STAR-Vote

Secure, Transparent, Auditable, and Reliable Voting System

In her 2011 EVT/WOTE keynote, Travis County, Texas County Clerk Dana Debeauvoir described the qualities she wanted in her ideal election system. In April of 2012, a group of researchers travelled to Austin, Texas and spent three days with Debeauvoir and her staff exploring options and searching out alternatives. The result of that meeting is a design of a system that has easy on voters, unambiguous, and has higher assurance than any system previously developed. This paper offers a detailed description of the Travis County requirements, the STAR-vote system designed for Travis County, and the properties of STAR-vote.

# Introduction and Background

Travis County, in central Texas, includes the state capital of Austin and has over 1 million residents. The county holds numerous elections each year and has been using Hart Intercivic (paperless) equipment for about a decade. Although the county is diligent in its use of best practices – including full parallel testing of randomly-selected equipment during actual elections – numerous concerns have been raised over the lack of verifiability of the election results. Although the County Clerk’s office dislikes paper for reasons that include the difficulties of counting paper, interpreting ambiguous marks, and storing records, many citizens have insisted of a full paper trail.

Debeauvoir has suggested the use of electronic ballot marking devices which have numerous advantages such as ease of use, accommodation of voters with disabilities, and lack of ambiguity. She proposes that the marking devices produce paper ballots which can be reviewed by voters before being deposited in a ballot box.

The research team coupled this design with an end-to-end verifiable process, a privacy-preserving risk-limiting audit, and a mechanism which avoids the necessity of routine counting of paper. There are essentially three redundant assurances: the end-to-end verifiability ensures that all cast ballots are properly counted, the privacy-preserving risk-limiting audit provides high confidence that the paper ballots match the reported electronic count, and the full set of paper ballots is retained in case a complete manual recount is ever desired. All of this is done in a way which minimizes the burdens on voters and poll workers.

# Design Overview

From the perspective of voters, the process of registration and poll-station sign-in is unchanged from current practice. Once authorized, voters proceed to an electronic ballot marking device where they can make use of a rich interface that prevents overvotes, warns of undervotes, and supports alternative input/output media for disabled and impaired voters. After indicating their selections, voters each receive two (possibly joined) items from a ballot marking device: a printed ballot listing their selections and a take-home printed receipt that includes information about the device and time of the vote as well as a short (12-16 byte) hash code which incorporates an encryption of the voter’s selections together with those of prior voters.

Voters can then review their printed ballots and decide whether they are happy with the indicated selections. Satisfied voters can then deposit their paper ballots into a ballot box to complete the process. Voters can alternately approach a poll worker to have their ballots spoiled and be given the option to return to a ballot marking device to start the process anew.

Voters who care to do so can later check their receipts (both cast and spoiled) against a published list to verify their correctness.

# Further Detail

From the perspective of election officials, the first *new* element in the election regiment is the cryptographic key generation process. A set of election trustees is designated as key holders and a threshold number is fixed. The functional effect is that if there are election trustees and the threshold value is , then any of the trustees can complete the election – even if the remaining are unavailable. This threshold mechanism provides robustness while preventing any fewer than of the trustees from performing election functions which might compromise voter privacy.

The trustees each generate an ElGamal key pair consisting of a private key and a public key and they publish their public keys. A standard public procedure is then used to compute a single ElGamal public key from the trustee public keys such that decryptions can be performed by any of the trustees. This single ElGamal election public key is published and provided to all ballot marking devices together with all necessary ballot style information to be used in the election. Each ballot marking device is also seeded with a start value that includes a unique identifier for both the device and the election.

During the election, voters use ballot marking devices to make their selections. Once selections are completed, the ballot marking device produces paper printouts of two items. The first is the paper ballot which consists of the selections made by the voter and also includes a random (non-sequential) serial number. The second is a receipt that consists of an identification number for the ballot marking device, the date and time of the vote, and a truncated SHA-256 hash of the ElGamal encryption of the voter’s selections together with the previous hash value. Specifically, if the voter’s selections are denoted by , the hash value produced by a particular ballot marking device in an election is computed as

where denotes the SHA-256 hash function and denotes ElGamal encryption.

The ballot marking device should retain both the encrypted ballot and the current hash value. At the conclusion of the election (if not sooner), the encrypted ballot should be posted on a publically-accessible web page and digitally signed by the election office using a simple signature key (not the key generated by the trustees). The posting of each encrypted ballot should also include a non-interactive zero-knowledge (NIZK) proof that the ballot is well-formed.

Once they receive their ballots and receipts, voters may either deposit their ballots into a ballot box or taken them a poll-worker and have them spoiled. Ballots deposited in a ballot box have their serial numbers scanned and recorded. The electronically stored encrypted vote is not considered complete (and not included in the tally) unless and until its corresponding serial number has been recorded in the ballot box.

Any electronic stored encrypted ballots for which no corresponding serial number has been scanned and recorded are deemed spoiled. The published election record should include all spoiled ballots as well as all cast ballots, but for each spoiled ballot the published record should also include a verifiable decryption of the ballot’s contents. Voters should be able to easily look up digitally-signed records for any receipts they hold and verify their presence and, for spoiled receipts, the ballot contents.

A voter who takes a completed paper ballot to a poll worker can request that the poll worker spoil the ballot and offer an opportunity to re-vote. The poll worker marks the paper ballot as spoiled (including removing or marking the serial number so that it will not be recorded if subsequently placed in the ballot box) and returns the spoiled ballot to the voter.

Upon completion of the election, the election office homomorphically combines the cast ballots into an aggregate encryption of the election tally (this is simply a multiplication of the public encrypted ballots). At last of the election trustees then each perform their share of the decryption of the aggregate as well as individual decryptions of each of the spoiled ballots. The trustees also post data necessary to allow observers to verify the accuracy of the decryptions.

After the tally is announced and the verification data is published, the set of cast ballots is verifiably shuffled with a mix network. This shuffling could be performed by the same trustees who act as key holders, but the shuffling task could be performed by other parties or even by the election office. A privacy-preserving risk-limiting audit is then performed by randomly selecting paper ballots and matching each selected ballot with a corresponding encrypted ballot to demonstrate the correct matching.

# Triple Assurance

The election tally is verified by three independent mechanisms. The homomorphic tallying process proves that the announced tally corresponds to the posted encrypted ballot records, and the ballot spoiling and receipt checking processes allow voters to check that these encrypted ballot records correctly reflect their selections. The risk-limiting audit process provides an independent check that the paper ballots match the encrypted ballot records (regardless of how many voters check their own ballots) and also that the announced tally is consistent with the paper records. Finally, the paper records remain available in case of systemic failure of the electronic records or if a manual count is ever desired.

The design of the election system ensures that all three of these checks should be perfectly synchronized and will not produce different tallies. There is sufficient information in the records so that if any discrepancies arise (for instance because of loss of some of the electronic or paper records), the discrepancies can be isolated to individual ballots that are mismatched or counted differently. There should be no instances in which any of the three tally verifications will produce inconsistent results.