Verifiable Randomness Pillar Technical Summary

Author: Christopher Vatcher

Editors: Alan Sherman and Aggelos Kiayias

The RSV system combines private randomness and public verifiable randomness to achieve its privacy and security properties. The initial private randomness contributed by the election authority protects voter privacy and secures the system against manipulation by entities other than the election authority. An additional layer of public verifiable randomness protects the voter selection process and election audit against meaningful manipulation by any entity, including the election authority.

We apply verifiable randomization before protocol participants act on information newly-supplied by the election authority. The application occurs in three phases.

1. Commit -- The election authority publicly commits new information. Before the initial draw, this includes the election definition, ballot information, and privacy randomization. Before the final draw, this includes the print audit information and votes.
2. Accumulate -- The election authority waits until the random beacon accumulates enough bits to run its next randomized procedure. Only entropy generated after the commit is admissible.
3. Execute -- The election authority uses the bits supplied by the random beacon to run a randomized procedure. For the initial draw, this is the generation of third summands. For the final draw, this is the partitioning of the audit tables.

The source of public verifiable random bits for the RSV system is our verifiable random beacon. The goal of our beacon is to provide public verifiable random bits as a service under a trust model with miniminal assumptions. The only data the beacon receives is entropy data that it scrapes from reputable authoritative sources. The beacon performs all randomness extraction to generate bits. To facilitate verifiability, the beacon publishes signed copies of all entropy data, randomness extraction algorithms, and resulting bits.

Our beacon aggregates multiple verifiable sources of entropy to supply a large

number of verifiable random bits. Currently available sources include stocks from the Consolidate Tape Association (i.e., New York Stock Exchange), which provide over 6,000 bits per day. Sources under active development include a re-broadcast of the NIST random beacon, which provides over 730,000 bits per day, and quality-controlled climatological data from the U.S. National Oceanic and Atmospheric Administration (NOAA).