversary *A* and a challenger *C*. According to the game rules, an adversary is allowed to define the election parameters, corrupt a number of entities, and act on behalf of all voters. As for we apply the E2E verifiability definition given by Kiayias et al., according to which even when all election administrators are corrupted, they can not manipulate the results without a high detection probability.

Under this framework, we prove that strict privacy is the weakest level of privacy that contradicts end-to-end verifiability. Namely, any meaningful relaxation of the strict privacy definition, leads to a notion if privacy that is feasible by some E2E verifiable e-voting system.

1. affilliation [↑](#footnote-ref-1)
2. affilliation

   \* corresponding author: email address [↑](#footnote-ref-2)