# Abstract (to expand)

In this report we will review past and current efforts in the area of e-voting, analyzing his challenges and how different technologies have been trying to address them. Also, we will review experiences of using the approaches that have been applied. In each technology, we will describe, also, the current security analysis with respect to specific attacks. We will go in-depth with some real-world experiences that could present interesting cases of e-voting.

As is possible to appreciate when someone read the different protocols and experiences, the task to define a completely secure protocol por electronic voting is very difficult, not only from the technical point of view but from the political and organizational perspective. In that sense, our main effort in this report is try to find a tendency in the different approaches to electronic voting that will allow to predict that a valid protocol will be accepted, at least for same time, or that this is a, more and more, elusive objective.

We have separated the protocols and experiences in a imaginary “pre and post blockchain word”. The use of blockchain, for real or “fancy” reasons, is a definitive moment specially for this kind of problem, so, in our opinion, add some simplicity at the hour of review so many cases.

# The evolution of non-traditional voting schemes

If we move ahead of what we can consider “traditional voting”, that is a vote with a ballot in a voting booth, the first and popular alternative that we need to consider is postal voting. Postal voting is still used in many elections around the world and is considered the standard against e-voting must be compared. Also, in the same category, we have telephone and fax voting.

Why postal, telephone, and fax voting are a standard to be compared? Because they offer a way to extend democracy to places and moments different than the traditional voting and, in that way, can achieve a major participation and in that way more representativity: many people who would be unable to vote through traditional ways will be able to participate in the democratic process using other ways. Following the same logic, e-voting can offer the democratic process major advantages more than cost or convenience (like electronic voting could be) [1].

In this report, we will explore mainly internet-based e-voting, because delivers a true opportunity to extend the benefits of postal, telephone, and fax voting in terms of extension of places and time and also could provide improvements in the fair conditions of the election process.

# E-voting online, pre-blockchain history

From the Second World War, mainly pushed by the democratization movement, efforts toward general availability and perfectability of the democratic process have encountered technical possibilities, and, in particular, the internet offers great promise in that goal. [2]

First, many theoretical protocols were proposed, but mainly that efforts rested in the academic world.

After this, a practical approach emerged from private companies and governments. The political race was ignited when President Bill Clinton ordered an investigation on the matter in 1999. Sadly, the events of the Bush versus Gore election put doubts over certainties in the role of machines in the election and the trials of internet voting were moved outside the U.S. [3]

## Main challenges

What makes electronic voting a harder process than e-banking for example? More than the fact that e-banking has problems and is subject to attack and fraud, is the special characteristics that e-voting needs that make this kind of project so challenging.

As an e-voting mechanism, it is necessary to achieve the goals of authentication, anonymity/privacy, and verifiability/auditability. In other words, we need that, for example, to be able to assure the voter that his vote was considered. His option was recorded correctly, and at the same time be able to assure him that his vote is anonymous, and there is no way that someone can coerce him with the vote. These objectives look, at first sight, as a contradiction. The fact that the voter receives some kind of paper or receipt is achieved when the voting is done in the voting booth using an electronic machine (which is called DRE = Direct recording voting, instead of REV = remote electronic voting), but in remote e-voting the issue of how to deliver assurance to the voter it has been matter of discussion.

Another aspect that is challenging is the possibility of fraud because any interference in the way of impersonation, communication intersection, tampering, or even the hack of the counting services at the end of the process can be used as fraud methods.

Also, being the process executed remotely, the concern of coercion is similar to the cases of postal, telephone, and fax. Electronic voting protocols need to address this issue. [4]

Even before considering blockchain as a technology interesting for electronic voting, there were three requirements that are very related.

1. One is End-to-end verifiability, which is the capacity of the system to offer the voter the verification that their own vote has been cast as intended.
2. Another characteristic is Web Bulletin Boards (WBBs) for posting all the cast ballots in a medium where anyone can see the information. WBBs are used in channels that are secured and where all the ballots are shown in encrypted form.
3. The last one is the use of a homomorphic tally, allowing algebraic operations in the group of ballots without the need for decryption.

## Proposals, experiences, and attacks: use of e-voting protocols in the world

In terms of adoption, we can find, in general terms, a prudent approach from many different countries: there are some who have been promoting the use of electronic voting, especially looking to avoid fraud. Other countries are analyzing electronic voting, especially using reports from expert commissions. There are also, small-scale adoptions and large-scale adoptions. In these cases we also explore what kind of criticism and attack this experiences have live.

### The Nedap/Groenendaal ES3B electronic voting system, experiences in Netherlands, portions of Germany, and France

[A1] The Nedap/Groenendaal ES3B electronic voting system, which is used in the Netherlands, portions of Germany, and France, has come under fire, particularly in Ireland, where its usage has been suspended. In this research, we investigate system vulnerabilities, raising concerns about the reliability of Direct Recording Electronic (DRE) voting devices.

The broad usage of the Nedap ES3B in the Netherlands, combined with its suspension in Ireland, emphasizes the importance of assessing the security and dependability of electronic voting systems. This article investigates realistic attacks on the Nedap ES3B, disclosing all probable flaws that could jeopardize the validity of the election results.

The "Screen and Keyboard Man-in-the-Middle Attack" is one of the attack scenarios outlined, in which a small board is installed inside the device's enclosure and can intercept and modify data between the computer and the display or keyboard. This raises the possibility of undetectable vote manipulation with limited access before elections. Another source of worry is the inclusion of a microcontroller in the ballot memory module, which allows for manipulation after votes have been cast, jeopardizing the entire integrity of the voting process.

The paper strongly opposes the reliance on obscurity for security and calls into question security methods that limit auditability. It focuses on the potential clash between the objectives of concerned voters and manufacturer-oriented security features. Furthermore, the failure to examine potential insider attacks and reliance on DRE systems are cited as major problems.

Because of the observed design flaws, the Nedap ES3B system is more vulnerable to exploitation by malevolent actors. While both attackers and governments might possibly exploit its weaknesses, the practicality of attacks and the type of vulnerabilities make hostile attackers more likely to compromise the system, particularly given quick pre-election access.

In conclusion, the Nedap ES3B is said to be insufficiently secure for use in elections. The current Dutch e-voting requirements have been criticized for putting too much emphasis on security against various attacks. The paper [1] advocates for new legal requirements addressing basic computer security and independent verification to ensure election results are legitimate. This analysis broadens the scope of potential attacks beyond specific vulnerabilities in the Nedap ES3B to fundamental questions about the security, transparency, and verifiability of electronic voting systems, urging for a comprehensive approach to election protocols.

[A2] In the same line, there are studies who explore the vulnerability of electronic voting (e-voting) systems to an attack known as the "clash attack." This attack has the potential to jeopardize the integrity of the voting process, particularly in systems that use receipt verification mechanisms. It has been tested on four different e-voting systems, some of which have been used in actual elections. The paper emphasizes the potential risks posed by the clash attack and provides insights into its applicability across various e-voting configurations. The goal is to raise awareness about this threat, which will lead to the development and implementation of strong countermeasures or the explicit articulation of trust assumptions in future e-voting systems.

In an actual election scenario at an Israeli college, the Wombat voting system was used. The system works by voters presenting ID cards, casting encrypted ballots, and then publishing these ballots on a public bulletin board. The clash attack is demonstrated in the context of Wombat, in which identical receipts are issued, allowing for undetected manipulation. In Wombat, the clash attack revolves around the creation of duplicated receipts for voters who make similar choices. To mitigate this attack, countermeasures such as pre-printing serial numbers on receipts and implementing procedures for clerks to identify and address duplicate receipts are proposed.

Helios is a widely used e-voting system that comes in a variety of flavors. The original variant, as well as versions with aliases and detached names, are discussed. These variants' vulnerabilities to clash attacks are described. The clash attack in Helios variants with detached names takes advantage of dishonest browsers and bulletin boards, resulting in the publication of identical ballots. The alias version is vulnerable to a clash attack in which the same alias is issued to voters with similar choices. Modifications to random coin usage and alias issuance procedures are among the countermeasures.

Analyzing the VAV (Vote, Audit, Verify) voting system, a ThreeBallot variant in which voters are given three ballots. Candidates are listed in a fixed order on each ballot, with one marked as 'A' and the others as 'V.' The clash attack on ThreeBallot and VAV involves changing the serial numbers on simple ballots, which allows for manipulation. The significance of verifiability is emphasized, and a countermeasure involving pre-printed serial numbers is suggested.

This also compares the clash attack to another previously presented attack, highlighting differences in trust assumptions and attack strategies. A Wombat-compliant countermeasure involving pre-printing serial numbers is proposed. The paper contributes to a broader understanding of e-voting system vulnerabilities and strengths, with a nuanced focus on both verifiability and accountability.

[A3] Dan S. Wallach's comprehensive approach evaluates the security and dependability of Webb County's ES&S voting system, focusing on the ES&S touchscreen systems used during the March 2006 Primary Election. The investigation included data collection via observations and data copying, which revealed potential vulnerabilities in the electronic voting infrastructure.

The Threat Analysis report starts by investigating potential threats to the voting system. It emphasizes the risks of software tampering during both the pre-election and election phases, as well as the vulnerability to reverse engineering and malicious firmware installations. Passwords are recommended to be strengthened, and enhanced security features are implemented.

During an election, the possibility of machine tampering and ballot stuffing increases. The paper discusses accessibility issues as well as the risk of sophisticated attacks. Concerns about poll worker-induced ballot stuffing are raised, emphasizing the importance of strong security measures to prevent fraudulent activities.

The Tabulation System may be subject to software and data tampering. The ES&S tabulation systems have centralized tampering risks, necessitating a "air gap" defense and strict physical access controls. The vulnerabilities also raise concerns about data corruption in event logs and voting logs, prompting recommendations for data protection measures such as system lockdown and digital signatures during transmission.

The report examines the mechanisms used to collect and transmit votes, highlighting the flaws in PEBs and CompactFlash cards. Procedural errors, such as incorrectly tabulating "test" votes, are discussed, as are suggestions such as incorporating sanity checks and rejecting votes cast after the election date has passed.

While both malicious attackers and governments could potentially exploit the vulnerabilities in Webb County's ES&S voting system, the practicality of attacks and the nature of identified vulnerabilities make it more likely that the system will be compromised by malicious attackers.

In conclusion, [3] the paper emphasizes the serious security flaws in Webb County's ES&S voting system. It makes useful recommendations to improve the voting infrastructure's security, transparency, and dependability. To maintain public trust and ensure the integrity of democratic processes, robust security measures and transparency in electronic voting systems are emphasized.

We see a shared vulnerability in the overall security of the Nedap ES3B, contactless smartcard systems, and Webb County's ES&S voting system, which is the reliance on outdated security paradigms. Recent technologies, such as blockchain, are frequently viewed as election security saviors. Although blockchain holds promise, its widespread application to election protocols remains a contentious issue. The immediate need for strengthened legal requirements, independent verification, and transparency trumps the current industry hype surrounding specific technologies. To defend democratic processes and maintain their integrity, an all-inclusive commitment to modernizing election systems and improving security measures is required.

### SIVP in Colombia

The SIVP protocol can be implemented in Colombia [C1] to ensure a fair and transparent voting process. The protocol provides a method to avoid fraud and assure the accuracy of election results. The article introduces the Secure Internet Voting system (SIVP), a novel voting system based on blind signatures and public key cryptography that assures votes are anonymous and cannot be traced back to the voter. The protocol also includes a method for validating each voter and ensuring that only qualified voters may vote. Eligibility, democracy, privacy, verifiability, correctness, fairness, robustness, receipt-freeness, and coercion resistance are all provided by the protocol. The protocol ensures eligibility, democracy, privacy, verifiability, correctness, fairness, robustness, receipt-freeness, and coercion resistance. The research compares the computational burden of SIVP to that of other voting protocols and concludes that, despite the addition of extra security measures, it is not excessively high.

The work also examines the security needs of electronic voting systems and describes the SIVP protocol's nomenclature and technique of creation. The various phases of the SIVP protocol are detailed, and a security analysis of SIVP is provided, as well as a comparison to comparable e-voting protocols. The SIVP protocol may also be used to boost voter turnout by making it simpler for people to vote.

The paper proposes the use of the Secure Internet Voting system (SIVP) in Colombia, highlighting how its use of public key cryptography and blind signatures can guarantee elections' security, fairness, and openness. By highlighting SIVP's eligibility verification, computational efficiency, and potential to increase voter turnout, the research presents SIVP as a reliable and secure option for election procedures.

# Theoretical framework

## Mathematics behind e-voting protocols

There are many fundamentals that are used in e-voting protocols:

1. Elliptic curves: can be used for secure and efficient cryptographic operations offering very high levels of security.
2. Cryptographic hash functions: play a crucial role in e-voting protocols by providing security and integrity to various aspects of the system.
3. Public Key Encryption Schemes: They are very important, providing a foundation for secure communication, authentication, and confidentiality.
4. Homomorphic Encryption: It allows one to make specific calculations in the encryption result of the voting, getting results without needing to decrypt the individual votes.
5. Digital Signature Schemes: Provides integrity in the public-key setting, authenticating the messages or data that are part of the process.
6. Blind Digital Signature Schemes: Allows to ensure the anonymity of protocol participants.
7. Commitment Schemes: They are like digital envelopes that guarantee privacy as long as the envelope has not been opened. In addition, there is a bind between the sealer (committer) and the message.
8. Secret Sharing: Allows the protection of the key, dividing it into different partners and defining a threshold of participants needed to decrypt the secret.
9. Zero-Knowledge proofs: It allows the check that no one can vote twice at the same time that the vote remains private.

# Current efforts in voting protocols

## Blockchain proposals

There are general reasons why blockchain is an alternative, especially if we remember the characteristics described in pre-blockchain efforts like bulletin boards and end-to-end verifiability.

Blockchain, as data that is built out of a chain of data packages, offers even better characteristics than a bulletin board. A block contains a timestamp, a hash value of previous transactions as well as a nonce which is a random number used to verify the hash. The integrity of the blockchain is guaranteed by the structure described. Also, every block is validated by the nodes in the network applying some kind of cryptographic mechanism (like authority-based or storage-based).

The functionality of the blockchain can be extended with the use of smart contracts, which are computerized transactions that enforce the terms of an agreement. Functionality located in smart contracts is executed in very specific conditions and their results are logged in the form of an immutable transaction [5]

(4)

* OVN
* BSJC Proof of Completeness
* Anti-Quatum EV Protocol
* BES
* Escalability?\*\*\*\*
* Ethereum

## Blockchain experiences

### Russian Internet voting protocol

The elections of 2021 in Russia have been the target of two papers that we analyzed in this survey. The special political situation of Russia, the big deployment used in that year, and the fact that many important exponents in the area of cryptographies and mathematics came from that area of the world make it very attractive to study the particularities and deployments in e-voting in that election event.

Two main protocols were deployed in the Russian 2021 elections: one developed by Kaspersky Lab and the Department of Information Technologies of Moscow and the other developed by Rostelecom and Waves Enterprise, which was used in six federal districts of Russia.

In the next area we analize the second one.

#### Russian Federal e-Voting - General ideas

Even when information and data about the protocol is relatively scarce, some authors have been exploring and putting together different sources to try to show an integrated scheme of the protocol that was used.

To describe the protocol, first, we can talk about the participants: Voter, Organiser, Internal Observer, External Observer, Election Observer, and Keyholders.

The voter is someone who has the right to vote and is included in a list form by accessing web portal for Russian citizens. It is important to notice that someone who votes through e-voting can’t vote in person. The voters can vote using a mobile application. During the authorization phase, the voting device generates a key pair for the GOST signature scheme.

The organizer is someone who coordinates the e-voting process. He (or It?) generates the organizer key pair and the final encryption key that encrypts all the votes.

The internal observer is a participant who observes all the processes, inspecting individual nodes of the blockchain and also conducting the auditing process.

The external observer is similar to the internal observer but accesses a web page (that was down during the elections)

Election observer is a combination of internal and external observers.

Key Holders are very important and particular participants of the process: they are who hold shares of the \*very important\* organizer's secret key.

In terms of process, we have a vote collector, which is a component that allows the voter to cast the vote, interacting with the blockchain and adding encrypted votes. The tallier uses the blockchain and decryptor components. The decryptos has a Hardware Security Module (HSM).

#### Process

The first step called the setup phase, is the generation of multiple keys from the Organiser and Registrar. In this step, the secret key of the organizer is split and distributed, the blockchain receives smart contracts with the information of the election, and the final key is composed of the organizer and teller's secret keys making them mutually dependent in the final result.

The second step, the authorization phase, is related to identifying the voter as someone who can vote using a multifactor e-mail mechanism. In terms of cryptography, the device generates a key pair and the voter is added to the voter list.

The voting phase, step three, utilizes proofing to prove that a bitstring contains correct values and uses smart-contract functionality to validate the vote. The addition of their vote can be validated by the voter on a web page.

The tallying phase, step four, is done by reconstructing the secret key from the shares and summing the ciphers in the blockchain by parts at the end of the aggregate votes. It is important to notice that is not possible to decrypt the transactions containing individual votes using publicly available information.

The final step, the audit phase, verifies the list of voters, the number of cast votes, and blind signatures, and the uniqueness of transactions related to voters.

#### Security Analysis

The main criticism of the process is that it doesn’t enable the voter to verify that their vote was published in the blockchain in the way that he marked and also is not possible to know if the vote was altered in the way to the blockchain. So, basically, the process doesn’t provide any form of individual verifiability.

A further criticism is based on the fact that opposing past ideas, the secret key of the organizer is not composed of different keys generated by trusted participants but generated by the organizer and then split.[6]

* Russian Federal Remote E-voting Scheme of 2021 – Protocol Description and Analysis
* Breaking the Encryption Scheme of the Moscow Internet Voting System

### Other experiences of Blockchain in the world

The study [C2] dives into blockchain e-voting systems that have been accepted and deployed in elections by several nations, with an emphasis on the registration process used.

In 2015, Australia launched blockchain e-voting during the State General Election of New South Wales, with around 280,000 residents voting using an app called Scytl. After completing the registration procedure, the voter registers with authorities, obtains their voter ID, and selects a 6-digit pin. After casting their vote, they enter the system with their ID and PIN and receive a 12-digit receipt number. To authenticate their vote, the voter uses their ID, PIN, and receipt number to get the information.

Estonia is the first country in the world to implement electronic e-voting in elections. It requires the Internet as well as an Electronic National Identification Card for authorization, encoding, and signatures. Voters must download the voting program, verify with their electronic ID, and then vote from a list of candidates if they are eligible.

Polyas is used in Germany for democratic elections. Polyas is the only e-voting software provider whose e-voting technology has been approved by the German Federal Office for Information Security. In 2011, Norway implemented e-voting for regional elections. The program is somewhat decentralized and anonymous. Due to cyber-attack worries, the nation discontinued the use of e-voting platforms.

In 2014, Russia launched e-voting for over two million individuals. Russia also made use of Waves' blockchain-based e-voting technology. The system employs a Proof of Authority-based crash fault tolerance consensus method. Smart contracts are used to save voting process rules, registration information, and vote verification.

Sierra Leone embraced Agora as their e-voting system for the election for president in 2018, making it the first time blockchain technology was employed in a presidential election.

In South Korea, around 9,000 citizens voted in 2017 for a Blockchain project that used a smart contract based on blockchain technologies.

Switzerland held municipal balloting utilizing Luxoft-developed e-voting technology. The bulk of their national voting procedures from state-wide elections and referendums use the Swiss e-voting system. The suggested system is a mobile phone application that confirms via Short Message Service (SMS). Voters insert their ID into the e-voting website and follow the instructions to cast their vote; they enter a PIN and match a security symbol to the one they got in the mail. If the two match, the vote is accepted by the system. Following that, individuals input PIN numbers, the name of the referendum, and the response (positive or negative).

The study [C2] evaluates blockchain-based electronic voting systems' global adoption, emphasizing on registration processes. Noteworthy implementations include Australia's use of Scytl for state elections, Estonia's pioneering use of Electronic National Identification Cards, and Russia's deployment of Waves' blockchain technology. Despite outcomes, challenges such cyberattacks forced Norway to abandon electronic voting, revealing the convoluted nature of e-voting adoption throughout the world.

### Ethereum efforts

Using blockchain technology, this study [C4] presents a privacy-preserving e-voting system that allows score voting. The method is built on the Ethereum blockchain to enable safe and private voting in the digital era. The system is made up of multiple modules, including a registration module, a balloting module, a tally module, and an authentication module, and it employs a variety of cryptographic approaches to protect the voting process's secrecy and integrity. The system enables score voting, a form of voting system in which voters award a score to each candidate rather than choosing a single candidate. This enables voters to express their choices more precisely, potentially leading to more representative election results.

The system is built on the Ethereum blockchain, an open-source system that allows developers to create and deploy distributed applications. Because all transactions are recorded on a public register that is available to all participants, the adoption of blockchain technology assures that the voting process is transparent and tamper-proof. The registration module enables voters to register for the election and assigns each voter a unique identification. Voters may cast their ballots using a safe and user-friendly interface thanks to the voting module. The tallying module gathers votes and computes election results autonomously. The verification module enables participants to validate the voting process and confirm that the results are correct. The system is examined using an empirical assessment on the Ethereum blockchain, which demonstrates that it can withstand workloads of up to 10,000 transactions transmitted at a rate of 200 per second before experiencing substantial performance decreases. Increased voter engagement, enhanced election integrity, and lower costs associated with traditional voting methods are all possible benefits of establishing a privacy-preserving e-voting system.

In order to ensure anonymity in score voting, this paper [C4] proposes an Ethereum-based blockchain-based electronic voting system. By utilizing cryptographic techniques across its modules, the system permits accurate voter expression, ensures transparency, and may provide advantages over conventional approaches such as improved election integrity, more voter participation, and lower costs.

### Risks in blockchain based protocols

The study [C3] indicates that blockchain technology has the potential to alter the way elections are conducted and gives insights for scholars and practitioners interested in this field.

Tsukuba City in Ibaraki Prefecture, Japan, employed blockchain and My Number cards for the first online voting validation test in August 2018, according to Jun Huang and Debiao.

The government urged residents to use innovative technology to generate new ideas to benefit society, and in the final voting phase, they employed a blockchain-based voting system to choose the final supported works from the contenders. The legitimate voters were identified using the My Number card.

The report additionally addresses the application of blockchain technology in the 2018 presidential election in Sierra Leone. The National Electoral Commission recorded and verified the votes cast in the election using a blockchain-based voting technology. The approach was developed to prevent fraud and preserve the voting process's openness. It further addresses the usage of blockchain technology in the 2019 Moscow City Duma election. To enable residents to vote remotely, the government adopted a blockchain-based voting system. The technology was created to protect the voting process's security and authenticity.

The study [C3] highlights how blockchain technology has the ability to completely change election processes and provides insightful information for professionals as well as scholars. Through case studies in Moscow, Sierra Leone, and Japan, it illustrates how blockchain technology may be effectively used to improve vote security, thwart fraud, and promote transparency in election processes.

## Other efforts

Follow my vote

Sovereign

Plus

Voatz

* The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

Swiss post:

* Running the Race: A Swiss Voting Story
* A privacy attack on the Swiss Post e-voting system
* Vulnerability Assessment of Swiss Post E-Voting System

French legislative e-voting protocol:

* Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol

Openvote network protocol

New south wales ivote system:

* The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election

# The future of e-voting… a dead end? (to expand)

Critical opinion - at the end

# References

[1] Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, *71*, 279-286.

[2] Horster P, Michels M (1995) Der vertrauensaspekt in elektronischen

wahlen. In: Trust Center. Springer, pp 180–189

[3] Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, *71*, 279-286.

[4] Tarasov, P., & Tewari, H. (2017). The future of e-voting. *IADIS International Journal on Computer Science & Information Systems*, *12*(2).

[5] Buck, M. (2022). *Security analysis of the Russian federal remote e-voting scheme* (Bachelor's thesis).

[6] Vakarjuk, J., Snetkov, N., & Willemson, J. (2022, June). Russian federal remote E-voting scheme of 2021–protocol description and analysis. In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference* (pp. 29-35)

[A1] Gonggrijp, R., & Hengeveld, W. J. (2007). Studying the Nedap/Groenendaal ES3B voting computer.

[A2] Kusters, R., Truderung, T., & Vogt, A. (2012, May). Clash attacks on the verifiability of e-voting systems. In 2012 IEEE Symposium on Security and Privacy (pp. 395-409). IEEE.

[A3] Wallach, D. (2006). Security and Reliability of Webb County’s ES&S Voting System and the March 06 Primary Election.