Mind the Gap: Individual- and universal-verifiability plus cast-as-intended don't yield verifiable voting systems

Ben Smyth

University of Birmingham, UK

Abstract

We show that verifiable voting systems require a security notion beyond individual- and universal-verifiability plus cast-as-intended.

Keywords: Voting; individual- and universal-verifiability; cast-as-intended.

Publishing cast ballots allows each voter to check the presence of their ballot (individual verifiability) and coupling tallies with proofs allows anyone to check whether a tally represents votes expressed in collected ballots (universal verifiability) [1, 2, 3, 4, 5, 6, 7, 8]. Taken together, these facets enable voters to check whether tallying includes the vote expressed by their ballot. Yet, digital ballots—one hopes—are constructed by cryptographic means; we mere mortals, even the most studious, can't compute ballots. Voters are at the mercy of machines, which mightn't even compute ballots, let alone correctly compute ballots expressing voters' votes. Individual- and universal-verifiability only suffice for verifiable voting systems when voters can compute their own ballots, which is atypical of digital ballots.

Mind the Gap. *Individual- and universal-verifiability don't suffice for verifiable voting systems.*

In an attempt to bridge this gap, some systems define ways for a voter to check whether machines produce a ballot expressing their vote (cast-as-intended) [9, 10, 11, 12, 13, 14, 15]. For instance, a voter may input a vote to some machine and receive a purported ciphertext, encrypting that vote. Rather than blindly trusting a machine, the voter can demand evidence, which a trusted system or party can check to determine whether the received

value represents such a ciphertext. (Checks are typically cryptographic, beyond comprehension of us mere mortals.) Relying on a trusted system or party may seem disingenuous: Trust is contrary to verifiability. However, multiple systems or parties can perform checks to limit trust. (Albeit, scalability takes a hit.) Evidence proves whether a ciphertext encrypts a particular vote and such ciphertexts shouldn't be cast to avoid compromising privacy. So, voters repeat the process until they're convinced a machine functions correctly, then they cast the next value received from the machine (without demanding evidence), providing probabilistic assurance that the value is a ciphertext encrypting their vote.

Mind the Gap. *Cast-as-intended and individual verifiability don't suffice to determine whether collected ballots express voters' votes.*

Digital ballot construction typically mandates sampling bits. If a machine abandons the prescribed sampling procedure, computation delivers something resembling a ballot, rather than a correctly computed ballot: A ballot constructed in disregard for the prescribed procedure is not correctly computed. It may resemble a ballot. A ballot may even be computable in that way. However, ignoring the construction mandate means the result cannot a priori be considered a correctly computed ballot. Herein lies the rub—voters cannot determine whether machines compute ballots or things resembling ballots. Cast-as-intended and individual verifiability don't compose to enable determination of whether collected ballots express voters' votes, since voters cannot determine whether machines even compute ballots correctly.

Mind the Gap. *Individual- and universal-verifiability plus cast-as-intended don't yield verifiable voting systems*

Consequently, voting systems accepted as verifiable, might not be. Clash attacks [16] are one example of insecurities that may arise. For example, rather than sampling bits correctly, a machine may sample bits in advance and use those bits when encrypting votes. Two voters inputting the same vote (having amassed equal volumes of evidence) will receive the same ciphertext. They'll rightly be assured the ciphertext encrypts their vote and rightly detect the ciphertext's presence, but neither can determine whether the ciphertext is theirs, since both voters received identical values. There's a mismatch between assumptions underpinning cast-as-intended and individual verifiability: Cast-as-intended assures a ballot expresses a vote, not whether the

ballot is correctly computed, whilst individual verifiability assures correctly computed ballots are collected. Cast-as-intended and individual verifiability don't compose in the expected way.

Bridging the Gap. *Verifiable voting systems require a security notion beyond individual- and universal-verifiability plus cast-as-intended.*

We've established that individual- and universal-verifiability plus cast-as-intended don't yield verifiable voting systems. Identifying a suitable security notion to bridge the gap is a direction for future research.

References

[1] A. Juels, D. Catalano, M. Jakobsson, Coercion-Resistant Electronic Elections, in: Towards Trustworthy Elections: New Directions in Electronic Voting, Vol. 6000 of LNCS, Springer, 2010, pp. 37–63.

[2] B. Smyth, M. D. Ryan, S. Kremer, M. Kourjieh, Towards automatic analysis of election verifiability properties, in: ARSPA-WITS'10, Vol. 6186 of LNCS, Springer, 2010, pp. 165–182.

[3] S. Kremer, M. D. Ryan, B. Smyth, Election verifiability in electronic voting protocols, in: ESORICS'10, Vol. 6345 of LNCS, Springer, 2010, pp. 389–404.

[4] R. Küsters, T. Truderung, A. Vogt, Accountability: Definition and relationship to verifiability, in: CCS'10, ACM Press, 2010, pp. 526–535.

[5] A. Kiayias, T. Zacharias, B. Zhang, End-to-end verifiable elections in the standard model, in: EUROCRYPT'15, Vol. 9057 of LNCS, Springer, 2015, pp. 468–498.

[6] B. Smyth, S. Frink, M. R. Clarkson, Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ, Cryptology ePrint Archive, Report 2015/233 (2017).

[7] V. Cortier, D. Galindo, R. Küsters, J. Mueller, T. Truderung, SoK: Verifiability Notions for E-Voting Protocols, in: S&P'16, IEEE Computer Society, 2016, pp. 779–798.

[8] B. Smyth, Surveying global verifiability, Information Processing Letters.

[9] D. Chaum, Secret-Ballot Receipts and Transparent Integrity: Better and less-costly electronic voting at polling places, `https://web.archive.org/web/*/http://vreceipt.com/article.pdf` (2002).

[10] D. Chaum, Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy 2 (1) (2004) 38–47.

[11] C. A. Neff, Practical high certainty intent verification for encrypted votes, unpublished manuscript (2004).

[12] B. Adida, C. A. Neff, Ballot casting assurance, in: EVT'06, USENIX Association, 2006.

[13] J. Benaloh, Simple Verifiable Elections, in: EVT'06, USENIX Association, 2006.

[14] J. Benaloh, Ballot Casting Assurance via Voter-Initiated Poll Station Auditing, in: EVT'07, USENIX Association, 2007.

[15] P. Roenne, P. Y. A. Ryan, B. Smyth, Cast-as-intended: A formal definition and case studies, draft (2020).

[16] R. Küsters, T. Truderung, A. Vogt, Clash Attacks on the Verifiability of E-Voting Systems, in: S&P'12, IEEE Computer Society, 2012, pp. 395–409.