CALTECH/MIT
VOTING TECHNOLOGY PROJECT

A multi-disciplinary, collaborative project of
the California Institute of Technology – Pasadena, California 91125 and
the Massachusetts Institute of Technology – Cambridge, Massachusetts 02139

Software Independence Revisited

Ronald L. Rivest, Massachusetts Institute of Technology
Madars Virza, Massachusetts Institute of Technology

Key words: ***software complexity of voting systems, software-independent approaches***

VTP WORKING PAPER #144

Chapter 1

Software Independence Revisited

Ronald L. Rivest
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology (MIT)
Cambridge, MA 02139
rivest@mit.edu

Madars Virza
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology (MIT)
Cambridge, MA 02139
madars@mit.edu

CONTENTS

1.1 Introduction

Democracy depends on elections, yet elections are complex but fragile processes involving voters, election officials, candidates, procedures, and technology. Voting systems are evaluated in terms of their security, usability, efficiency, cost, accessibility, and reliability. A good voting system design should be based on sound principles.

The principle of "software independence" was introduced by Rivest and Wack [488] and Rivest [486]:

> A voting system is *software-independent* if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome.

For example, optical scan and some cryptographically-based voting systems are software-independent.

Software independence is one form of auditability, enabling detection and possible correction of election outcome errors caused by malicious software or software bugs.

This chapter begins with a review of the definition of software independence as given by Rivest and Wack [488] and Rivest [486]; starting with a review of the issue of software complexity (Section 1.2) and a re-presentation of the definition of software independence and its rationale (Section 1.3). The reader is encouraged to consult the original papers [488, 486] for further details, elaboration, and clarification of the original definition.

Further sections discuss evidence-based elections (Section 1.6), end-to-end verifiable voting (Section 1.8), and verifiable computation (Section 1.10).

1.2 Problem: Software complexity of voting systems

We start by describing the problem that software-independence addresses: the difficulty of assuring oneself that voted ballots will be recorded accurately by complex and difficult-to-test software in all-electronic voting systems. We emphasize that the

problem is providing such assurance: the software may well be correct, but convincing oneself (or others) that this is the case is effectively impossible.

Electronic voting systems are complex and continue to grow more so. The requirements for privacy for the voter, for security against attack or failure, and for the accuracy of the final tally are in serious conflict with each other. It is common wisdom that complex and conflicting system requirements lead to burgeoning system complexity.

Voting system vendors express and capture this complexity via software in their voting systems.

As an example, consider a Direct-Recording Electronic (DRE) voting system, which typically provides a touch-screen user interface for voters to make selections and cast ballots, and which stores the cast vote records in memory and on a removable memory card. A DRE may display an essentially infinite variety of different ballot layouts, and may include complex accessibility features for the sight-impaired (e.g., so that a voter could use headphones and be guided to make selections using an audio ballot).

An issue, then, is how to provide assurance, despite the complexity of the software, that the voting system will accurately record the voter's intentions. A pure DRE voting system produces only electronic cast ballot records, which are not directly observable or verifiable by the voter.

Consequently, no meaningful audit of the DRE's electronic records to determine their accuracy is possible; accuracy can only be estimated by a variety of other (imperfect) measures, such as comparing the accumulated tallies to pre-election canvassing results, performing software code reviews, and testing the system accuracy before (or even during) the election.

1.2.1 The difficulty of evaluating complex software for errors

It is a common maxim that complexity is the enemy of security and accuracy, thus it is very difficult to evaluate a complex system. A very small error, such as a transposed pair of characters or an omitted command to initialize a variable, in a large complex system may cause unexpected results at unpredictable times. Or, it may provide a vulnerability that can be exploited by an adversary for large benefits.

Finding all errors in a large system is generally held to be impossible in general or else highly demanding and extremely expensive. Our ability to develop complex software vastly exceeds our ability to prove its correctness or test it satisfactorily within reasonable fiscal constraints (extensive testing of a voting system's software would certainly be cost-prohibitive given how voting in general is funded). A voting system for which the integrity of the election results intrinsically depends on the correctness of its software will always be somewhat suspect.

As we shall see, the software-independent approach follows the maxim, "Verify the election results, not the voting system."

1.2.2 The need for software-independent approaches

With the DRE approach, one is forced to trust (or assume) that the software is correct. If questions arise later about the accuracy of the election results (or if a recount is demanded), there is again no recourse but to trust (or assume) that the voting system did indeed record the votes accurately. We feel that one should strongly prefer voting systems where the integrity of the election outcome is not dependent on trusting the correctness of complex software.

The notion of "software-independence" captures exactly this desirable characteristic of providing election results that are verifiable, without having to depend on the assumption that the software is correct.

For users of software-independent voting systems, verification of the correctness of the election results is possible. There need be no lingering unanswerable concern that the election outcome was affected or actually determined by some software bug (or worse, e.g., by a malicious piece of code).

1.3 Definition and rationale for software-independence

We now repeat the definition of software-independence, and explore its meaning.

> A voting system is *software-independent* if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome.

A voting system that is not software-independent is said to be *software-dependent*—it is, in some sense, vulnerable to undetected programming errors, malicious code, or software manipulation, thus the correctness of the election results are dependent on the correctness of the software.

The first use of "undetected" in the definition is to give emphasis to software faults that are *undetected* not being able to cause *undetectable* changes; it is in parenthesis because already known faults may be dealt with by other means.

The intent of the definition of software independence is to capture the notion that a voting system is unacceptable if a software error can cause a change in the election outcome, with *no evidence available that anything has gone wrong*. A "silent theft" of the election should not be possible with a software-independent system. (At least, not a theft due to software...)

To illustrate the rationale for software-independence, let us run a "thought experiment." Put yourself in the place of an adversary and imagine that you have the

power to secretly replace any of the existing software used by the voting systems by software of your own construction. (You may assume that you have the original source code for the existing software).

With such an ability, can you (as the adversary) change an election outcome or "rig an election" without fear of detection?

If so, the system is *software-dependent*—the software is an "Achilles heel" of the voting system. Corrupting the software gives an adversary the power to secretly and silently steal an election.

If not, the system is *software-independent*—the voting system as whole (including the non-software components) has sufficient redundancy and potential for cross-checking that misbehavior by the software can be detected. The detection might be by the voter, by an election official or technician, by a post-election auditor, by an observer, or by some member of the public. (Indeed, anyone but the adversary.)

In such a "thought-experiment," we are considering the adversary as some evil agent that could load fraudulent software into voting systems. More realistically, we may consider this adversary to be an abstraction of the limitations of the software development process and testing process. (As such, for the purposes of determining whether a system is software-independent, one should presume that the software errors were present when the software was written and were not caught by software development control processes or by the certification process.)

As we have stated, complex software is difficult to write and to test, and will therefore contain numerous unintentional "bugs" that occasionally can cause voting systems to report incorrect election results. It would be extremely difficult and expensive to determine with certainty that a piece of software is free of bugs that might change an election outcome. Given the relatively small amounts of funding allocated for developing and testing voting system software, we may safely consider it as *effectively impossible*. Thus, the software itself is not considered evidence of a change in the election outcome for the purposes of the definition of software independence. Such "evidence" is too hard to evaluate.

1.3.1 Refinements and elaborations of software-independence

There are a number of possible refinements and elaborations of the notion of software-independence. We now motivate and introduce the distinction between *strong software-independence* and *weak software-independence*.

Security mechanisms are typically one of two forms: *prevention* or *detection*. Detection mechanisms may also be coupled with means for *recovery*. When identification of participants and accountability for actions is also present, then detection mechanisms are also the foundation for *deterrence*. Given the importance of recovery mechanisms in addition to detection mechanisms, we propose the following two refinements of the notion of software independence:

A voting system is *strongly software-independent* if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome, *and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected without re-running the election.*

A voting system that is *weakly software-independent* conforms to the basic definition of software-independence but is not strongly software-independent—that is, there is no recovery mechanism.

1.3.2 Examples of software-independent approaches

Currently, there are two general categories of software-independent approaches.

Voter-verifiable paper record (VVPR) approaches constitute the first category, since the VVPR allows (via a recount) the possibility of detecting (and even correcting) errors due to software. Accordingly, these voting systems can be strongly software-independent.

The most prominent example in this category is the optical scan voting system used by most U.S. voters since the 2006 elections. The paper ballot is voter-verifiable because the voter completes the ballot and can attest to its accuracy before it is fed into the optical scanner; the paper ballot thus serves as an audit trail that can be used in post-election audits of the optical scanner's electronic results. An electronic ballot marking system (EBM) may also be used to record the voter's choices electronically with a touch-screen interface and then to print a high-quality voter verifiable paper ballot for feeding into the optical scanner.

Another example in this category is the voter-verified paper audit trail (VVPAT) voting system, similar to a DRE but with a printer and additional logic. It produces two records of the voter's choices, one on the touch-screen display and one on paper (a VVPR). The voter must verify that both records are correct before causing them to be saved.

Cryptographic voting systems constitute the second category of software-independent voting system approaches. They can provide detection mechanisms for errors caused by software changes or errors [43, 143, 150, 340, 418, 501, 503]). At one level, they can enable voters to detect when their votes have been improperly represented to them at the polling site, and a simple recovery mechanism (re-voting) is available. At another level, they can enable anyone to detect when their votes have been lost or changed, or when the official tally has been computed incorrectly. Recovery is again possible. Most of the recently proposed cryptographic voting systems are strongly software-independent.

Receipt-based cryptographic voting systems involve a physical, e.g., paper receipt that the voter can use to verify, during the process of voting, whether his or her ballot was captured correctly. The contents of the receipt, in general, employ cryptography in some form so that the voter is able to verify that the votes were recorded accurately; the receipt does not show how the voter voted.

Approaches to software-independence other than pure use of VVPR or cryptographic voting systems are potentially possible, although beyond the scope of our paper.

1.4 How does one test for software-independence?

This brings up a more subtle point in the definition. What aspects of the voting system make it "software-independent?" Is it just the hardware and software, or does it also include the surrounding procedures? For example, is a voting system still software-independent if no post-election audits are performed?

The answer is that a voting system is software-independent if, after consideration of its software and hardware, it enables use of any election procedures needed to determine whether the election outcome is accurate without having to trust that the voting system software is correct. The election procedures could include those carried out by voters in the course of casting ballots, or in the case of optical scan and VVPAT, they could include election official procedures such as post-election audits.

The detection of any software misbehavior does not need to be perfect; it only needs to happen with sufficiently high probability, in an assumed ideal environment with alert voters, pollworkers, etc.

As an example, consider the EBM which prints out a filled-in optical scan ballot. Some voters may not review the printed ballot at all. Yet the EBM is still software-independent; there is a significant probability that software misbehavior by the EBM will be detected (this is similarly true of VVPAT). For the purposes of the definition of "software independence," we assume that (enough) voters are sufficiently observant to detect such misbehavior. (If this assumption were discovered to be false in practice, some increase in voter education might be necessary.) Although some forms of such detectable misbehavior may leave no tangible proof of misbehavior, the definition of software independence does not require that all misbehavior have tangible proof; it is sufficient that the relevant misbehavior be detectable and reportable.

Continuing with this example, we note that there is also software in the optical scanner used to scan the ballots that might produce incorrect output. But such misbehavior is detectable by a post-election audit procedure that hand-counts the paper ballots, thus the optical scan voting system is software-independent. (Note that such audits are typically statistical in nature and are thus not perfect detectors of misbehavior. But a well-designed audit will catch such misbehavior with reasonable probability. See [66, 285].

To illustrate further, then, say that no post-election audit of an optical scan-based election is required if the apparent margin of victory is more than 10%. An optical scan system would be still be considered software-independent in such an election, since the original voter-verified paper ballots are available for review, and software misbehavior can still in principle be detected. (As a side note: we feel that such post-

election audits are always a good idea and that "no audit" should not be an option. If an apparent margin of victory is large, a smaller audit is appropriate.)

As a final example, say that electronic pollbook systems are used in an optical scan-based election, but the electronic pollbooks do not create a contemporaneous paper record for each voter. Thus, their software must be trusted to show that the number of optical scan records (paper and electronic) accurately reflect the actual number of voters who used the scanners. Are these systems software-independent? We would argue that the answer is no for the electronic pollbook, as the design of this system has prevented an audit to determine if the number of optical scan records is correct, i.e., its software must be trusted to be correct. A contemporaneous paper record would have made the electronic pollbook software-independent.

1.5 Discussion

1.5.1 Implications for testing and certification

Given the exceptional difficulty of proving software to be correct, it is a reasonable proposal to disallow voting systems that are software-dependent altogether.

If testingand certification of software-dependent voting systems are to be nonetheless contemplated, then one should expect the certification process should be very much more demanding and rigorous for a software-dependent voting system than for a software-independent voting system. The manufacturer should submit a formal proof of correctness, with perhaps an assurance level corresponding to EAL level 6 or 7 [1] and public disclosure of the source code. Moreover, the voting system must permit proof it is running the software it is supposed to.

1.5.2 Related issues

There may be other aspects of software misbehavior that don't quite fit our proposed notion of software-independence. For example, software may bias a voter's choices in subtle ways (say by displaying one candidate's name in slightly brighter characters on a touch-screen). These issues fall outside the scope of software-independence, since the correct "election outcome" isn't well-defined until the voter indicates her choice. Software independence is focused on the correctness of the election results, and not on other aspects of the voting process.

Some voting systems, such as certain STV (Single Transferable Vote) systems, determine an election outcome in a way that may be randomized (e.g. for breaking ties). A voting system whose software breaks ties in different ways would not be

[1] `http://en.wikipedia.org/wiki/Common_Criteria`, `http://en.wikipedia.org/wiki/Evaluation_Assurance_Level`

considered to violate software independence, as long as any outcome so determined is a legally acceptable election outcome given the cast vote records.

It is worth emphasizing that the records produced of voters' choices should be of sufficient quality and durability to be usable in an post-election audit.

1.6 Evidence-based elections

Recently (2012), Stark and Wagner proposed [541] the notion of "evidence-based elections," a broad framework for understanding how confidence in election outcomes can be achieved, through a combination of auditability (achieved via strongly software-independent voting systems), and auditing (specifically, compiliance audits and risk-limiting audits).

In this framework, strongly software-independent voting systems generate the audit trail (typically, but not necessarily, consisting of voter-verified paper ballots), while the compliance checks that the audit trail has not been corrupted or compromised, and the risk-limiting audit ensures (by appropriate statistical sampling and analysis) that the audit trail is consistent with the stated election outcome.

It is the combination of auditability and actual auditing that provides the evidence for the correctness of the election outcome. As they put it,

$$\text{evidence} = \text{auditability} + \text{auditing}$$

In this framework, the voting system software is not part of the evidence being evaluated during the audit. Furthermore, as Stark and Wagner argue effectively, trust in the software is not necessary for developing confidence in election outcomes. Indeed, the need to have time-consuming and expensive voting system certifications may be hampering the development of voting systems that enable elections that provide the evidence necessary to have trustworthy outcomes.

We endorse the "evidence-based elections" framework described by Stark and Wagner. Software-independence is a necessary component of such a framework.

1.7 The use of a public ledger

The development of the internet has made possible the "democratization" of many capabilities previously reserved for the few. The diversity and quantity of information available for public review, compared to the situation only two decades ago, is quite astonishing.

Of interest here is the availability of *transactional* data generated by users with some information system. Usually such information is made available in the form of a per-application database, maintained by the transaction service provider. Sometimes

the transaction data is available only to the user involved in the transaction (e.g. credit-card data); sometimes it is public (e.g. real-estate transactions).

So, one may reasonably ask whether election data can or should be made available online and even made available to the public in the form of a "public ledger" or "public bulletin board".

There is no reason not to do so, except when doing so might violate voter privacy. Making election information available online should not enable voters to sell their votes or be coerced into voting in a certain way.

Indeed, making the audit trail publicly available may engender greater trust in the election outcome, since the public may help with the verification that the audit trail is consistent with their knowledge as to how they voted and with the stated election outcome.

The Bitcoin [403] block chain exemplifies an extreme position with respect to democratization: not only is the transaction ledger totally public, but the ledger is maintained without trusted third parties by a clever peer-to-peer mechanism based on incentives for "miners" who extend the block-chain containing the ledger by solving cryptographic puzzles.

Yet, while proposals have been floated, and even tested, for block-chain based voting [2], it is important to distinguish the questions "(1) What information is on the audit trails?" and "(2) Is that information public?". The use of a public ledger (as, for example, provided by block-chain based ledger) provides an affirmative answer to (2), it does nothing to answer (1)—other mechanisms, such as those based on digital signatures, provided evidence as to what information is authentically part of the audit trail.

Whether the audit trail is made public on a peer-to-peer based public ledger (as with bitcoin) or is made public on a web site maintained by election officials is not the key question; the critical questions are whether the audit trail is readable by the public and whether there is reason to believe that it is complete and accurate (the sort of questions asked in compliance audit).

The notion of having the audit trail totally public is a good one. It existed in the early days of our republic, but disappeared when secret ballots and voting machines became the norm. *It is time to again make election audit trails public.*

In the context of a public ledger containing the audit trail, a strongly software independent voting system enables the reconstruction of the correct election outcome from the public audit trail.

[2] `http://www.coindesk.com/bitcoin-foundation-blockchain-voting-system-controversy/`

1.8 End-to-end verifiable voting systems

"Cryptographic voting systems" were mentioned briefly in Section 1.3.2 as an example of (strongly) software-independent voting systems; here we elaborate a bit more on their properties, and their relationship to software-independence and evidence-based elections.

This line of research has progressed significantly since our original paper on software independence was published (2006).

The common name for such systems has evolved to "*end-to-end auditable voting systems*" (or sometimes "*end-to-end verifiable voting systems*", to emphasize that the verification covers all the way from the voter's head (where her choices are selected) to the final outcome (reflecting all cast votes):

- a voter may verify that her vote is *cast as intended*,
- anyone may verify that a given vote is *collected as cast*, and
- anyone may verify that the votes are *counted as collected*.

In these systems, the collected cast votes are placed in a public ledger; to protect voter privacy, the votes are encrypted before being cast (e.g. with the public key of an election authority).

Some protocol, such as Benaloh's "*ballot casting assurance*" protocol [85], is needed to assure voters that their votes are being properly encrypted. *Such a protocol is essential for making the design software-independent*; without it the voting terminal could mis-represent the voter's intent by encrypting something other than the voter's choice.

For some designs, such as "Prêt à voter" [499], "Scratch and Vote" [49], and "Scantegrity" [386, 133, 146, 144], ballots are preprinted, containing both plaintext (human-readable) choices and corresponding ciphertexts. For such designs one should include a process (a "ballot audit") for allowing voters (and other auditors) to randomly select preprinted ballots, spoil them (remove them from the pool of ballots eligible to be cast), and challenge the system to demonstrate that the ciphertexts properly represent the corresponding plaintexts. Again, such a ballot-auditing process is essential for making the design software-independent; without it the ballot-printing subsystem could effectively cause voters' selections to be represented incorrectly by the corresponding ciphertexts.

The "ThreeBallot" design of Rivest [487] was proposed primarily for pedagogic purposes to illustrate the principles of end-to-end verifiable voting system design *without using cryptography*. ThreeBallot was not intended as a practical proposal, since each voter must submit *three* ballots, which must have an enforced relationship to each other (vote exactly twice in favor of a candidate to support him, vote exactly once in favor of a candidate to oppose him). The voter retains a randomly-chosen one of her three submitted ballots as a receipt so that she can check for its presence

in the public ledger. The question as to whether ThreeBallot is software-independent reduces to a consideration of the device that enforces the necessary relationship of the three submitted ballots. Clearly, the device should not know which of the three ballots was retained by the voter as her receipt.

However, a maliciously-programmed device in ThreeBallot might allow a voter to submit *three* ballots in favor of a certain candidate, which should not be allowed. Is this a violation of software independence? It seems not, since it requires not only that the device software be changed, but also that some voters collude in submitting illegal triples of ballots. Perhaps a new definition is needed.

We may define a voting system to be *vote-validating* if it checks that each cast vote is valid, and *publicly vote-validating* if anyone may determine from the public ledger that each vote is valid.

We see that ThreeBallot is thus vote-validating but not publicly vote-validating.

Note that vote-validation is not the same as providing ballot assurance; the former checks that the cast vote is one of the possible allowed votes, while the latter allows a voter to check that her cast vote correctly captures her intent.

Some end-to-end verifiable voting system designs, such as the homomorphic method proposed by Baudron et al. [76], achieve public vote-validation by providing each vote with a zero-knowledge proof of its validity (the vote and corresponding zero-knowledge proof of validity are posted together on the public ledger).

It is worth noting that the inclusion of such zero-knowledge proofs may provide malicious software with a means to cause an election to fail to produce an output: what should happen when one (or many) of such zero-knowledge proofs of input validity fail to verify? This is outside the scope of the notion of software-independence, since the activity of the malicious (or erroneous) software will of course be detected.

Some end-to-end verifiable voting designs, such as Scantegrity [386, 133, 146, 144] and STAR-Vote [77], are "paper/electronic hybrid" methods using a combination of paper-based and electronic methods, so that the paper ballot audit trail provides a backup mechanism for recovering the correct election outcome should the electronic or cryptographic methods completely fail somehow. This design also provides comfort to those who don't quite understand or trust the cryptographic techniques being used. Furthermore, the auditing process may include checks of both the paper audit trail and the electronic audit trail. (Should they disagree on the correct election outcome, the paper audit trail should probably take precedence, unless there is evidence that the paper audit trail was damaged or incomplete.)

Many proposed end-to-end verifiable voting system designs use mix-nets to provide voter privacy; the mix-net scrambles (permutes) the collection of cast votes while not adding or deleting votes, nor changing the content of any cast vote. To make a mix-net verifiable, the mix-net servers provide a zero-knowledge proof of these desired correctness properties; this zero-knowledge proof is also posted on the public ledger. In the absence of a paper audit trail, such zero-knowledge proof methods are essential for providing software-independence.

The other major category of end-to-end verifiable voting system proposals are those that are based on encryption methods with homomorphic properties [49, 76, 77]. Such methods do not need zero-knowledge proofs of correct mix-net operation, since they do not use mix-nets; the homomorphic aggregation of votes provides the desired anonymity. However, achieving software independence requires some method (such as a zero-knowledge proof) that provides assurance that the decryption of the aggregated tally was correctly performed.

Recently we have seen increasing attention to the possibility of running elections remotely "over the internet." In particular, the question is asked as to whether end-to-end verifiable elections can be run over the internet.

While voting over the internet has been done in Estonia [563], Springall et al. [535] argue that the Estonian voting system is not end-to-end verifiable and that it has numerous security vulnerabilities.

The Helios voting system [44] is perhaps the most widely-used internet-based end-to-end verifiable voting system. Like any remote voting system (such as vote-by-mail), there is no pretense of avoiding voter coercion; indeed, Helios makes the possibility of coercion explicit by providing a "Coerce-Me" button(!).

Küsters et al. [356] have demonstrated an interesting "clash" attack on some versions of Helios and on some other end-to-end voting systems, wherein voters who vote the same way may be given identical receipts (so when voters look them up on the public ledger everything seems OK, but the clash attack thereby provides the attacker with the freedom to add new ballots to the collection of cast votes). (The same authors also have an interesting definition of *accountability* applicable to voting systems [336].) Here the vulnerability lies with the random number generator; manipulating it can cause receipts to become identical. Systems with such a flaw are not software-independent.

Remotegrity [586] is an interesting extension to the Scantegrity system, employing *both* paper and electronic communications to allow remote voters to detect whether their votes have been tampered with, and to prove that such tampering exists without having to reveal how they have voted. Although Remotegrity utilizes a complex protocol involving code voting and scratch-off cards mailed to the voters, it does appear to achieve software independence, among other properties.

1.9 Program verification

As we discuss in Section 1.2.1, evaluating a software system for errors is generally held to be impossible. That said, approaches exist to verify that a software conforms to a given *specification*.

Given a specification S describing the input/output relationships, and a program P it is possible to write a formal proof π that interfaces of P satisfy the requirements outlined in S. Moreover such proofs π are verifiable. This is called *program*

verification and is an active research area. Thus, by spending a considerable and highly-skilled effort it is, in principle, possible to produce a proof that software used in voting conforms to a specification.

However, for such proof to be relevant it must be possible to determine that the particular program is in fact being executed by the hardware, and that the hardware executes *nothing else* that could interfere with the said program. As demonstrated by Checkoway et al. [154] the latter is extremely hard and believed impossible in general.

1.10 Verifiable computation and zero-knowledge proofs

In early days of the field, program verification techniques comprised the only set of techniques to try proving output of a computation correct. A relatively recent approach, which circumvents the outlined impossibility outlined faced by program verification techniques, is based on zero-knowledge proofs. Here, an output of a program is augmented with a proof that the *output* conforms to the specification, and thus is correct for the given input.

This is consistent with the "evidence-based elections" theme described above (Section 1.6), following the mantra of "verify the outcome, not the equipment", and is the approach we examine further in this section.

Proofs for end-to-end voting systems, e.g. those that verify correct shuffling of a mixnet or that vote is well-formed, can be seen as tailored examples of such zero-knowledge proofs. In contrast, recent years have seen a spark of availability of efficient *general-purpose* zero-knowledge proof systems. Provided people trust and accept them, those could greatly expand the domain of cryptographically verified voting schemes.

In more detail, a zero-knowledge proof system, given a program P, input x and secret input w, produces the output $z := P(x,w)$ and a proof π attesting to the fact that $z = P(x,w)$. Anyone, given x, P, z and π, can be convinced that there exists w such that $z = P(x,w)$, however the proof reveals nothing about w other than its existence. A weaker variant called *verifiable computation* system, assumes that there is no secret input w.

Zero-knowledge proofs in voting. As we explain next, zero-knowledge proofs are very powerful cryptographic tools with immediate applicability to voting. Consider the scenario of counting encrypted votes. Here x could comprise encrypted votes, w be the decryption key held by the election officials, and P be the program that does the tallying. Any observer, given encrypted votes, final election result and the corresponding proof, can be convinced that votes were counted correctly. Moreover, the observer does *not* need to trust the hardware used to produce the proof, nor that P's computation was not interfered with, etc.

More generally, the beautiful line of zero-knowledge works [261, 347, 393, 251]

have culminated in constructions that admit efficient practical prototypes [81, 454, 82]; we refer reader to [258] for a survey. Most efficient constructions sport linear verification time and constant-sized proofs (in practice: verification in few milliseconds and proofs of few hundreds of bytes, respectively). In particular, this efficiency means that most recent developments can greatly speed-up existing voting primitives (e.g. verifiable mixnets) and support new ones (e.g. proofs of correct decryption for complex encryption schemes).

That said, from a cryptographic perspective, constructions of very efficient zero-knowledge proofs tend to be a bit "heavy-weight" — current proposals tend to require complex theoretical machinery or strong cryptographic assumptions.

Moreover, all non-interactive proof systems require a *trusted setup* phase which, if done improperly or maliciously, yields the proofs vacuous. This is in line with preparations for regular elections, where mistakes could potentially turn out to be fatal. However, there is recent theoretical work that tries to lessen the trust requirements of the setup phase, but the degree of practicality such a solution would provide remains to be evaluated.

1.11 Conclusions and suggestions

The history of computing systems is that, given improvements and breakthroughs in technology and speed, software is able to do more and thus its complexity increases. The ability to prove the correctness of software diminishes rapidly as the software becomes more complex. It would effectively be impossible to adequately test future (and current) software-dependent voting systems for flaws and introduced fraud, and thus these systems would always remain suspect in their ability to provide secure and accurate elections.

A *software-independent* approach to voting systems assures voters that errors or fraud in election results can be reliably detected. Since the correctness of the election results does not ultimately depend on the correctness of the software, one can reduce the effort and expense to test and certify voting system software.

References

[1] ACCURATE: A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections. http://accurate-voting.org/.

[2] The American Statistical Association, by-laws, article III.2. http://www.amstat.org/about/bylaws.cfm.

[3] Chapter 2, rule 13: election of president - opening address. http://www.europarl.europa.eu/.

[4] Comment on the article published in the Guardian. http://vvk.ee/valimiste-korraldamine/vvk-uudised/vabariigi-valimiskomisjoni-vastulause-the-guardianis-ilmunud-artiklile/.

[5] Communities in America currently using proportional voting. The FairVote website archives. http://archive.fairvote.org/?page=2101.

[6] The constitution of FSFE, section 6, article 3. http://fsfe.org/about/legal/Constitution.en.pdf.

[7] Cumulative voting in Texas. The Texas Politics Project website, University of Texas at Austin. http://texaspolitics.utexas.edu/.

[8] Debian voting information. http://www.debian.org/vote/.

[9] Derwent valley council results in the 2014 Tsmanian local government elections, Tasmanian electoral commission. http://www.tec.tas.gov.au/LocalGovernmentElections2014/2014LGResults/DerwentValley.html.

[10] e-Estonia: Electronic ID card. https://e-estonia.com/component/electronic-id-card/.

[11] E-voting concept security: analysis and measures. http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf.

[12] E-voting system general overview. http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf.

[13] Election of the speaker of the house. http://www.parl.gc.ca/About/House/compendium/web-content/c_d_electionspeakerhouse-e.htm.

[14] Frequently asked questions: speaker's election. http://www.parliament.uk/about/faqs/house-of-commons-faqs/speakers-election/.

[15] Gauteng provincial legislature results in the 2014 national and provincial elections, electoral commission of South Africa. http://www.elections.org.za/resultsNPE2014.

[16] IMDb votes/ratings top frequently asked questions. http://www.imdb.com/help/show_leaf?votestopfaq.

[17] The institute for operations research and the management sciences, by-law 3. http://www.informs.org/About-INFORMS/Constitution-and-Bylaws.

[18] International Association for Voting Systems Sciences. http://www.iavoss.org/.

[19] Internet voting in Estonia. http://www.vvk.ee/voting-methods-in-estonia/engindex/.

[20] The ISU judging system general rules. http://www.isu.org/en/single-and-pair-skating-and-ice-dance/isu-judging-system.

[21] The Mathematical Association of America, by-laws, article IX.9. http://www.maa.org/about-maa/governance-documents/bylaws.

[22] Our response to the national election committee's statement. https://estoniaevoting.org/press-release/response-national-election-committees-statement/.

[23] Riigikogu election act. https://www.riigiteataja.ee/en/eli/ee/514112013015/consolide/current.

[24] Rules of procedures for online voting, section 3.4.1. https://ev.kde.org/rules/online_voting.php.

[25] Sejm constituency no. 28 (częstochowa) results in the 2011 parliamentary elections, the polish national electoral commission. http://www.wybory2011.pkw.gov.pl/wsw/en/sjm-28.html.

[26] Should the IACR use e-voting for its elections? http://www.iacr.org/elections/eVoting/.

[27] The south region results in the 2009 aboriginal land council of Tasmania, Tasmanian electoral commission. http://www.tec.tas.gov.au/OtherElections/ALCT.

[28] Statistics about internet voting in Estonia. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

[29] Ubuntu IRC council position. http://fridge.ubuntu.com/2012/05/17/ubuntu-irc-council-position/.

[30] Voting at home. http://www.vvk.ee/voting-methods-in-estonia/voting-on-election-day/voting-at-home/.

[31] Voting systems in the UK. http://www.parliament.uk/about/how/elections-and-voting/voting-systems/.

[32] What is Digi-ID, how can I get it and what can I do with it? http://www.id.ee/index.php?id=34410.

[33] Wombat voting system. http://www.wombat-voting.com/.

[34] e-voting security study, July 2002. CESG Report Issue 1.2.

[35] ECRYPT II yearly report on algorithms and keysizes, 2012. http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf.

[36] Public rules of the 60th Eurovision song contest. European Broadcasting Union, 2015. http://www.eurovision.tv.

[37] The Federal Constitutional Court Press Release No. 19/2009. Use of voting computers in 2005 bundestag election unconstitutional, March 3 2009. http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html.

[38] Jussi Aaltonen. Electronic voting case law in Finland. In Ardita Driza / Jordi Barrat, editor, *E-Voting Case Law. A Comparative Analysis*, pages 173–181. Farnham: Ashgate, 2015.

[39] ABC News. Computer voting may feature in March NSW election, February 4, 2015. http://www.abc.net.au/news/2015-02-04/computer-voting-may-feature-in-march-nsw-election/6068290.

[40] Claudia Z Acemyan, Philip Kortum, Michael D Byrne, and Dan S Wallach. Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems*, page 26, 2014.

[41] ACM. *ACM Statement on Voting Systems*. Association of Computer Machinery, 2004. `usacm.acm.org/images/documents/acm_evoting_reccomendations_press_release.pdf`.

[42] ACM Council Election. `http://www.acm.org/acmelections`.

[43] Ben Adida. *Advances in cryptographic voting systems*. PhD thesis, Massachusetts Institute of Technology, 2006.

[44] Ben Adida. Helios: Web-based open-audit voting. In *USENIX Security Symposium*, volume 17, pages 335–348, 2008.

[45] Ben Adida. Encrypting your vote in Javascript. In *Rump Session for EVT/WOTE*, 2011.

[46] Ben Adida, Olivier De Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a university president using open-audit voting: analysis of real-world use of Helios. In *International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, 2009.

[47] Ben Adida and C Andrew Neff. Ballot casting assurance. In *USENIX/Accurate Electronic Voting Technology Workshop*, 2006.

[48] Ben Adida and Olivier Pereira. State of Helios 2010: features and deployments. In *EVT/WOTE'10 – Rump Session Talk*, 8 2010.

[49] Ben Adida and Ronald L Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *the 5th ACM workshop on Privacy in electronic society*, pages 29–40. ACM, 2006.

[50] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *ACM Conference on Computer and Communications Security (CCS'15)*, October 2015.

[51] Anziani Alain and Antoine Lefèvre. *Information Report on behalf the Commission on Constitutional Laws, Legislation, Universal Suffrage, on the e-Voting Regulations and General Management*. 2014. `http://www.senat.fr/rap/r13-445/r13-4451.pdf`. Title translated from French.

[52] Joel Albarrán Bugié and Jesús Sancho. Hereu admits that the system did not work. *La Vanguardia*, May 12th 2010, 2010. `http://ves.cat/mfkr`. Translated from Catalan.

[53] Jordi Puiggalí Allepuz and Sandra Guasch Castelló. Universally verifiable efficient re-encryption mixnet. *Electronic Voting*, 167:241–254, 2010.

[54] Jordi Puiggalí Allepuz and Sandra Guasch Castelló. Internet voting system with cast as intended verification. In *E-Voting and Identity*, pages 36–52. Springer, 2012.

[55] R Michael Alvarez and Thad E Hall. *Electronic elections: The perils and promises of digital democracy*. Princeton University Press, 2010.

[56] Francisco Amato, Iván A Barrera Oro, Enrique Chaparro, Sergio Demian Lerner, Alfredo Ortega, Juliano Rizzo, Fernando Russ, Javier Smaldone, and Nicolas Waisman. Vot.Ar: Una mala elección, July 2015. `http://ivan.barreraoro.com.ar/vot-ar-una-mala-eleccion/`. In Spanish.

[57] Ross Anderson, Serge Vaudenay, Bart Preneel, and Kaisa Nyberg. The newton channel. In *Information hiding*, pages 151–156. Springer, 1996.

[58] Rudy B Andeweg. The Netherlands: the sanctity of proportionality. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 491–510. Oxford University Press, 2005.

[59] Andrew W Appel. How to defeat Rivest's ThreeBallot voting system. *Manuskrypt, pazdziernik*, 2006.

[60] Andrew W Appel, Maia Ginsburg, Harri Hursti, Brian W Kernighan, Christopher D Richards, and Gang Tan. Insecurities and inaccuracies of the Sequoia AVC Advantage 9.00H DRE voting machine, October 17, 2008. `https://www.cs.princeton.edu/~appel/papers/advantage-insecurities-redacted.pdf`.

[61] Marlos Ápyus. Na Câmara, o PT foi o único partido a votar contra a impressão do voto na urna eletrônica, November 18, 2015. `http://www.implicante.org/blog/na-camara-o-pt-foi-o-unico-partido-a-votar-contra-a-impressao-do-voto-na-urna-eletronica/`. In Portuguese.

[62] Diego F Aranha, Marcelo Monte Karam, André de Miranda, and Felipe Scarel. Software vulnerabilities in the Brazilian voting machine. In *Design, Development, and Use of Secure Electronic Voting Systems*, pages 149–175. IGI Global, 2014.

[63] Roberto Araujo, Sébastien Foulle, and Jacques Traoré. A practical and secure coercion-resistant scheme for internet voting. In *Towards Trustworthy Elections*, pages 330–342. Springer, 2010.

[64] Kenneth J. Arrow. A difficulty in the concept of social welfare. *Journal of Political Economy*, 58(4):328–346, 1950.

[65] Kenneth J. Arrow. *Social Choice and Individual Values*. Yale University Press, 1951.

[66] Javed A Aslam, Raluca A Popa, and Ronald L Rivest. On auditing elections when precincts have different sizes. In *EVT*, 2008.

[67] UN General Assembly. Universal declaration of human rights. *Resolution adopted by the General Assembly*, 10(12), 1948.

[68] Rishab Bailey and Rohit Sharma. E-voting case law in India. In Ardita Driza / Jordi Barrat, editor, *E-Voting Case Law. A Comparative Analysis*, pages 89–104. Farnham: Ashgate, 2015.

[69] Melle Bakker. The Netherlands. In *5th Review Meeting of Recommendation CM Rec(2004)11 on legal, operation and technical standards for e-voting*, 2014. `http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/5thmeeting/Netherlands.pdf`.

[70] Michael Bär, Christian Henrich, Jörn Müller-Quade, Stefan Röhrich, and Carmen Stüber. Real world experiences with Bingo Voting and a comparison of usability. In *Workshop On Trustworthy Elections (WOTE)*, volume 2008, 2008.

[71] Jordi Barrat. The certification of e-voting mechanisms. fighting against opacity. In Robert Krimmer / Rüdiger Grimm, editor, *Electronic Voting*, volume P-131 of *(Col. "Lecture Notes in Informatics-LNI")*, pages 197–206. Bonn: Gesellschaft für Informatik, 2008.

[72] Jordi Barrat. E-voting certification procedures. In Paloma Biglino, editor, *New Democratic and Electoral Expectations*, pages pp. 157–192. Title translated from Spanish. Madrid: Iustel, 2008.

[73] Jordi Barrat. Electoral observation and evoting. *Revista Catalana de Dret Públic*, 39, 2009. `http://ves.cat/fEUH`. Title translated from Catalan.

[74] Jordi Barrat. E-voting vis-à-vis contradictory interests: Profit motivations against democracy. with an special emphasis on non disclosure agreements (NDA). In *Digital democracy, participation and electronic voting*, pages 57–69. Title translated from Spanish. Valencia: CEPS, 2010.

[75] Jordi Barrat, Ben Goldmisht, Rakesh Sharma, Michel Chevallier, and John Turner. Internet voting and individual verifiability: The Norwegian return codes. In *Electronic Voting*, volume P-205 of *(Col. "Lecture Notes in Informatics-LNI")*. Bonn: Gesellschaft für Informatik, 2012.

[76] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. Practical multi-candidate election system. In *Annual ACM symposium on Principles of distributed computing*, pages 274–283. ACM, 2001.

[77] Susan Bell, Josh Benaloh, Michael D Byrne, Dana DeBeauvoir, Bryce Eakin, Gail Fisher, Philip Kortum, Neal McBurnett, Julian Montoya, Michelle Parker, Olivier Pereira, Philip B Stark, Dan S Wallach, and Michael Winn. Star-vote: A secure, transparent, auditable, and reliable voting system. *The USENIX Journal of Election Technology Systems, 1 (1)*, pages 18–37, 2013.

[78] Giampaolo Bella, Peter Y A Ryan, and Vanessa Teague. Virtually perfect democracy. In *Security Protocols XVIII*, pages 161–166. Springer, 2014.

[79] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM conference on Computer and communications security*, pages 62–73. ACM, 1993.

[80] Jonathan Ben-Nun, Niko Fahri, Morgan Llewellyn, Ben Riva, Alon Rosen, Amnon Ta-Shma, and Douglas Wikström. A new implementation of a dual (paper and cryptographic) voting system. In *Electronic Voting*, pages 315–329, 2012.

[81] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In *Advances in Cryptology–CRYPTO 2013*, pages 90–108. Springer, 2013.

[82] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. In *Advances in Cryptology–CRYPTO 2014*, pages 276–294. Springer, 2014.

[83] Josh Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis. Yale University, Department of Computer Science Department, 1987.

[84] Josh Benaloh. Simple verifiable elections. In *USENIX/Accurate Electronic Voting Technology Workshop*, pages 5–5. USENIX Association, 2006.

[85] Josh Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In *USENIX Workshop on Accurate Electronic Voting Technology*, 2007.

[86] Josh Benaloh. Administrative and public verifiability: can we have both? *EVT*, 8:1–10, 2008.

[87] Josh Benaloh, Douglas Jones, Eric Lazarus, Mark Lindeman, and Philip B Stark. Soba: Secrecy-preserving observable ballot-level audits. *EVT/WOTE*, 2011.

[88] Josh Benaloh and Eric Lazarus. The trash attack: An attack on verifiable voting systems and a simple mitigation. Technical report, Technical Report MSR-TR-2011-115, Microsoft, 2011.

[89] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections. In *ACM symposium on Theory of computing*, pages 544–553. ACM, 1994.

[90] Josh Benaloh, Serge Vaudenay, and Jean-Jacques Quisquater. Iacr 2010 election results, 2010. `http://www.iacr.org/elections/2010`.

[91] Josh C Benaloh and Moti Yung. Distributing the power of a government to enhance the privacy of voters. In *ACM symposium on Principles of distributed computing*, pages 52–62. ACM, 1986.

[92] Cory Bennett. States ditch electronic voting machines, November 2, 2014. `http://thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines`.

[93] Scott Bennett and Rob Lundie. Australian electoral systems, 2007. Parliamentary Library Research Paper Series, No. 5, Parliament of Australia, Department of Parliamentary Services.

[94] Lynn Bennie. Transition to STV: Scottish local government elections 2007. *Representation*, 42(4):273–287, 2006.

[95] Kenneth Benoit. Hungary: Holding back the tiers. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 231–252. Oxford University Press, 2005.

[96] David Bernhard, Veronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. SoK: A comprehensive analysis of game-based ballot privacy definitions. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 5 2015.

[97] David Bernhard, Véronique Cortier, Olivier Pereira, Ben Smyth, and Bogdan Warinschi. Adapting Helios for provable ballot privacy. In *Computer Security–ESORICS 2011*, pages 335–354. Springer, 2011.

[98] David Bernhard, Véronique Cortier, Olivier Pereira, and Bogdan Warinschi. Measuring vote privacy, revisited. In *ACM conference on Computer and communications security*, pages 941–952. ACM, 2012.

[99] David Bernhard, Olivier Pereira, and Bogdan Warinschi. How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios. In *Advances in Cryptology–ASIACRYPT 2012*, pages 626–643. Springer, 2012.

[100] David Bernhard and Bogdan Warinschi. Cryptographic voting – a gentle introduction. In *Foundations of Security Analysis and Design VII*, pages 167–211. Springer, 2014.

[101] John Bethencourt, Dan Boneh, and Brent Waters. Cryptographic methods for storing ballots on a voting machine. In *NDSS*, 2007.

[102] Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue. A messy state of the union: Taming the composite state machines of TLS. In *IEEE Symposium on Security and Privacy*, 2015.

[103] David Bismark, James Heather, Roger Peel, Steve Schneider, Zhe Xia, and Peter Y A Ryan. Experiences gained from the first pret a voter implementation. In *International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE)*, pages 19–28. IEEE, 2010.

[104] André Blais. The classification of electoral systems. *European Journal of Political Research*, 16(1):99–110, 1988.

[105] Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee. Source code review of the Sequoia voting system, July 2007. `http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-source-public-jul26.pdf`.

[106] David Bogado and Danny O'Brien. Buenos Aires censors and raids the technologists fixing its flawed e-voting system. EFF Deeplinks Blog, July 15, 2015. `https://www.eff.org/deeplinks/2015/07/buenos-aires-censors-and-raids-technologists-fixing-its-flawed-e-voting-system`.

[107] J-M Bohli, Christian Henrich, Carmen Kempka, J Muller-Quade, and S Rohrich. Enhancing electronic voting machines on the example of Bingo voting. *IEEE Transactions on Information Forensics and Security*, 4(4):745–750, 2009.

[108] Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Röhrich. Bingo voting: Secure and coercion-free voting using a trusted random number generator. In *E-Voting and Identity*, pages 111–124. Springer, 2007.

[109] Ingo Boltz. evoting system certification in the USA. federal vs. state. In *eVoting Certification Seminar*, 2009. `http://www.coe.int/t/dgap/goodgovernance/Source/EVoting/Workshops/Certification/26-27Nov_2009/Certification_USA.ppt`.

[110] Dan Boneh. The decision diffie-hellman problem. In *Algorithmic Number Theory Symposium*, pages 48–63. Springer, 1998.

[111] Shaun Bowler, Todd Donovan, and Jennifer Van Heerde. The united states of america: Perpetual campaigning in the absence of competition. *The politics of electoral systems*, pages 185–207, 2005.

[112] Udo C Braendle. Shareholder protection in the USA and Germany - "law and finance" revisited. *German Law Journal*, 7(3):257–278, 2006.

[113] Felix Brandt. Efficient cryptographic protocol design based on distributed el gamal encryption. In *Information Security and Cryptology-ICISC 2005*, pages 32–47. Springer, 2006.

[114] Jennie Bretschneider, Sean Flaherty, Susannah Goodman, Mark Halvorson, Roger Johnston, Mark Lindeman, Ronald L Rivest, Pam Smith, and Philip B Stark. Risk-limiting post-election audits: Why and how, 2012. `http://statistics.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf`.

[115] Ian Brightwell, Jordi Cucurull, David Galindo, and Sandra Guasch. An overview of the iVote 2015 voting system, August 2015. `https://www.elections.nsw.gov.au/__data/assets/pdf_file/0019/204058/An_overview_of_the_iVote_2015_voting_system_v4.pdf`.

[116] Jonathan Brossard. Hardware backdooring is practical. *BlackHat, Las Vegas, USA*, 2012.

[117] Shuki Bruck, David Jefferson, and Ronald L Rivest. A modular voting architecture ("frog voting"). In *Towards Trustworthy Elections*, pages 97–106. Springer, 2010.

[118] Amilcar Brunazo Filho and Augusto Tavares Rosa Marcacini. Legal aspects of e-voting in Brazil. In Ardita Driza / Jordi Barrat, editor, *E-Voting Case Law. A Comparative Analysis*, pages 65–87. Farnham: Ashgate, 2015.

[119] Johannes Buchmann, Denise Demirel, and Jeroen van de Graaf. Towards a publicly-verifiable mix-net providing everlasting privacy. In *Financial Cryptography and Data Security*, pages 197–204. Springer, 2013.

[120] Jurlind Budurushi, Stephan Neumann, Maina M Olembo, and Melanie Volkamer. Pretty understandable democracy: A secure and understandable Internet voting scheme. In *International Conference on Availability, Reliability and Security (ARES)*, pages 198–207. IEEE, 2013.

[121] Philippe Bulens, Damien Giry, Olivier Pereira, et al. Running mixnet-based elections with Helios. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. Usenix*, 2011.

[122] Bundesverfassungsgericht Press release no. 19/2009. Use of voting computers in 2005 Bundestag election unconstitutional, 2009. `https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html`.

[123] Sergiu Bursuc, Gurchetan S Grewal, and Mark Ryan. Trivitas: Voters directly verifying votes. In *E-Voting and Identity*, pages 190–207. Springer, 2012.

[124] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y A Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. A supervised verifiable voting protocol for the Victorian Electoral Commission. In *International Conference on Electronic Voting*, 2012.

[125] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y A Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. Using prêt á Voter in the Victorian state elections. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*, 2012.

[126] Craig Burton, Chris Culnane, and Steve Schneider. Verifiable electronic voting in practice: the use of vvote in the victorian state election. *IEEE Security & Privacy*, 2016.

[127] Michael D Byrne, Kristen K Greene, and Sarah P Everett. Usability of voting systems: Baseline data for paper, punch cards, and lever machines. In *PSIGCHI conference on Human factors in computing systems*, pages 171–180. ACM, 2007.

[128] Susanne Caarls. *E-voting Handbook: Key steps in the implementation of e-enabled elections*. Council of Europe, 2010.

[129] Joseph A Calandrino, Ariel J Feldman, J Alex Halderman, David Wagner, Harlan Yu, and William P Zeller. Source code review of the Diebold voting system, July 2007. `http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf`.

[130] California Secretary of State's Office. "Top-to-Bottom" Review of voting systems, main website, 2007. `http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/`.

[131] Bryan Campbell, Michael D Byrne, et al. Straight-party voting: what do voters think? *IEEE Transactions on Information Forensics and Security*, 4(4):718–728, 2009.

[132] Bryan A Campbell and Michael D Byrne. Now do voters notice review screen anomalies? a look at voting system usability. In *Proceedings of the 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2009.

[133] Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L Rivest, Emily Shen, et al. Scantegrity ii municipal election at takoma park: the first e2e binding governmental election with ballot privacy. In *USENIX Security*, pages 19–19. USENIX Association, 2010.

[134] Richard Carback, Alan Sherman, and Lynn Baumeister. Data analysis report from Takoma Park 2011 municipal election. Technical report, Scantegrity, 2012.

[135] Richard Carback, Alan Sherman, Travis Mayberry, Paul Herrnson, Bimal Sinha, Aleks Essex, Jeremy Clark, Ron Rivest, Emily Shen, Poorvi Vora, Stefan Popoveniuc, John Conway, and David Chaum. Exploring reactions to Scantegrity: Analysis of surveys of Takoma Park voters and election judges. Technical report, Scantegrity, 2009.

[136] Richard T Carback III, Jeremy Clark, Aleks Essex, and Stefan Popoveniuc. On the independent verification of a Punchscan election. *Proc. VoComp*, 42, 2007.

[137] Carter Center. Developing a methodology for observing electronic voting. *Atlanta*, 2007.

[138] Carter Center. Observing the 2006 presidential elections in venezuela. *Final Report of the Technical Mission*, 2007.

[139] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of cryptology*, 1(1):65–75, 1988.

[140] David Chaum. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In *Advances in Cryptology–EUROCRYPT'88*, pages 177–182. Springer, 1988.

[141] David Chaum. SureVote, 2000. `http://www.surevote.com`.

[142] David Chaum. Surevote: technical overview. In *Workshop on trustworthy elections (WOTE'01)*, 2001.

[143] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE security & privacy*, 2(1):38–47, 2004.

[144] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L Rivest, Peter Y A Ryan, Emily Shen, and Alan T Sherman. Scantegrity ii: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *Conference on Electronic voting technology (EVT'08)*, page 14. USENIX Association, 2008.

[145] David Chaum, Richard T Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L Rivest, Peter Y A Ryan, Emily Shen, Alan T Sherman, and Poorvi L Vora. Scantegrity ii: End-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE Transactions on Information Forensics and Security*, 4(4):611–627, 2009.

[146] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *Security & Privacy, IEEE*, 6(3):40–46, 2008.

[147] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In *Advances in Cryptology—CRYPTO'86*, pages 200–212. Springer, 1987.

[148] David Chaum, Ben Hosp, Stefan Popoveniuc, and Poorvi L Vora. Accessible voter-verifiability. *Cryptologia*, 33(3):283–291, 2009.

[149] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In *Advances in Cryptology–CRYPTO'92*, pages 89–105. Springer, 1993.

[150] David Chaum, Peter Y A Ryan, and Steve Schneider. A practical, voter-verifiable election scheme. Technical Report CS-TR-880, University of Newcastle upon Tyne School of Computing Science, December 2004. `http://www.cs.ncl.ac.uk/research/pubs/trs/papers/880.pdf`.

[151] David Chaum, Peter Y A Ryan, and Steve Schneider. A practical voter-verifiable election scheme. In *Computer Security – ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 118–139. Springer Berlin Heidelberg, 2005.

[152] David Chaum, Jeroen Van De Graaf, Peter Y A Ryan, and Poorvi L Vora. *Secret ballot elections with unconditional integrity*. University of Newcastle upon Tyne, Computing Science, 2007.

[153] David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[154] Stephen Checkoway, Ariel J Feldman, Brian Kantor, J Alex Halderman, Edward W Felten, and Hovav Shacham. Can dres provide long-lasting security? the case of return-oriented programming and the avc advantage. *EVT/WOTE*, 2009, 2009.

[155] Jacek Cichoń, Mirosław Kutyłowski, and Bogdan Weglorz. Short ballot assumption and threeballot voting protocol. In *SOFSEM 2008: Theory and Practice of Computer Science*, pages 585–598. Springer, 2008.

[156] J Clark, A Essex, and C. Adams. Secure and observable auditing of electronic voting systems using stock indices. In *Proceedings, IEEE CCECE*, 2007.

[157] Jeremy Clark and Urs Hengartner. On the use of financial data as a random beacon. In *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, EVT/WOTE'10, 2010.

[158] Jeremy Clark and Urs Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In *Financial Cryptography and Data Security*, pages 47–61. Springer, 2012.

[159] Michael R Clarkson, Stephen Chong, and Andrew C Myers. Civitas: Toward a secure voting system. In *IEEE Symposium on Security and Privacy*, pages 354–368. IEEE Computer Society, 2008.

[160] Mark Clayton. Ukraine election narrowly avoided "wanton destruction" from hackers, June 2014. http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

[161] Josh D Cohen and Michael J Fischer. A robust and verifiable cryptographically secure election scheme. In *26th Annual Symposium on Foundations of Computer Science*, pages 372–382. IEEE, 1985.

[162] Kevin J Coleman and Eric A Fischer. The help america vote act and elections reform: Overview and issues, 2011.

[163] MacCárthaigh Colm. *Electronic Voting in Ireland*. Irish Citizens for Trustworthy E-voting, 2004. http://www.stdlib.net/~colmmacc/e-voting-ireland.pdf.

[164] Commission. *Report and Recommendations of the Presidential Commission on Election Administration*. 2014. http://www.supportthevoter.gov.

[165] European Commission. *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*. 2002.

[166] European Commission. *Methodological Guide to Electoral Assistance, European Commission: Brussel*. 2006.

[167] European Commission. *Compendium of International Electoral Standards: Second Edition*. 2007.

[168] Compuware. Direct recording electronic (DRE) technical security assessment report, 2003. http://www.sos.state.oh.us/sos/hava/compuware112103.pdf.

[169] Clyde H. Coombs. *A theory of data*. John Wiley & Sons, 1964.

[170] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachène. Distributed elgamal á la pedersen: application to Helios. In *ACM Workshop on Workshop on Privacy in the Electronic Society*, pages 131–142. ACM, 2013.

[171] Véronique Cortier, David Galindo, Stephane Glondu, and Malika Izabachene. A generic construction for voting correctness at minimum cost-application to Helios. *IACR Cryptology ePrint Archive*, 2013:177, 2013.

[172] Véronique Cortier, David Galindo, Stephane Glondu, and Malika Izabachene. Election verifiability for Helios under weaker trust assumptions. In *Computer Security-ESORICS*, pages 327–344. Springer, 2014.

[173] Véronique Cortier and Ben Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. *Journal of Computer Security*, 21(1):89–148, 2013.

[174] Olivier Costa, André Freire, and Jean-Benoit Pilet. Political representation in Belgium, France and Portugal: MPs and their constituents in very different political systems. *Representation*, 48(4):351–358, 2012.

[175] Gary W Cox, Frances M Rosenbluth, and Michael F Thies. Electoral rules, career ambitions, and party structure: comparing factions in Japan's upper and lower houses. *American Journal of Political Science*, 44(1):115–122, 2000.

[176] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Advances in Cryptology—CRYPTO'94*, pages 174–187. Springer, 1994.

[177] Ronald Cramer, Matthew Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority secret-ballot elections with linear work. In *Advances in Cryptology—EUROCRYPT'96*, pages 72–83. Springer, 1996.

[178] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology–EUROCRYPT'97*, pages 103–118. Springer, 1997.

[179] Lorrie Faith Cranor and Ron K Cytron. Sensus: A security-conscious electronic polling system for the internet. In *Thirtieth Hawaii International Conference on System Sciences*, volume 3, pages 561–570. IEEE, 1997.

[180] Mariano Cucho and Mariano Augusto. Electronic voting: Lessons learned before and after its implementation on ERM 2014. *Elecciones*, 14:11–29, 2014. titled translated from Spanish.

[181] Chris Culnane, David Bismark, James Heather, Steve Schneider, Sriramkrishnan Srinivasan, and Zhe Xia. Authentication codes. In *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'11)*, 2011.

[182] Chris Culnane, James Heather, Rui Joaquim, Peter Y A Ryan, Steve Schneider, and Vanessa Teague. Faster print on demand for prêt à voter. *USENIX Journal of Election Technology and Systems*, 2(1), 2013.

[183] Chris Culnane, Peter Y A Ryan, Steve Schneider, and Vanessa Teague. vVote: a verifiable voting system. *arXiv preprint arXiv:1404.6822*, 2014.

[184] Chris Culnane, Peter Y A Ryan, Steve Schneider, and Vanessa Teague. vVote: A verifiable voting system. *ACM Transactions on Information and System Security*, 18(1):3:1–3:30, 2015.

[185] Chris Culnane and Steve Schneider. A peered bulletin board for robust use in verifiable voting systems. In *IEEE 27th Computer Security Foundations Symposium (CSF)*, pages 169–183. IEEE, 2014.

[186] Edouard Cuvelier, Olivier Pereira, and Thomas Peters. Election verifiability or ballot privacy: Do we need to choose? In *Computer Security–ESORICS 2013*, pages 481–498. Springer, 2013.

[187] Ivan Damgård. On Σ-protocols, 2004. http://www.daimi.au.dk/~ivan/Sigma.ps.

[188] Ivan Damgård and Mads Jurik. A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In *Public Key Cryptography*, volume 1992 of *LNCS*, pages 119–136. Springer, 2001.

[189] George Danezis. *Better anonymous communications*. PhD thesis, University of Cambridge, 2004.

[190] DCBOEE press release. Board announces public test of Digital Vote by Mail service, September 2010. http://www.dcboee.org/popup.asp?url=/pdf_files/nr_588.pdf.

[191] Ajuntament de Barcelona. *Report on the Popular Consultation of Diagonal Avenue*. Barcelona: Ajuntament de Barcelona, 2010. http://www.vilaweb.cat/media/attach/vwedts/docs/informediagonal.pdf. Title translated from Catalan.

[192] Nicolas de Condorcet. *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix*. Paris: l'Imprimerie Royale, 1785.

[193] Fédération Internationale de Gymnastique. FIG code of points 2013–2016, trampoline gymnastics. http://www.fig-gymnastics.com/site/.

[194] Stephanie Delaune, Steve Kremer, and Mark Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Computer Security Foundations Workshop, 2006. 19th IEEE*, pages 12–pp. IEEE, 2006.

[195] Alex Delis, Konstantina Gavatha, Aggelos Kiayias, Charalampos Koutalakis, Elias Nikolakopoulos, Lampros Paschos, Mema Rousopoulou, Georgios Sotirellis, Panos Stathopoulos, Pavlos Vasilopoulos, Thomas Zacharias, and Bingsheng Zhang. Pressing the button for European elections: verifiable e-voting and public attitudes toward internet voting in Greece. In *International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, pages 1–8. IEEE, 2014.

[196] Denise Demirel, Jeroen Van De Graaf, and Roberto Araújo. Improving Helios with everlasting privacy towards the public. In J Alex Halderman and Olivier Pereira, editors, *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE'12*. USENIX Association, 2012.

[197] Community Department of the Environment and The Government of the Republic of Ireland Local Government. How the president is elected. http://www.environ.ie/en/LocalGovernment/Voting/.

[198] Yvo Desmedt and Pyrros Chaidos. Applying divertibility to blind ballot copying in the Helios internet voting system. In *Computer Security–ESORICS 2012*, pages 433–450. Springer, 2012.

[199] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. In *Advances in Cryptology–CRYPTO'89 Proceedings*, pages 307–315. Springer, 1990.

[200] Collège d'Experts. *Report on Elections June 13th 1999*. 1999. `http://www.poureva.be/IMG/pdf/19990701.pdf`. Title translated from French.

[201] Collège d'Experts. *Report on Elections May 18th 2003*. 2003. `http://www.poureva.be/IMG/pdf/RapportExpert20030605.pdf`. Title translated from French.

[202] Collège d'Experts. *The Simultaneous Elections on May 25th 2014*. 2014. `http://www.poureva.be/IMG/pdf/54K0014001.pdf`. Title translated from French.

[203] Roberto Di Cosmo. On privacy and anonymity in electronic and non electronic voting: the ballot-as-signature attack. *Hyper Articles en Ligne hal-00142440 (2)*, 2007.

[204] Alberto Díaz-Cayeros and Beatriz Magaloni. Mexico: Designing electoral rules by a dominant party. In Josep M. Colomer, editor, *Handbook of Electoral System Choice*, pages 145–154. Palgrave Macmillan, 2004.

[205] Diebold Election Systems. Press release: State of Maryland awards Diebold electronic voting equipment order valued at up to $55.6 million, 2003. `http://www.diebold.com/news/newsdisp.asp?id=2979`.

[206] Diebold Election Systems. Technical response to the Johns Hopkins study on voting systems, 2003. `http://www-personal.umich.edu/~wmebane/gov317/diebold/technical.25jul2003.htm`.

[207] Jérôme Dossogne and Frédéric Lafitte. Blinded additively homomorphic encryption schemes for self-tallying voting. *Journal of Information Security and Applications*, 2014.

[208] John Duggan and Thomas Schwartz. Strategic manipulability without resoluteness or shared beliefs: Gibbard-satterthwaite generalized. *Social Choice and Welfare*, 17(1):85–93, 2000.

[209] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J Alex Halderman. Tracking the FREAK attack, March 2015. `https://freakattack.com/`.

[210] Maurice Duverger. *Political Parties: Their Organisation and Activity in the Modern State*. London: Methuen, Wiley, 1963.

[211] Election Science Institute. 2006 voting equipment study. `http://www.edssurvey.com/images/File/ve2006_nrpt.pdf`.

[212] Princeton Undergraduate Elections. https://princeton.heliosvoting.org/.

[213] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology*, pages 10–18. Springer, 1985.

[214] Robert Elgie. France: Stacking the deck. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 119–136. Oxford University Press, 2005.

[215] Aleks Essex, Jeremy Clark, and Carlisle Adams. Aperio: High integrity elections for developing countries. In *Towards Trustworthy Elections*, pages 388–401. Springer, 2010.

[216] Aleks Essex, Jeremy Clark, Richard Carback, and Stefan Popoveniuc. Punchscan in practice: an e2e election case study. In *Workshop on Trustworthy Elections*, 2007.

[217] Aleks Essex, Jeremy Clark, Urs Hengartner, and Carlisle Adams. How to print a secret. In *Proceedings of the 4th USENIX conference on Hot topics in security, Hot-Sec*, volume 9, pages 3–3, 2009.

[218] Aleksander Essex, Jeremy Clark, Urs Hengartner, and Carlisle Adams. Eperio: Mitigating technical complexity in cryptographic election verification. *IACR Cryptology ePrint Archive*, 2012:178, 2012.

[219] Aleksander Essex and Urs Hengartner. Hover: Trustworthy elections with hash-only verification. *IEEE Security & Privacy*, 10(5):18–24, 2012.

[220] Aleksander Essex and Urs Hengartner. Oblivious printing of secret messages in a multi-party setting. In *Financial Cryptography and Data Security*, pages 359–373. Springer, 2012.

[221] Aleksander Essex, Christian Henrich, and Urs Hengartner. Single layer optical-scan voting with fully distributed trust. In *E-Voting and Identity*, pages 122–139. Springer, 2012.

[222] Saghar Estehghari and Yvo Desmedt. Exploiting the client vulnerabilities in internet e-voting systems: Hacking Helios 2.0 as an example. In *Electronic Voting Technology Workship/Workshop on Trustworthy Elections (EVT/WOTE)*, 2010.

[223] Estonian Internet Voting Committee. Statistics about Internet voting in Estonia, May 2014. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

[224] Estonian Internet Voting Committee. Using ID-card and mobil-ID, May 2014. https://www.valimised.ee/eng/kkk.

[225] Estonian Public Broadcasting. Center Party petitions European human rights court over e-voting, 2013. http://news.err.ee/v/politics/4ee0c8a2-b9c2-4d28-8ae4-061e7d9386a4.

[226] Sarah Everett, Kristen Greene, Michael Byrne, Dan Wallach, Kyle Derr, Daniel Sandler, and Ted Torous. Is newer always better? the usability of electronic voting machines versus traditional methods. *CHI*, 2008.

[227] Sarah P Everett. *The usability of electronic voting machines and how votes can be changed without detection*. PhD thesis, RICE UNIVERSITY, 2007.

[228] Sarah P Everett, Michael D Byrne, and Kristen K Greene. Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 50, pages 2547–2551. SAGE Publications, 2006.

[229] David Farrell and Ian McAllister. Australia: the alternative vote in a compliant political culture. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 79–98. Oxford University Press, 2005.

[230] David M Farrell. *Electoral Systems: A Comparative Introduction*. Palgrave Macmillan, 2nd edition, 2011.

[231] David M. Farrell, Malcolm Mackerras, and Ian McAllister. Designing electoral institutions: STV systems and their consequences. *Political studies*, 44(1):24–43, 1996.

[232] Ariel J Feldman, J Alex Halderman, and Edward W Felten. Security analysis of the diebold accuvote-ts voting machine. 2006.

[233] Ariel J Feldman, J Alex Halderman, and Edward W Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

[234] Edward W Felten. "Hotel minibar" keys open Diebold voting machines. Freedom to Tinker blog, 2006. https://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines/.

[235] Niels Ferguson and Bruce Schneier. *Practical cryptography*. Wiley New York, 2003.

[236] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology—CRYPTO'86*, pages 186–194. Springer, 1987.

[237] Russell A Fink, Alan T Sherman, and Richard Carback. TPM meets DRE: reducing the trust base for electronic voting using trusted platform modules. *Information Forensics and Security, IEEE Transactions on*, 4(4):628–637, 2009.

[238] Kevin Fisher, Richard Carback, and Alan T Sherman. Punchscan: Introduction and system definition of a high-integrity election system. In *Workshop on Trustworthy Elections (WOTE)*, 2006.

[239] Catherine Fisk and Erwin Chemerinsky. The filibuster. *Stanford Law Review*, 49(2):181–254, 1997.

[240] Offce for Democratic Institutions and Human Rights. *Estonia Parliamentary Elections 6 March 2011 OCSE/ODIHR Election Assessment Mission Final Report*.

[241] Centre for Human Rights. Professional training series no.2: Human rights and elections – a handbook on the legal technical and human rights aspects of elections. 1994.

[242] Organization for Security and Cooperation in Europe. *Supplementary Human Dimension Meeting on Challenges of Election Technologies and Procedures, 21-22 April 2005: Final Report*. Organization for Security and Cooperation in Europe, 2005. http://www.osce.org/odihr/elections/15996.

[243] Organization for Security and Cooperation in Europe. *Election Observation Handbook: Fifth Edition*. The OSCE Office for Democratic Institutions and Human Rights, 2007. http://www.osce.org/odihr/elections/14355?download=true.

[244] Organization for Security and Cooperation in Europe. *Discussion Paper in Preparation of Guidelines for the Observation of Electronic Elections*. Organization for Security and Cooperation in Europe, 2008. http://www.osce.org/odihr/elections/34725.

[245] Organization for Security and Cooperation in Europe. *Handbook for the Observation of New Voting Technologies*. Organization for Security and Cooperation in Europe, 2013. http://www.osce.org/odihr/elections/104939.

[246] Organization for Security and Cooperation in Europe (OSCE). Netherlands. Parliamentary Elections, 22 November 2006. Election Assessment Mission Report, 2006. http://www.osce.org/odihr/elections/netherlands/24322.

[247] Michael Gallagher. Comparing proportional representation electoral systems: Quotas, thresholds, paradoxes and majorities. *British Journal of Political Science*, 22(04):469–496, 1992.

[248] Michael Gallagher. Ireland: the discreet charm of PR-STV. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 511–532. Oxford University Press, 2005.

[249] Michael Gallagher and Paul Mitchell, editors. *The Politics of Electoral Systems*. Oxford University Press, 2005.

[250] David Geer. Technical maturity, reliability, implicit taxes, and wealth creation. *login: The magazine of Usenix & Sage*, 26(8), 2001.

[251] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct nizks without pcps. In *EUROCRYPT*, volume 7881, pages 626–645. Springer, 2013.

[252] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology*, 20(1):51–83, 2007.

[253] Allan Gibbard. Manipulation of voting schemes: A general result. *Econometrica: journal of the Econometric Society*, pages 587–601, 1973.

[254] Kristian Gjøsteen. A latency-free election scheme. In *Topics in Cryptology–CT-RSA 2008*, pages 425–436. Springer, 2008.

[255] Kristian Gjøsteen. Analysis of an internet voting protocol. *IACR Cryptology ePrint Archive*, 380, 2010.

[256] Kristian Gjøsteen. The Norwegian internet voting protocol. *IACR Cryptology ePrint Archive*, 473, 2013.

[257] Marcin Gogolewski, Marek Klonowski, Przemysław Kubiak, Mirosław Kutyłowski, Anna Lauks, and Filip Zagórski. Kleptographic attacks on e-voting schemes. In *Emerging Trends in Information and Communication Security*, pages 494–508. Springer, 2006.

[258] Oded Goldreich. A short tutorial of zero-knowledge. In *Secure Multi-Party Computation*, Secure Multi-Party Computation 10, pages 28–60, 2013.

[259] Ben Goldsmith. *Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies*. International Foundation for Electoral Systems, 2011. `http://www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf`.

[260] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[261] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[262] Rop Gonggrijp and Willem-Jan Hengeveld. *Nedap/Groenendaal ES3B voting computer security analysis*. Amsterdam: Foundation "Wij vertrouwen stemcomputers niet", 2006. `wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf`.

[263] Rop Gonggrijp and Willem-Jan Hengeveld. Studying the nedap/groenendaal es3b voting computer: A computer security perspective. In *USENIX workshop on accurate electronic voting technology (EVT'07)*, pages 1–1. USENIX Association, 2007.

[264] Rop Gonggrijp, Willem-Jan Hengeveld, Eelco Hotting, Sebastian Schmidt, and Frederik Weidemann. RIES—Rijnland internet election system: A cursory study of published source code. In *VOTE-ID*, 2009.

[265] Ezequiel Gonzalez-Ocantos, Chad Kiewiet De Jonge, Carlos Meléndez, Javier Osorio, and David W Nickerson. Vote buying and social desirability bias: Experimental evidence from nicaragua. *American Journal of Political Science*, 56(1):202–217, 2012.

[266] Guy S Goodwin-Gill. *Free and fair elections*. Inter-Parliamentary Union, 2006.

[267] Amanda Gouws and Paul Mitchell. South Africa: one party dominance despite perfect proportionality. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 353–374. Oxford University Press, 2005.

[268] Kristen K Greene. *Usability of New Electronic Voting Systems and Traditional Methods: Comparisons Between Sequential and Direct Access Electronic Voting Interfaces, Paper Ballots, Punch Cards, and Lever Machines*. PhD thesis, RICE UNIVERSITY, 2008.

[269] Gurchetan S Grewal, Mark Ryan, Sergiu Bursuc, and Peter Y A Ryan. Caveat coercitor: Coercion-evidence in electronic voting. In *IEEE Symposium on Security and Privacy (SP)*, pages 367–381. IEEE, 2013.

[270] Jens Groth. Efficient maximal privacy in boardroom voting and anonymous broadcast. In *Financial Cryptography*, pages 90–104. Springer, 2004.

[271] Jens Groth. Evaluating security of voting schemes in the universal composability framework. In *Applied Cryptography and Network Security*, pages 46–60. Springer, 2004.

[272] Jens Groth. Review of RIES. Technical report, Cryptomathic, 2004.

[273] Eitan Grundland. An analysis of the wombat voting system model, 2012. `http://www.grundland.org/An\%20Analysis\%20of\%20the\%20Wombat\%20Voting\%20System\%20Model.pdf`.

[274] Rolf Haenni and Reto E Koenig. A generic approach to prevent board flooding attacks in coercion-resistant electronic voting schemes. *Computers & Security*, 33:59–69, 2013.

[275] Alireza Toroghi Haghighat, Mohammad Sadeq Dousti, and Rasool Jalili. An efficient and provably-secure coercion-resistant e-voting protocol. In *Annual International Conference on Privacy, Security and Trust (PST)*, pages 161–168. IEEE, 2013.

[276] Lim Hong Hai. Electoral politics in Malaysia: 'managing' elections in a plural society. *Electoral Politics in Southeast and East Asia*, pages 101–148, 2002.

[277] J Alex Halderman. Diebold shows how to make your own voting machine key. Freedom to Tinker blog, 2007. `https://freedom-to-tinker.com/blog/jhalderm/diebold-shows-how-make-your-own-voting-machine-key/`.

[278] J Alex Halderman. Electronic voting researcher arrested over anonymous source. Freedom to Tinker blog, August 2010. `https://freedom-to-tinker.com/blog/jhalderm/electronic-voting-researcher-arrested-over-anonymous-source/`.

[279] J Alex Halderman. Are DREs toxic waste? EVT/WOTE rump session talk, August 2011.

[280] J Alex Halderman. Hacking the D.C. Internet voting pilot. Freedom to Tinker blog, 2011. `http://www.freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot`.

[281] J Alex Halderman and Ariel J Feldman. PAC-MAN on the Sequioia AVC-Edge DRE voting machine, August 2010. `https://jhalderm.com/pacman/`.

[282] J Alex Halderman and Vanessa Teague. The New South Wales iVote system: Security failures and verification flaws in a live online election. In *International Conference on E-Voting and Identity (VoteID'15)*, August 2015.

[283] Joseph Lorenzo Hall. *Design and the Support of Transparency in VVPAT Systems in the US Voting Systems Market*. National Institute of Standards and Technology (NIST), 2006. `http://www.nist.gov/itl/vote/upload/jlh-vvpat-design-transparency.pdf`.

[284] Joseph Lorenzo Hall. Transparency and access to source code in electronic voting. In *EVT'06*. Vancouver: Usenix / Accurate, 2006. `josephhall.org/papers/jhall_evt06.pdf`.

[285] Joseph Lorenzo Hall. Post-election manual auditing of paper records: Bibliography, 2007. `http://www.josephhall.org/papers/auditing_biblio.pdf`.

[286] Ursula Hall. Greeks and romans and the secret ballot. *Owls to Athens: Essays on Classical Subjects Presented to Sir Kenneth Dover, ed. EM Craik, Oxford*, 191:199, 1990.

[287] Feng Hao, Dylan Clarke, and Carlton Shepherd. Verifiable classroom voting: Where cryptography meets pedagogy. In *Security Protocols Workshop*. Springer, 2013.

[288] Feng Hao, Matthew Kreeger, Brian Randell, Dylan Clarke, Siamak F Shahandashti, and Peter Hyun-Jeen Lee. Every vote counts: ensuring integrity in large-scale electronic voting. *The USENIX Journal of Election Technology and Systems*, pages 1–25, 2014.

[289] Feng Hao and Matthew Nicolas Kreeger. Every vote counts: Ensuring integrity in large-scale dre-based electronic voting, 2010. `https://eprint.iacr.org/2010/452.pdf`.

[290] Feng Hao, Brian Randell, and Dylan Clarke. Self-enforcing electronic voting. In *Security Protocols Workshop*. Springer, 2012.

[291] Feng Hao, Peter Y A Ryan, and Piotr Zieliński. Anonymous voting by two-round public discussion. *IET Information Security*, 4(2):62–67, 2010.

[292] Feng Hao and Piotr Zieliński. A 2-round anonymous veto protocol. In *Security Protocols Workshop 2006*, pages 202–211. Springer, 2009.

[293] Feng Hao and Piotr Zieliński. A 2-round anonymous veto protocol (transcript). In *Security Protocols Workshop 2006*, pages 212–214. Springer, 2009.

[294] Feng Hao and Piotr Zieliński. The power of anonymous veto in public discussion. In *Transactions on Computational Science IV*, pages 41–52. Springer, 2009.

[295] Thomas Hare. *The Machinery of Representation*. W. Maxwell, 1857.

[296] Joseph Pratt Harris. *Election administration in the United States*. Number 27. Brookings institution, 1934. `http://www.nist.gov/itl/vote/josephharrisrpt.cfm`.

[297] Ricardo Hausmann and Roberto Rigobón. *Looking for the Black Swan: Statistical Evidence Analysis on Electoral Fraud in Venezuela*. Boston: Harvard University / MIT, 2004. `http://www.proveo.org/hausmann.pdf`. Title translated from Spanish.

[298] Anthony Heath, Siana Glouharova, and Oliver Heath. India: Two-party contests within a multiparty system. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 137–156. Oxford University Press, 2005.

[299] James Heather. Implementing stv securely in prêt à voter. In *Computer Security Foundations Symposium (CSF'07)*, pages 157–169. IEEE, 2007.

[300] James Heather and David Lundin. The append-only web bulletin board. In *Formal Aspects in Security and Trust*, pages 242–256. Springer, 2009.

[301] James Heather, Peter Y A Ryan, and Vanessa Teague. Pretty good democracy for more expressive voting schemes. In *Computer Security–ESORICS 2010*, pages 405–423. Springer, 2010.

[302] Mario Heiderich, Tilman Frosch, Marcus Niemietz, and Jörg Schwenk. The bug that made me president a browser-and web-security case study on Helios voting. In *E-voting and identity*, pages 89–103. Springer, 2012.

[303] Christian Henrich. *Improving and Analysing Bingo Voting*. PhD thesis, Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2012, 2012.

[304] Kevin Henry, Douglas R Stinson, and Jiayuan Sui. The effectiveness of receipt-based attacks on threeballot. *Information Forensics and Security, IEEE Transactions on*, 4(4):699–707, 2009.

[305] Paul S Herrnson, Richard G Niemi, Michael J Hanmer, Benjamin B Bederson, Frederick G Conrad, and Michael Traugott. The importance of usability testing of voting systems. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

[306] Mark A Herschberg. *Secure electronic voting over the world wide web*. PhD thesis, Massachusetts Institute of Technology, 1997.

[307] Allen Hicken. Thailand: Combating corruption through electoral reform. In Andrew Reynolds, Ben Reilly, and Andrew Ellis, editors, *Electoral System Design: The New International IDEA Handbook*, pages 105–107. International Institute for Democracy and Electoral Assistance, 2005.

[308] Richard Hill. Challenging the Geneva e-voting system in court. In *E-Voting Seminar*. Biel: Evoting.ch, 2013. `http://e-voting.bfh.ch/seminar/fall-2013/`.

[309] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *Advances in Cryptology–EUROCRYPT 2000*, pages 539–556. Springer, 2000.

[310] Jonathan K Hodge and Richard E Klima. *The Mathematics of Voting and Elections: A Hands-on Approach*, volume 22 of *Mathematical world*. American Mathematical Society, 2005.

[311] Kjell Hole and Lars-Helge Netland. Toward risk assessment of large-impact and rare events. *IEEE Security & Privacy*, (3):21–27, 2010.

[312] Jonathan Hopkin. Spain: Proportional representation with majoritarian outcomes. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 375–396. Oxford University Press, 2005.

[313] HT Correspondent. "Enhance confidence in EVMs". Hindustan Times, New Delhi, October 4, 2015.

[314] Engelbert Hubbers, Bart Jacobs, Berry Schoenmakers, Henk van Tilborg, and Benne de Weger. Description and analysis of the RIES internet voting system. Technical report, Eindhoven Institute for the Protection of Systems and Information (EiPSI), 2008.

[315] Harri Hursti. Critical security issues with Diebold TSx (unredacted), May 2006. http://www.bbvdocs.org/reports/BBVreportIIunredacted.pdf.

[316] ICTE. *The Accuracy, Secrecy and Testing of the Nedap/Powervote Electronic Voting System*. Irish Citizens for Trustworthy Evoting, 2004. http://www.stdlib.net/~colmmacc/CEV/icte-cev.pdf.

[317] Srinivas Inguva, Eric Rescorla, Hovav Shacham, and Dan S Wallach. Source code review of the Hart InterCivic voting system, July 2007. http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/Hart-source-public.pdf.

[318] Srinivas Inguva, Eric Rescorla, Hovav Shacham, and Dan S Wallach. *Source Code Review of the Hart InterCivic Voting System*. California Sec. of State's "Top to Bottom" Review, July 2007. http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf.

[319] ISO, Geneva, Switzerland. *Ergonomic requirements for office work with visual display terminal (VDT's) – Part 11: Guidance on usability*. ISO 9241-11(E).

[320] Bart Jacobs and Wolter Pieters. Electronic voting in the Netherlands: from early adoption to early abolishment. In *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*, volume 5705 of *LNCS*, pages 121–144. Springer, 2009.

[321] Markus Jakobsson, Ari Juels, and Ronald L Rivest. Making mix nets robust for electronic voting by randomized partial checking. In *USENIX security symposium*, pages 339–353, 2002.

[322] David R Jefferson, Aviel D Rubin, Barbara Simons, and David A Wagner. A security analysis of the secure electronic registration and voting experiment (SERVE), 2004. http://servesecurityreport.org/paper.pdf.

[323] Peter Sandholt Jensen and Mogens K Justesen. Poverty and vote buying: Survey-based evidence from africa. *Electoral Studies*, 33:220–232, 2014.

[324] Rui Joaquim, Paulo Ferreira, and Carlos Ribeiro. Eviv: An end-to-end verifiable internet voting system. *computers & security*, 32:170–191, 2013.

[325] Rui Joaquim and Carlos Ribeiro. An efficient and highly sound voter verification technique and its implementation. In *E-voting and identity*, pages 104–121. Springer, 2012.

[326] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. Veryvote: A voter verifiable code voting system. In *E-voting and identity*, pages 106–121. Springer, 2009.

[327] Douglas Jones. *A Brief Illustrated History of Voting*. Iowa: The University of Iowa, 2001.

[328] Douglas Jones. Some problems with end-to-end voting. In *End-to-End Voting Systems Workshop*. Washington DC: NIST, 2009. homepage.cs.uiowa.edu/~jones/voting/E2E2009.pdf.

[329] Douglas Jones and Barbara Simons. *Broken Ballots. Will Your Vote Count?* Chicago: The University of Chicago Press, 2012.

[330] Douglas W Jones. The case of the Diebold FTP site, 2003. http://homepage.cs.uiowa.edu/~jones/voting/dieboldftp.html.

[331] Douglas W Jones. Kazakhstan: The sailau e-voting system. In Michael Yard, editor, *Direct Democracy: Progress and Pitfalls of Election Technology*. Washington: IFES, 2010. http://homepage.cs.uiowa.edu/~jones/voting/IFESkazakhstan.pdf.

[332] Douglas W Jones and Tom C Bowersox. Secure data export and auditing using data diodes. *Technology*, 6:7, 2006.

[333] Harvey Jones, Jason Juang, and Greg Belote. Threeballot in the field. *Term paper for MIT course*, 6, 2006.

[334] Hugo Jonker, Sjouke Mauw, and Jun Pang. Privacy and verifiability in voting systems: Methods, developments and trends. *Computer Science Review*, 10:1–30, 2013.

[335] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[336] Ralf K üsters, Tomasz Truderung, and Andreas Vogt. Accountability: definition and relationship to verifiability. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 526–535. ACM, 2010.

[337] Erik Kain. Report: NSA intercepting laptops ordered online, installing spyware, December 29, 2013. http://www.forbes.com/sites/erikkain/2013/12/29/report-nsa-intercepting-laptops-ordered-online-installing-spyware/.

[338] Fatih Karayumak, Michaela Kauer, Maina M Olembo, Tobias Volk, and Melanie Volkamer. User study of the improved Helios voting system interfaces. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 37–44. IEEE, 2011.

[339] Fatih Karayumak, Maina M Olembo, Michaela Kauer, and Melanie Volkamer. Usability analysis of Helios – an open source verifiable remote electronic voting system. In *USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2011.

[340] Chris Karlof, Naveen Sastry, and David Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security*, volume 5, pages 33–50, 2005.

[341] John Kelsey, Andrew Regenscheid, Tal Moran, and David Chaum. Attacking paper-based e2e voting systems. In *Towards Trustworthy Elections*, pages 370–387. Springer, 2010.

[342] S Khazaei and D Wikström. Randomized partial checking revisited. In *Topics in Cryptology - CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 115–128. Springer Berlin Heidelberg, 2013.

[343] Aggelos Kiayias, Michael Korman, and David Walluck. An internet voting system supporting user privacy. In *Annual Computer Security Applications Conference (ACSAC'06), 2006*, pages 165–174. IEEE, 2006.

[344] Aggelos Kiayias and Moti Yung. Self-tallying elections and perfect ballot secrecy. In *Public Key Cryptography*, pages 141–158. Springer, 2002.

[345] Aggelos Kiayias and Moti Yung. Non-interactive zero-sharing with applications to private distributed decision making. In *Financial Cryptography*, pages 303–320. Springer, 2003.

[346] Aggelos Kiayias and Moti Yung. The vector-ballot e-voting approach. In *Financial Cryptography*, pages 72–89. Springer, 2004.

[347] Joe Kilian. A note on efficient zero-knowledge proofs and arguments. In *Annual ACM Symposium on Theory of Computing*, STOC '92, pages 723–732, 1992.

[348] Melanie Kiser. Internet voting 2.0 and other advances in election technology in Takoma Park, 2011. `http://www.fairvote.org/internet-voting-2-0-and-other-advances-in-election-technology-in-takoma-park`.

[349] Marek Klonowski, Mirosław Kutyłowski, Anna Lauks, and Filip Zagórski. A practical voting scheme with receipts. In *Information Security*, pages 490–497. Springer, 2005.

[350] Reto Koenig, Rolf Haenni, and Stephan Fischli. Preventing board flooding attacks in coercion-resistant electronic voting schemes. In *Future Challenges in Security and Privacy for Academia and Industry*, pages 116–127. Springer, 2011.

[351] Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin, and Dan S Wallach. Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy, 2004. Proceedings*, pages 27–40. IEEE, 2004.

[352] Petr Kopecký. The Czech Republic: Entrenching proportional representation. In Josep M Colomer, editor, *Handbook of Electoral System Choice*, pages 347–358. Palgrave Macmillan, 2004.

[353] Steve Kremer, Mark Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. *Computer Security–ESORICS*, pages 389–404, 2010.

[354] Robert Krimmer. Electronic voting. *GI Lecture Notes in Informatics, P-86, Bonn*, 2006.

[355] Taisya Krivoruchko. Robust coercion-resistant registration for remote e-voting. In *Workshop on Trustworthy Elections (WOTE'07)*, 2007.

[356] R Kusters, T Truderung, and A Vogt. Clash attacks on the verifiability of e-voting systems. In *2012 IEEE Symposium on Security and Privacy*, pages 395–409, 2012.

[357] Ralf Kusters, Tomasz Truderung, and Andreas Vogt. Clash attacks on the verifiability of e-voting systems. In *IEEE Symposium on Security and Privacy (SP)*, pages 395–409. IEEE, 2012.

[358] Mirosław Kutyłowski and Filip Zagórski. Scratch, click & vote: E2e voting over the internet. In *Towards trustworthy elections*, pages 343–356. Springer, 2010.

[359] Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer. A taxonomy refining the security requirements for electronic voting: analyzing Helios as a proof of concept. In *International Conference on Availability, Reliability, and Security (ARES'10)*, pages 475–480. IEEE, 2010.

[360] Sharon J Laskowski, Marguerite Autry, John Cugini, William Killam, and James Yen. Improving the usability and accessibility of voting systems and products. *NIST Special Publication*, 2004.

[361] Arjen K Lenstra and Hendrik W Lenstra Jr. Algorithms in number theory. Technical report, Elsevier, 1990.

[362] Rafi Letzter. A new voting machine could make sure every vote really counts, 2014. `http://www.popsci.com/article/technology/new-voting-machine-could-make-sure-every-vote-really-counts`.

[363] Samantha Levine. Hanging Chads: As the Florida Recount Implodes, the Supreme Court Decides Bush v. Gore, Jan. 17 2008. `http://www.usnews.com/news/articles/2008/01/17/the-legacy-of-hanging-chads`.

[364] LexisNexis. 2014 LexisNexis true cost of fraud study, August 2014. `http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf`.

[365] Andra Lim. Travis county, tx developing electronic voting system with a paper trail, July 15 2014. http://www.govtech.com/products/Travis-County-TX-Developing-Electronic-Voting-System-With-a-Paper-Trail.html.

[366] Mark Lindeman, Mark Halvorson, Pamela Smith, Lynn Garland, and Vittorio Addona. Principles and best practices for post-election audits. 2008. http://www.electionaudits.org/files/best%20practices%20final_0.pdf.

[367] Mark Lindeman and Philip B Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, (5):42–49, 2012.

[368] Helger Lipmaa. Paper-voted (and why I did so), 2011. http://helger.wordpress.com/2011/03/05/paper-voted-and-why-i-did-so/.

[369] Yining Liu, Peiyong Sun, Jihong Yan, Yajun Li, and Jianyu Cao. An improved electronic voting scheme without a trusted random number generator. In *Information Security and Cryptology*, pages 93–101. Springer, 2012.

[370] Mieke Loncke and Jos Dumortier. Online voting: a legal perspective. *International Review of Law, Computers & Technology*, 18(1):59–79, 2004.

[371] Panos Louridas, Georgios Tsoukalas, Kostas Papadimitriou, and Panayiotis Tsanakas. Zeus: Bringing internet voting to greece. In *E-Democracy, Security, Privacy and Trust in a Digital World*, pages 213–223. Springer, 2014.

[372] Simon Luechinger, Myra Rosinger, and Alois Stutzer. The impact of postal voting on participation: Evidence for switzerland. *Swiss Political Science Review*, 13(2):167–202, 2007.

[373] Anders Smedstuen Lund. Refining the internet voting protocol. Master's thesis, Norwegian University of Science and Technology, June 2011.

[374] David Lundin and Peter Y A Ryan. Human readable paper verification of Prêt à Voter. In *European Symposium on Research in Computer Security (ESORICS'08)*, pages 379–395. Springer-Verlag, 2008.

[375] Georg Lutz. First come, first served: the effect of ballot position on electoral success in open ballot PR elections. *Representation*, 46(2):167–181, 2010.

[376] Epp Maaten. Towards remote e-voting: Estonian case. *Electronic Voting in Europe*, 47:83–100, 2004.

[377] Ülle Madise and Tarvi Martens. E-voting in Estonia 2005. the first practice of country-wide binding internet voting in the world. *Electronic voting*, 86, 2006.

[378] Pieter Maene. Helios election system. `https://github.com/Pmaene/Helios`.

[379] Mandiant. APT1: Exposing one of China's cyber espionage units, February 2013. `http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf`.

[380] Tarvi Martens. Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, 3(1):213–233, 2010.

[381] Rubén Martínez Dalmau. Venezuela: Finding the relationship between e-voting and democracy. In Ardita Driza / Jordi Barrat, editor, *E-Voting Case Law. A Comparative Analysis*, pages 261–275. Farnham: Ashgate, 2015.

[382] Louis Massicotte. Canada: Sticking to first-past-the-post, for the time being. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 99–118. Oxford University Press, 2005.

[383] Richard E Matland. Enhancing women's political participation: Legislative recruitment and electoral systems. *Women in parliament: Beyond numbers. International IDEA Handbook. Stockholm*, pages 93–111, 2005.

[384] Kenneth O May. A set of independent necessary and sufficient conditions for simple majority decision. *Econometrica: Journal of the Econometric Society*, 20(4):680–684, 1952.

[385] Eric Mazur. *Peer instruction*. Upper Saddle River, NJ: Prentice Hall, 1997.

[386] Neal McBurnett, Richard T Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L Rivest, Emily Shen, Alan T Sherman, and Poorvi L Vora. Scantegrity Responds to Rice Study on Usability of the Scantegrity II Voting System, December 2014. In review, Journal of Election Technology and Systems (JETS).

[387] Patrick McDaniel, Kevin Butler, William Enck, Harri Hursti, Steve McLaughlin, Patrick Traynor, Matt Blaze, Adam Aviv, Pavol Černý, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, Giovanni Vigna, Richard Kemmerer, Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, William Robertson, Fredrik Valeur, Joseph Lorenzo Hall, and Laura Quilter. EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, final report, December 2007. `http://www.patrickmcdaniel.org/pubs/everest.pdf`.

[388] Ronan McDermott. *Electronic Voting in Ireland. A Case Study*. Brussels: EC-UNDP Partnership on Electoral Assistance, 2012. Thematic Workshop / Mombassa (Kenia).

[389] Margaret McGalley and J Paul Gibson. *Electronic Voting: A Safety Critical System*. Maynooth: National University of Ireland, 2003. http://www.umic.pt/images/stories/publicacoes1/nuim-cs-tr-2003-02.pdf.

[390] Iain McLean. Forms of representation and systems of voting. *Political Theory Today*, pages 172–196, 1991.

[391] Juan Manuel Mecinas Montiel. *Constitutional Analysis of the Internet Voting*. PhD thesis, Universidad Complutense de Madrid, 2013. Doctoral dissertation. Title translated from Spanish.

[392] Paul Melia and Luke Byrne. €54m voting machines scrapped for €9 each. *Independent*, June 29th, 2012. http://www.independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212.html.

[393] Silvio Micali. Computationally sound proofs. *SIAM Journal on Computing*, 30(4):1253–1298, 2000.

[394] Paul Mitchell. The United Kingdom: plurality rule under siege. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 157–184. Oxford University Press, 2005.

[395] Ester Moher, Jeremy Clark, and Aleksander Essex. Diffusion of voter responsibility: Potential failings in E2E voter receipt checking. *USENIX Journal of Election Technology and Systems (JETS)*, 1, 2014.

[396] David Molnar, Tadayoshi Kohno, Naveen Sastry, and David Wagner. Tamper-evident, history-independent, subliminal-free data structures on prom storage-or-how to store ballots on a voting machine. In *IEEE Symposium on Security and Privacy*, pages 6–pp. IEEE, 2006.

[397] Tal Moran and Moni Naor. Receipt-free universally-verifiable voting with everlasting privacy. In *Advances in Cryptology-CRYPTO 2006*, pages 373–392. Springer, 2006.

[398] Tal Moran and Moni Naor. Split-ballot voting: everlasting privacy with distributed trust. *ACM Transactions on Information and System Security (TISSEC)*, 13(2):16, 2010.

[399] Dan Morrell. Secret Ballots, Verifiable Votes, May-June 2010. http://harvardmagazine.com/2010/05/secret-ballots-verifiable-votes.

[400] Robert G Moser. Electoral systems and the number of parties in postcommunist states. *World Politics*, 51:359–384, 1999.

[401] Mozilla wiki. Security/server side TLS configuration guide. https://wiki.mozilla.org/Security/Server_Side_TLS.

[402] Judith Murray. Usability testing for end-to-end verifiable internet voting project feasibility study. *Publication Pending*, 2015.

[403] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, May 24 2009. (Posted on Cryptography Mailing List at metzdowd.com).

[404] Mridul Nandi, Stefan Popoveniuc, and Poorvi L Vora. Stamp-it: a method for enhancing the universal verifiability of e2e voting systems. In *Information Systems Security*, pages 81–95. Springer, 2010.

[405] Moni Naor and Adi Shamir. Visual cryptography. In *Advances in Cryptology–EUROCRYPT'94*, pages 1–12. Springer, 1995.

[406] C Andrew Neff. A verifiable secret shuffle and its application to e-voting. In *ACM conference on Computer and Communications Security*, pages 116–125. ACM, 2001.

[407] Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer. Analysis of security and cryptographic approaches to provide secret and verifiable electronic voting. In *Design, Development, and Use of Secure Electronic Voting Systems*. IGI Global, 2014.

[408] Stephan Neumann, Christian Feier, Melanie Volkamer, and Reto E Koenig. Towards a practical jcj/civitas implementation. *IACR Cryptology ePrint Archive*, 2013:464, 2013.

[409] Stephan Neumann, Oksana Kulyk, and Melanie Volkamer. A usable android application implementing distributed cryptography for election authorities. In *International Conference on Availability, Reliability and Security (ARES)*, pages 207–216. IEEE, 2014.

[410] Stephan Neumann, M Maina Olembo, Karen Renaud, and Melanie Volkamer. Helios verification: To alleviate, or to nominate: Is that the question, or shall we have both? In *Electronic Government and the Information Systems Perspective (EGOVIS)*, pages 246–260. Springer, 2014.

[411] Stephan Neumann and Melanie Volkamer. Civitas and the real world: Problems and solutions from a practical point of view. In *International Conference on Availability, Reliability and Security (ARES)*, pages 180–185. IEEE, 2012.

[412] Glenn M Newkirk. Trends in American trust in voting technology. Technical report, whitepaper for InfoSENTRY Services, 2008.

[413] NewsGram. EVM controversy: VVPAT to be used as Delhi votes tomorrow, February 6, 2015. `http://www.newsgram.com/evm-controversy-and-vvpat-in-delhi/`.

[414] Jairo M Nicolau. Brazil: Democratizing with majority runoff. In Josep M Colomer, editor, *Handbook of Electoral System Choice*, pages 121–132. Palgrave Macmillan, 2004.

[415] Valtteri Niemi and Ari Renvall. How to prevent buying of votes in computer elections. In *Advances in Cryptology–ASIACRYPT'94*, pages 164–170. Springer, 1995.

[416] Kees Niemoller. Experiences with voting machines in the Netherlands and in Germany. In Commission on Electronic Voting, editor, *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Interim report. Appendix 2K*, pages 327–348. Commission on Electronic Voting, 2004. wijvertrouwenstemcomputersniet.nl/images/a/a2/Bijlage_over_Nederland_bij_rapport_Ierse_commissie.pdf.

[417] NIST. *Accessibility and Usability Considerations for UOCAVA Remote Electronic Voting Systems*. Gaithersburg: National Institute of Standards and Technology (NIST), 2011. http://www.eac.gov/assets/1/Documents/Usability\%20Accessibility\%20for\%20Remote\%20Voting\%20Systems\%202011-02-14\%20v3-final.pdf.

[418] C Andrew NNeff. Practical high certainty intent verification for encrypted votes. vote-here (2004), 2004. http://www.votehere.net/vhti/documentation.

[419] Lawrence Norden, David Kimball, Whitney Quesenbery, and Margaret Chen. *Better Ballots*. New York: Brennan Center for Justice, 2008. http://www.brennancenter.org/sites/default/files/legacy/Democracy/Better\%20Ballots.pdf.

[420] Donald F Norris. Maryland registered voters' opinions about voting and voting technologies. Technical report, National Center for the Study of Elections of the Maryland Institute for Policy Analysis & Research University of Maryland, Baltimore County, 2006.

[421] Notimerica. Mexico to use electronic voting in presidential elections. 2015. http://www.notimerica.com/politica/noticia-mexico-probara-voto-electronico-elecciones-presidenciales-20150601213118.html. Title translated from Spanish.

[422] NSW Electoral Commission. 2015 legislative council—final distribution of preferences. http://vtr.elections.nsw.gov.au/lc-home.htm#lc/state/dop/dop_index.

[423] NSW Electoral Commission. Index of iVote reports. http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports.

[424] NSW Electoral Commission. iVote threat analysis and risk assessment, January 2014. http://www.elections.nsw.gov.au/

__data/assets/pdf_file/0008/175760/NSW_Election_-_iVote_Threat_Analysis_and_Risk_Assessment_v3.0.pdf.

[425] NSW Electoral Commission. iVote system security implementation statement, March 2015. http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/193219/iVote-Security_Implementation_Statement-Mar2015.pdf.

[426] Marianne Wiik Øberg. Improving the Norwegian internet voting protocol. Master's thesis, Norwegian University of Science and Technology, June 2011.

[427] OSCE / ODIHR. *The Netherlands. Parliamentary Elections 22 November 2006. OSCE/ODIHR Election Assessment Mission Report*. Warsaw: OSCE / ODIHR, 2007. http://www.osce.org/odihr/elections/netherlands/24322.

[428] Council of Europe. *Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory Memorandum*. 2004.

[429] Council of Europe. *E-Voting Handbook: Key steps in the implementation of e-enabled elections*. 2010.

[430] Council of Europe. *Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards*. 2011.

[431] Council of Europe. *Guidelines on transparency of e-enabled elections*. 2011.

[432] General Secretariat of the Organization of American States. *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*. Organization of America States, 2010. https://www.oas.org/es/sap/docs/Technology\%20English-FINAL-4-27-10.pdf.

[433] Title 29 of the United States Code. Vocational rehabilitation act, 1973. § 794d, Section 508.

[434] Ohio Secretary of State's Office. Evaluation and Validation of Election-Related Equipment, Standards and Testing (EVEREST), 2007. http://siis.cse.psu.edu/everest.html.

[435] Stephen C ohlig and Martin E Hellman. An improved algorithm for computing logarithms over gf(p) and its cryptographic significance (corresp.). *Information Theory, IEEE Transactions on*, 24(1):106–110, Jan 1978.

[436] Urmas Oja. Paavo Pihelgas: Elektroonilise hääletamise vaatlemine on lihtsalt võimatu, 2011. http://forte.delfi.ee/news/digi/paavo-pihelgas-elektroonilise-haaletamise-vaatlemine-on-lihtsalt-voimatu.d?id=41933409. In Estonian.

[437] Tatsuaki Okamoto. An electronic voting scheme. In *Advanced IT Tools*, pages 21–30. Springer, 1996.

[438] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In *Security Protocols Workshop*, pages 25–35. Springer, 1998.

[439] Ersin Öksüzoglu and Dan S Wallach. Votebox nano: A smaller, stronger fpga-based voting machine (short paper). In *USENIX/Accurate Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2009.

[440] M Maina Olembo, Karen Renaud, Steffen Bartsch, and Melanie Volkamer. Voter, what message will motivate you to verify your vote. In *Workshop on Usable Security, USEC*, 2014.

[441] Maina M Olembo, Steffen Bartsch, and Melanie Volkamer. Mental models of verifiability in voting. In *E-Voting and Identify*, pages 142–155. Springer, 2013.

[442] Commission on Electronic Voting. *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*. 2006. `http://www.stdlib.net/~colmmacc/www.cev.ie/htm/report/download_second.htm`. Second Report.

[443] ONPE. *Electronic Voting History 1996-2004*. Lima: Oficina Nacional de Procesos Electorales (ONPE), 2011. `http://www.web.onpe.gob.pe/modEducacion/Publicaciones/dt-28.pdf`. Title translated from Spanish.

[444] ONPE. *Electronic Voting in Practice: Perspectives and Dynamics From the Experience of Local and Regional Elections 2014*. Lima: Oficina Nacional de Procesos Electorales (ONPE), 2014. `http://www.web.onpe.gob.pe/modEducacion/Publicaciones/L-0102.pdf`. Title translated from Spanish.

[445] Anne-Marie Oostveen and Peter Van den Besselaar. Internet voting technologies and civic participation: the users' perspective. *Javnost-the public*, 11(1):61–78, 2004.

[446] Anne-Marie Oostveen and Peter Van den Besselaar. Security as belief. user's perceptions on the security of electronic voting systems. In A Prosser / Robert Krimmer, editor, *Electronic Voting in Europe: Technology, Law, Politics and Society*, volume P47 of *(Col. "Lecture Notes in Informatics")*, pages 73–82. Bonn: Gesellschaft für Informatik, 2004. `http://www.social-informatics.net/ESF2004.pdf`.

[447] Open Source Digital Voting Foundation. District of Columbia's Board of Elections and Ethics adopts open source digital voting foundation technology to support ballot delivery, June 2010. `http://www.businesswire.com/news/home/20100622006238/en/District-Columbia%E2%80%99s-Board-Elections-Ethics-Adopts-Open`.

[448] OSCE/ODIHR. *Norway Parliamentary Elections 9 September 2013, OSCE/ODIHR Election Assessment Mission Final Report*. Warsaw: OSCE / ODIHR, 2013. http://www.osce.org/odihr/elections/109517?download=true.

[449] OSCE/ODIHR. *Estonia. Parliamentary Elections 1 March 2015. OSCE / ODIHR Election Expert Team, Final Report*. Warsaw: OSCE /ODIHR, 2015. http://www.osce.org/odihr/elections/estonia/160131?download=true.

[450] OSCE/ODIHR. *Swiss Confederation. Federal Assembly Elections 18 October 2015. OSCE / ODIHR Needs Assessment Mission Report*. Warsaw: OSCE / ODIHR, 2015. http://www.osce.org/odihr/elections/switzerland/172056?download=true.

[451] Eric Pacuit. Voting methods. In Edward N Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Winter 2012 edition, 2012. http://plato.stanford.edu/archives/win2012/entries/voting-methods.

[452] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology–EUROCRYPT'99*, pages 223–238. Springer, 1999.

[453] Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa. Efficient anonymous channel and all/nothing election scheme. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 248–259. Springer Berlin Heidelberg, 1994.

[454] Brian Parno, Craig Gentry, Jon Howell, and Mariana Raykova. Pinocchio: Nearly practical verifiable computation. In *IEEE Symposium on Security and Privacy*, S&P '13, pages 238–252, 2013.

[455] Nathanael Paul, David Evans, Avi Rubin, and Dan Wallach. Authentication for remote voting. In *Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale*, 2003.

[456] Nathanael Paul and Andrew S Tanenbaum. Trustworthy voting: From machine to system. *IEEE Computer*, 42(5):23–29, 2009.

[457] Torben Pryds Pedersen. A threshold cryptosystem without a trusted party. In *Advances in Cryptology–EUROCRYPT'91*, pages 522–526. Springer, 1991.

[458] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in Cryptology–CRYPTO'91*, pages 129–140. Springer, 1992.

[459] Gonçalo David Martins Tourais Pereira. Scroll, match & vote: An e2e coercion resistant mobile voting system. In *EVOTE*, pages 149–152. IEEE, 2014.

[460] Birgit Pfitzmann and Andreas Pfitzmann. How to break the direct rsa-implementation of mixes. In *Advances in Cryptology–EUROCRYPT'89*, pages 373–381. Springer, 1990.

[461] W Pieters and MJ Becker. Ethics of e-voting: An essay on requirements and values in internet elections. *Ethics of New Information Technology: Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Inquiry*, pages 307–318, 2005.

[462] Gillian E Piner and Michael D Byrne. The experience of accessible voting results of a survey among legally-blind users. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 55, pages 1686–1690. SAGE Publications, 2011.

[463] John M Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32(143):918–924, Jul 1978.

[464] Stefan Popoveniuc. Speakup: remote unsupervised voting. *Industrial Track ACNS*, 2010.

[465] Stefan Popoveniuc and Ben Hosp. An introduction to Punchscan. In *Workshop on Trustworthy Elections (WOTE)*, 2006.

[466] Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, and Poorvi Vora. Performance requirements for end-to-end verifiable elections. In *International conference on Electronic voting technology/workshop on trustworthy elections*, pages 1–16. USENIX Association, 2010.

[467] Stefan Popoveniuc and David Lundin. A simple technique for safely using Punchscan and prêt à voter in mail-in elections. In *E-Voting and Identity*, pages 150–155. Springer, 2007.

[468] Stefan Popoveniuc and Poorvi L Vora. Remote ballot casting with captchas. In *Workshop on information and System Security*, 2008.

[469] Nicolas Pouillard. Helios pull request #46, 2013. `https://github.com/benadida/helios-server/pull/46`.

[470] Vladimir Pran and Patrick Merloe. Monitoring electronic technologies in electoral processes. *National Democratic Institute*, 2007.

[471] prometheus. Monitoring electronic technologies in electoral processes. Github repository, June 2015. `https://github.com/prometheus-ar/vot.ar`.

[472] Estat Propi. Declared innocent the journalist who impersonated Alberto Fernández Díaz during the popular consultation on diagonal avenue ... *Racó Català*, February 23rd, 2013. `http://ves.cat/mfkl`. Title translated from Catalan.

[473] Niels Provos, Markus Friedl, and Peter Honeyman. Preventing privilege escalation. In *USENIX Security*, volume 3, 2003.

[474] PSDB. Auditoria do PSDB nas urnas eletrônicas mostra que sistema eleitoral brasileiro é vulnerável, November 4, 2015. `http://www.psdb.org.br/auditoria-do-psdb-nas-urnas-eletronicas-mostra-que-sistema-eleitoral-brasileiro-e-vulneravel/`. In Portuguese.

[475] RABA Technologies. Trusted agent report: Diebold AccuVote-TS voting system, 2004. `http://www.raba.com/press/TAReportAccuVote.pdf`.

[476] Douglas W Rae. *The Political Consequences of Electoral Laws*. Yale University Press, New Haven, 1967.

[477] Kim Ramchen and Vanessa Teague. Parallel shuffling and its application to prêt à voter. In *USENIXAccurate Electronic Voting Technology Workshop*, 2010.

[478] Brian Randell and Peter Y A Ryan. Voting technologies and trust. *IEEE SECURITY & PRIVACY*, 4(5):0050–56, 2006.

[479] Steven R Reed. Japan: haltingly toward a two-party system. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 277–294. Oxford University Press, 2005.

[480] Ben Reilly, Andrew Ellis, and Andrew Reynolds. *Electoral system design: the new international IDEA handbook*. International Institute for Democracy and Electoral Assistance, 2005.

[481] Benjamin Reilly. Social choice in the south seas: Electoral innovation and the Borda count in the Pacific island countries. *International Political Science Review*, 23(4):355–372, 2002.

[482] Eric Rescorla. Understanding the security properties of ballot-based verification techniques. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, volume 1, 2009.

[483] Pedro A D Rezende. Electronic elections: a balancing act. In *Towards trustworthy elections*, pages 124–140. Springer, 2010.

[484] Timothy S Rich. Evaluating South Korea's mixed legislative system: A cross-national analysis of district competition. *Korea Observer*, 44(3):365, 2013.

[485] Ronald L Rivest. Electronic voting. In *Financial Cryptography*, volume 1, pages 243–268, 2001.

[486] Ronald L Rivest. On the notion of 'software independence' in voting systems. *Philosophical Transactions of The Royal Society A*, 366(1881):3759–3767, August 6, 2008.

[487] Ronald L Rivest and Warren D Smith. Three voting protocols: Threeballot, vav, and twin. In *USENIX Workshop on Accurate Electronic Voting Technology*, volume 16. USENIX Association, 2007.

[488] Ronald L Rivest and John P Wack. On the notion of "software independence" in voting systems, July 28, 2006. http://vote.nist.gov/SI-in-voting.pdf.

[489] E Arthur Robinson Jr and Daniel H Ullman. *A Mathematical Look at Politics*. CRC Press, Taylor & Francis, 2010.

[490] Tom Roeder. Pyrios library, 2014. `https://github.com/google/pyrios/`.

[491] Jörg Rothe and Irene Rothe. *Economics and Computation: An Introduction to Algorithmic Game Theory, Computational Social Choice, and Fair Division*. Springer, 2015.

[492] Avi Rubin. Security considerations for remote electronic voting over the Internet. `http://avirubin.com/e-voting.security.html`.

[493] Avi Rubin. *Brave New Ballot*. New York: Morgan Road Books, 2006. `http://www.bravenewballot.org`.

[494] Peter Y A Ryan. A variant of the chaum voter-verifiable scheme. Technical Report CS-TR-864, University of Newcastle upon Tyne School of Computing Science, October 2004. `http://www.cs.newcastle.ac.uk/publications/trs/papers/864.pdf`.

[495] Peter Y A Ryan. Human readable paper verification of Prêt à Voter. Technical Report CS-TR-966, Newcastle University, 2006.

[496] Peter Y A Ryan. Human readable paper verification of Prêt à Voter. Technical Report CS-TR-1038, Newcastle University, 2007.

[497] Peter Y A Ryan. Putting the human back in voting protocols. In *Security Protocols Workshop*, pages 20–25. Springer, 2009.

[498] Peter Y A Ryan. Prêt à voter with confirmation codes. In *USENIX Electronic Voting Technology Workshop*, 2011.

[499] Peter Y A Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

[500] Peter Y A Ryan and Jeremy Bryans. A simplified version of the chaum voting scheme. Technical Report CS-TR-843, Newcastle University, 2004.

[501] Peter Y A Ryan and Thea Peacock. Prêt à Voter: A system perspective. Technical Report CS-TR-929, University of Newcastle upon Tyne School of Computing Science, September 2005. `http://www.cs.ncl.ac.uk/research/pubs/trs/papers/929.pdf`.

[502] Peter Y A Ryan and Thea Peacock. A threat analysis of prêt à voter. In *Towards Trustworthy Elections*, pages 200–215. Springer, 2010.

[503] Peter Y A Ryan and Steve Schneider. Prêt à Voter with re-encryption mixes. Technical Report CS-TR-956, University of Newcastle upon Tyne School of Computing Science, April 2006. `http://www.cs.ncl.ac.uk/research/pubs/trs/papers/956.pdf`.

[504] Peter Y A Ryan and Steve Schneider. Prêt à voter with re-encryption mixes. In *ESORICS*, number 4189 in LNCS. Springer-Verlag, 2006.

[505] Peter Y A Ryan and Vanessa Teague. Ballot permutations in prêt à voter. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2009.

[506] Peter Y A Ryan and Vanessa Teague. Pretty good democracy. In *Security Protocols Workshop XVII*, pages 111–130. Springer, 2013.

[507] Thomas Saalfeld. Germany: stability and strategy in a mixed-member proportional system. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 209–229. Oxford University Press, 2005.

[508] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme. In *Advances in Cryptology–EUROCRYPT'95*, pages 393–403. Springer, 1995.

[509] Bassel F Salloukh. The limits of electoral engineering in divided societies: elections in postwar Lebanon. *Canadian Journal of Political Science*, 39(03):635–655, 2006.

[510] Daniel Sandler, Kyle Derr, and Dan S Wallach. Votebox: A tamper-evident, verifiable electronic voting system. In *USENIX Security Symposium*, volume 4, page 87, 2008.

[511] Daniel Sandler and Dan S Wallach. Casting votes in the auditorium. In *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

[512] Daniel Sandler and Dan S Wallach. The case for networked remote voting precincts. *EVT*, 8:1–7, 2008.

[513] David E Sanger. Obama order sped up wave of cyberattacks against Iran. The New York Times, June 1, 2012. `http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html`.

[514] Bo Särlvik. Party and electoral system in Sweden. In Bernard Grofman and Arend Lijphart, editors, *The Evolution of Electoral and Party Systems in the Nordic Countries*, page 225. Algora Publishing, 2007.

[515] Mark Allen Satterthwaite. Strategy-proofness and Arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions. *Journal of Economic Theory*, 10(2):187–217, 1975.

[516] Steve Schneider, Morgan Llewellyn, Chris Culnane, James Heather, Sriramkrishnan Srinivasan, and Zhe Xia. Focus group views on prêt à voter 1.0. In *Workshop on Requirements Engineering for Electronic Voting Systems*, pages 56–65, 2011.

[517] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174, 1991.

[518] Guido Schryen and Eliot Rich. Security in large-scale internet elections: A retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security*, 4(4):729–744, Dec 2009.

[519] Markus Schulze. A new monotonic, clone-independent, reversal symmetric, and condorcet-consistent single-winner election method. *Social Choice and Welfare*, 36(2):267–303, 2011.

[520] Bryan P Schwartz and Dan Grice. Establishing a legal framework for e-voting in canada. *Man. LJ*, 36:301, 2012.

[521] Science Applications International Corporation. Risk assessment report: Diebold AccuVote-TS voting system and processes (unredacted), 2003. `http://www.bradblog.com/?p=3731`.

[522] Bock Segaard, Dag Arne Christensen, Bjarte Folkestad, and Jo Saglie. Internettvalg: Hva gjør og mener velgerne?, 2014. `https://www.regjeringen.no/globalassets/upload/kmd/komm/rapporter/isf_internettvalg.pdf`. In Norwegian.

[523] Hovav Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In *ACM conference on Computer and communications security (CCS'07)*, pages 552–561. ACM, 2007.

[524] Daniel Shanks. Class number, a theory of factorization, and genera. In *Symposium on Pure Math*, volume 20, pages 415–440, 1971.

[525] Alan T Sherman, Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, and Poorvi Vora. Scantegrity mock election at Takoma Park (summary), October 2009. NIST End-to-End Voting Systems Workshop.

[526] Alan T Sherman, Richard T Carback, David Chaum, Jeremy Clark, Aleksander Essex, Paul S Hernson, Travis Mayberry, Stefan Popoveniuc, Ronald L Rivest, Emily Shen, Bimal Sinha, and Poorvi L Vora. Scantegrity mock election at Takoma Park. In *EVOTE*, 2010.

[527] Alan T Sherman, Russell A Fink, Richard Carback, and David Chaum. Scantegrity iii: automatic trustworthy receipts, highlighting over/under votes,

and full voter verifiability. In *Conference on Electronic voting technology/workshop on trustworthy elections*, pages 7–7. USENIX Association, 2011.

[528] Victor Shoup and Rosario Gennaro. Securing threshold cryptosystems against chosen ciphertext attack. *Journal of Cryptology*, 15(2):75–96, 2002.

[529] Matthew Shugart and Martin P Wattenberg. *Mixed-Member Electoral Systems: The Best of Both Worlds?* Oxford University Press, 2001.

[530] Gustavus J Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology*, pages 51–67. Springer, 1984.

[531] Barbara Simons. Report on the Estonian Internet voting system. Verified Voting Blog, September 3, 2011. `https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/`.

[532] Matt Smart and Eike Ritter. True trustworthy elections: remote electronic voting using trusted computing. In *Autonomic and Trusted Computing*, pages 187–202. Springer, 2011.

[533] Benjamin Smith, Sharon Laskowski, and Svetlana Lowry. Implications of graphics on usability and accessibility for the voter. In *E-Voting and Identity*, pages 54–74. Springer, 2009.

[534] Eivind Smith. Secret electronic vote? *Lov og rett: Norsk Juridisk Tidsskrift*, 49(6):307–323, 2010. title translated from Norwegian.

[535] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the Estonian Internet voting system. In *ACM Conference on Computer and Communications Security*, CCS'14, pages 703–715. ACM, 2014.

[536] Oliver Spycher, Reto Koenig, Rolf Haenni, and Michael Schläpfer. A new approach towards coercion-resistant remote e-voting in linear time. In *Financial Cryptography and Data Security*, volume 7035, page 182. Springer Science & Business Media, 2012.

[537] Sriramkrishnan Srinivasan, Chris Culnane, James Heather, Steve Schneider, and Zhe Xia. Countering ballot stuffing and incorporating eligibility verifiability in Helios. In *Network and System Security (NDSS)*, pages 335–348. Springer, 2014.

[538] Richard P Stanley. Enumerative combinatorics. vol. 2, volume 62 of cambridge studies in advanced mathematics, 1999.

[539] Emily Stark, Mike Hamburg, and Dan Boneh. Stanford javascript crypto library. `http://bitwiseshiftleft.github.io/sjcl/`.

[540] Philip B Stark. Super-simple simultaneous single-ballot risk-limiting audits. In *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'10)*, 2010.

[541] Philip B Stark and David Wagner. Evidence-based elections. *Security & Privacy, IEEE*, 10(5):33–41, 2012.

[542] Paul Stenbjorn. An overview and design rationale memo, September 2010. `http://www.dcboee.us/dvm/DCdVBM-DesignRationale-v3.pdf`.

[543] Ida Sofie Gebhardt Stenerud and Christian Bull. When reality comes knocking Norwegian experiences with verifiable electronic voting. In *Electronic Voting*, volume P-205 of *(Col. "Lecture Notes in Informatics-LNI")*. Bonn: Gesellschaft für Informatik, 2012.

[544] John Stewart. A banana republic? the investigation into electoral fraud by the birmingham election court. *Parliamentary Affairs*, 59(4):654–667, 2006.

[545] Stichting Wij Vertrouwen Stemcomputers Niet. The Netherlands return to paper ballots and red pencils, October 2009. `http://wijvertrouwenstemcomputersniet.nl/English`.

[546] Douglas R Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[547] Susan Stokes, Thad Dunning, Marcelo Nazareno, and Valeria Brusco. What killed vote-buying in britain and the united states? 2012. `http://www.princeton.edu/csdp/online-community/historical-theoretical-pe/What-Killed-Vote-Buying-in-Britain-and-the-US.pdf`.

[548] Nicolas Strauch and Robertas Pogorelis. Electoral systems: The link between governance, elected members and voters. An OPPD publication on topical parliamentary affairs, European Parliament – Office for Promotion of Parliamentary Democracy, 2011.

[549] Supreme Court of India. Dr. Subramanian Swamy v. Election Commission of India, civil appeal no. 9093 of 2013. Judgment, October 8, 2013. `http://supremecourtofindia.nic.in/outtoday/9093.pdf`.

[550] Vanessa Teague and J Alex Halderman. Security flaw in New South Wales puts thousands of online votes at risk. Freedom to Tinker blog, March 22, 2015. `https://freedom-to-tinker.com/blog/teaguehalderman/ivote-vulnerability/`.

[551] Vanessa Teague and J Alex Halderman. Thousands of NSW election online votes open to tampering, March 23, 2015. `https://theconversation.com/thousands-of-nsw-election-online-votes-open-to-tampering-39164`.

[552] Björn Terelius and Douglas Wikström. Proofs of restricted shuffles. In *Progress in Cryptology–AFRICACRYPT*, pages 100–113. Springer, 2010.

[553] The portal of the Swiss government The Federal Council. Federal council elections since 1848. https://www.admin.ch/gov/en/start/federal-council.html.

[554] Procedures The Standards and Scottish Parliament Website Public Appointment Committee. Election of parliamentary posts. http://www.scottish.parliament.uk.

[555] TNN. New EVMs to have paper trail. Times of India, January 20, 2012. http://timesofindia.indiatimes.com/india/New-EVMs-to-have-paper-trail/articleshow/11561762.cms.

[556] Ian Traynor. Russia accused of unleashing cyberwar to disable Estonia, May 17, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

[557] Ian Traynor. GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm, October 3, 2013. http://www.theguardian.com/uk-news/2013/oct/03/gchq-eu-surveillance-cyber-attack-belgian.

[558] Georgios Tsoukalas, Kostas Papadimitriou, Panos Louridas, and Panayiotis Tsanakas. From Helios to Zeus. *The USENIX Journal of Election Technology and Systems*, 1(1):1–17, 2013.

[559] Jim Tyre. 2010 Pioneer Award winner Hari Prasad defends India's democracy. EFF Deeplinks Blog, November 1, 2010. https://www.eff.org/deeplinks/2010/11/2010-pioneer-award-winner-hari-prasad-defends.

[560] European Union. *Final Report. Presidential Election Venezuela 2006*. Caracas: European Union Election Observation Mission, 2006. http://eeas.europa.eu/eueom/pdf/missions/moe_ue_venezuela_2006_final_eng.pdf.

[561] United Nations Office on Drugs and Crime. United nations convention against corruption. 2005.

[562] Antti Vähä-Sipilä. *A Report on the Finnish E-Voting Pilot*. Helsinki: Electronic Frontier Finland, 2009. http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf.

[563] Vabariigi Valimiskomisjon. Internet voting in Estonia, 2007. http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf.

[564] Jeroen Van De Graaf. Voting with unconditional privacy by merging prêt à voter and Punchscan. *IEEE Transactions on Information Forensics and Security*, 4(4):674–684, 2009.

[565] Henk van der Kolk. Local electoral systems in Western Europe. *Local Government Studies*, 33(2):159–180, 2007.

[566] Carlos Vegas González. The new Belgian e-voting system. In *Electronic Voting*, volume P-205 of *(Col. "Lecture Notes in Informatics-LNI")*, pages 199–211. Bonn: Gesellschaft für Informatik, 2012.

[567] Victorian Electoral Commission. Report to Parliament on the 2006 Victorian State election, July 2007.

[568] Melanie Volkamer. Electronic voting in Germany. In Serge Gurwirth / Yves Poullet / Paul de Hert, editor, *Data protection in a Profiled World*, pages 177–191. Dordrecht: Springer, 2010.

[569] Melanie Volkamer and Rüdiger Grimm. Determine the resilience of evaluated internet voting systems. In *International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE'09)*, pages 47–54. IEEE, 2010.

[570] Vot.ar: Sistema de boleta unica electrónica. `http://www.vot-ar.com.ar/`. In Spanish.

[571] Jack Vowles. New Zealand: the consolidation of reform. In Michael Gallagher and Paul Mitchell, editors, *The Politics of Electoral Systems*, pages 295–313. Oxford University Press, 2005.

[572] Janna-Lynn Weber and Urs Hengartner. Usability study of the open audit voting system Helios. INCLUDE, 2009.

[573] Michael Wei, Laura M Grupp, Frederick E Spada, and Steven Swanson. Reliably erasing data from flash-based solid state drives. In *Proceedings of the 9th USENIX Conference on File and Storage Technologies*, FAST'11, 2011.

[574] Wikipedia. Booth capturing. `https://en.wikipedia.org/w/index.php?title=Booth_capturing&oldid=689575624`.

[575] Wikipedia. Results of the Indian general election, 2014. `https://en.wikipedia.org/w/index.php?title=Results_of_the_Indian_general_election,_2014&oldid=691240029`.

[576] Douglas Wikström. A commitment-consistent proof of a shuffle. In *Australasian Conference on Information Security and Privacy (ACISP'09)*, pages 407–421. Springer, 2009.

[577] Douglas Wikström. User manual for the verificatum mix-net version 1.4. 0. *Verificatum AB, Stockholm, Sweden*, 2013.

[578] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of India's electronic voting machines. In *ACM conference on Computer and Communications Security*, CCS'10, pages 1–14. ACM, 2010.

[579] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J Alex Halderman. Attacking the washington, dc internet voting system. In *Financial Cryptography and Data Security*, pages 114–128. Springer, 2012.

[580] Peter Wolf and Nadia Handal Zander. *The Use of Open Source Technology in Elections*. Stockholm: IDEA, 2014.

[581] Zhe Xia, Chris Culnane, James Heather, Hugo Jonker, Peter Y A Ryan, Steve Schneider, and Sriramkrishnan Srinivasan. Versatile prêt à voter: Handling multiple election methods with a unified interface. In *Progress in Cryptology-INDOCRYPT 2010*, pages 98–114. Springer, 2010.

[582] Alec Yasinsac. Independent computations for safe remote electronic voting. In *Security Protocols Workshop XXI*, pages 71–83. Springer, 2013.

[583] Ka-Ping Yee. Extending prerendered-interface voting software to support accessibility and other ballot features. In *USENIX Workshop on Accurate Electronic Voting Technology*, pages 5–5. USENIX Association, 2007.

[584] Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M Bellovin. Prerendered user interfaces for higher-assurance electronic voting. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

[585] Adam Young and Moti Yung. Bandwidth-optimal kleptographic attacks. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 235–250. Springer Berlin Heidelberg, 2001.

[586] Filip Zagórski, Richard T Carback, David Chaum, Jeremy Clark, Aleksander Essex, and Poorvi L Vora. Remotegrity: Design and use of an end-to-end verifiable remote voting system. In *Applied Cryptography and Network Security*, pages 441–457. Springer, 2013.

[587] Nickolai Zeldovich, Silas Boyd-Wickizer, and David Mazieres. Securing distributed systems with information flow control. In *NSDI*, volume 8, pages 293–308, 2008.