Voting Without a Trace

Degree programme: Master of Science in Engineering | Specialisation: Information and Communications Technologies
Thesis advisor: Prof. Dr. Reto Koenig
Experts: Prof. Jacques André Augustin (EFREI Paris), Dr. Karola Marky (University of Glasgow)

Voting is one of the main pillars that allows citizens to elect their representatives and express their opinions in a democratic society. However, our voting protocols haven't evolved with the technological improvements in sensing and forensics, and so start losing protection against attacks concerning anonymity. This work demonstrates these weaknesses and proposes solutions to regain protection against de-anonymization.

Context

Voting is part of democracy's rituals, where members of the society are allowed to express their volition. Each voter leaves a mark on its ballot by expressing its volition. Unfortunately, though, oblivious to the voter, any current voting process itself leads to individual markers, so that track-marking along the voting process becomes unavoidable. While this has always been the case, it's only with the great advances in sensing storage and forensics that backtracking a marked ballot to its origin (i.e. the voter) is becoming more accessible (i.e. cheaper). This results in an attack vector for complete de-anonymization of voters after having cast their ballots. Thus, this renders any guarantee of the preservation of anonymity void for any current voting process.

In e-voting, the aspect of anonymity is tackled using various techniques such as mixnets or homomorphic tallying. The drawback of those solutions is that there are long-term secrets involved (permutations within the mixnet, decryption key ...). They create an attack vector that can be used to act against people in the future, regarding a mark on a specific vote in the past. Members of the society and parties must have confidence in the entire voting process to be able to accept any voting outcome. This requires the whole process to be verifiable individually and universally (i.e. end-to-end verifiable). The introduction of a new voting protocol, especially if it requires non-trivial steps or devices, has to be understood and approved by the public in order to be trusted. Therefore, the use of mathematics and technologies that require specialized knowledge (such as cryptography) must be reduced to the bare minimum.

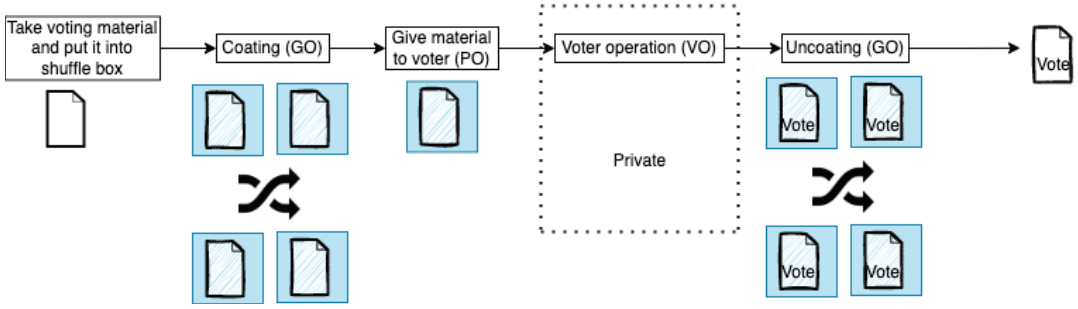
Layered Architecture for Voting

To enable verifiable traceless voting, I propose a new approach. Inspired by the double envelope voting, I revisit and extend the well-known multilayer approach. Nowadays, each covering (coating) or uncovering of an envelope (uncoating) is performed per ballot, i.e., one local operation per ballot. I propose the introduction of a global operation for coating and uncoating, where those two operations are each performed on all ballots at the same time and location, leading to a hidden shuffling. I claim that this results in a voting approach, where the tracing link between the individual markers and the vote is broken. This results in voting without a trace.

This requires the voter to cast and verify its vote on the ballot without having to remove or even touch the opaque coating. For this purpose, I propose a new physical ballot and an appropriate procedure. This allows end-to-end verifiable voting without a trace, where targeted attacks on vote privacy are detectable with a very high probability.

Paul-Henri Guy Maurice Zimmerlin

paulhenri.zimmerlin@gmail.com



Voting Protocol with Layered Architecture