Championing tally-then-decrypt secrecy

Ben Smyth

University of Birmingham, UK

December 7, 2024

Abstract

Ballot secrecy is achievable with varying degrees of information leakage: At one extreme, *winner-only secrecy* reveals just the winning candidate. At the other, *secrecy by anonymity* reveals anonymised votes. I champion *tally-then-decrypt secrecy* for delivering on traditional privacy expectations, wherein an election reveals nothing more than a frequency distribution of voters' votes. The gulf between anonymised votes and vote frequency distributions is witnessed by mixnets revealing the contents of every individual ballot (i.e., anonymised votes), whilst homomorphically combining ballots reveals only a frequency distribution.

Homomorphic combinations beat mixing for elections, witness:

Tally-then-decrypt secrecy, meaning indistinguishability between any election and any other election with the same outcome.

Tally-then-decrypt secrecy excludes mixnet-based voting systems, whereby mixed encrypted ballots are decrypted, since such systems reveal the contents of every individual ballot, not mere outcomes, e.g.,

□ □ ☑ □ □   □ ☑ □ □ □   □ □ □ ☑ □

□ □ □ □ ☑   □ □ □ □ ☑   □ □ ☑ □ □

□ □ □ ☑ □   ☑ □ □ □ □   □ □ □ ☑ □

is distinguishable from the following, because mixnet-based systems reveal the correlation between a voter's choices

□ ☑ □ □ □   □ □ □ ☑ □   □ □ ☑ □ □

□ □ ☑ □ □   □ □ □ □ ☑   □ □ □ □ ☑

□ □ □ ☑ □   □ □ □ ☑ □   ☑ □ □ □ □

whilst both correspond to the same outcome (frequency distribution of votes)

□ $\boxed{1}$ $\boxed{1}$ $\boxed{1}$ □

□ □ $\boxed{1}$ □ $\boxed{2}$

$\boxed{1}$ □ □ $\boxed{2}$ □

Tally-then-decrypt secrecy demands encrypted ballots be homomorphically combined, rather than mixed and decrypted.

Voting systems inevitably leak information. At the very least, an electorate's decision must be revealed:

Winner-only secrecy, revealing just the winning candidate.

Society opts for a more nuanced voice, that of the electorate, suggesting a communal choice cannot be reduced to a single candidate name; society demands not only revealing the winner, but also the break-down of that decision, as afforded by tally-then-decrypt secrecy.

An established class of voting systems anonymise votes and decrypt, revealing the contents of each individual ballot, failing tally-then-decrypt secrecy. (Except for first-past-the-post voting, wherein a frequency distribution of votes is equivalent to anonymised votes.) Mixnet-based voting systems require a weaker privacy notion:

Secrecy by anonymity, only anonymised votes are revealed.

A further established class of voting systems tally votes and decrypt: Tally-then-decrypt voting systems deliver on society's privacy expectations, whilst leaking less information than anonymise-then-decrypt systems.

Subtleties between anonymise-then-decrypt and tally-then-decrypt voting systems have gone unnoticed. Voting systems adopted by nation states fall short. (E.g., Swiss Post provide mixnet-based voting for Switzerland and acknowledge need for improvement.) I champion tally-then-decrypt voting systems.