Vincent-Lübeck-Gymnasium
Glückstädter Str. 4,
21682 Stade

Facharbeit im Seminarfach:
Computing and Society (Bilingual)

Electronic Voting:
An opportunity or liability for society?

Verfasser/in: Jonas Wilms
Fachlehrer: Dominic Twyman
Abgabetermin: 21.2.2018
Ort und Datum: Stade 19.02.2018

Contents

1 Introduction

"Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. [...] The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."

– Article 21, Universal Declaration of Human Rights [19]

Elections and Voting are the core of every modern democracy. They ensure that no single person or minority is able to take over the power of state, therefore creating a stable way of forming a government. As being vital to a fair and democratic system, they are always a target for manipulation by parties, who want to influence the outcome of an election towards their candidate or towards their opinion. To prevent such influences, countries developed complicated systems for collecting, counting and verifying the results of voting. The recent development involves the usage of computers to replace the volunteers involved in that process, which is called E-Voting. This paper should compare the different methods for voting and especially processing elections to then judge if E-Voting is a viable or even better alternative compared to other voting systems concerning security and accessibility.

2 Principles of an Election

To ensure that the outcome of an election represents the free wish of the people, certain rules were developed over time to enforce that no one can influence the election. These rules are a good way to judge if a certain voting system is able to process a fair election. As there are no international standards on how to process a fair voting, I will now try to present a set of guidelines that represent the different international standards. If the government could forbid certain people to vote or could change how much a certain vote is counted, it could influence the outcome greatly. Therefore it is mandatory for a fair election that everyone who is able to vote is also allowed to vote and that every vote has the same weight. This also means that everyone can only cast the same number of ballots, usually one per election. In addition an election is only considered fair, if everyone is allowed to run for office, and everyone is allowed to vote based on his own opinion, without their choice being

influenced by others. To ensure that the choice is free, it is important that a voters decision is as secret as possible. If it would not be secret, a party could identify the supporters of the opposition and force them to retract or change their vote or prevent them to participate. While a secret voting enables a fair election, the result could still be influenced while counting. To prevent this, the counting must be as transparent as possible so that everyone can verify that the counted results are valid. This transparency must apply to every part of the voting process, from the counting of the ballots at the polling station until the final results are summed up. Just one unverifiable step might allow fraud to happen.

3 Paper based voting

The first votings were held without any ballots at all. The candidates were read out and every voter simply raised his arm when he heard the name he wanted to vote for and the arms were counted. Another method was that every voter went to the polling station and simply told his vote to the personnel. They then kept big lists of voters and their choice and summed that up [9]. While these systems worked quite well for small votings with a few hundred voters involved, they tend to fail in a large scale. They also do not fulfill the voting principles that ensure that a voting is indeed fair. Therefore systems using paper ballots were developed. After the voter went to a polling station and authenticated himself, he receives a paper ballot with a list of all candidates written on it. He then marks the candidate he wants to elect using a pen or a stamp and then folds the paper to hide his vote from the polling station officials and puts it into a closed box were all the ballots are collected. This does not require any special knowledge so everyone can participate in the voting. However that excludes disabled people that are not able to leave their house and go to the polling station. Additionally, many people are too busy to vote, and if there is no law that forces the voters to vote, a lot just don't participate. To resolve both problems, voting via the mail was invented. The voters that can't vote in person send a form to the authorities to order the ballots. They then receive them with the mail, fill them out at home and send them back to the authorities. While this is very comfortable, it comes with a huge risk: Fraudsters might exchange the ballots on their way to the authorities. There is no way for the voter to verify that his vote was cast as intended. After the

election closes, the polling station officials open the box and count the votes. The officials are often volunteers. As the counting is very simple nearly everyone can volunteer in the polling station which increases the trustworthiness of the results as the officials are part of ”the people”. To count the thousands of ballots that arrive at the polling stations, the volunteers count them manually in some countries. In most countries the counting is held in public so that everyone can actually see that his vote is counted. As there is no complicated math involved, everyone can verify that the votes are summed up correctly, and every voter can see that all the paper ballots put into the box are indeed counted, so he can be sure that his own vote is counted as intended. Germany is one of the countries that still uses paper voting. To collect, count and verify about 46 million votes casted at the Bundestagswahl in 2017, about 650 000 voluntary election officials helped [18][1]. The volunteers need to be paid and the ballots need to be printed, which summed up to a total cost of 69 993 925 € for the federal elections in 2013[22]. This shows that manual voting requires a lot of work to be done, which is quite expensive. To reduce the amount of work needed, systems were invented to count the votes with machines. So called optical scanners scan the collected votes after the polling stations closed and count the votes for each candidate. But while the machines are able to count much faster than humans which reduces the time needed to count, this also means that humans are unable to follow which makes it difficult to verify that the machines were right. In South Korea they came up with a method of making it easier to verify the results: The scanning machines do not only count the votes but also sort them and bundle them in stacks with 100 votes each. Therefore it is easy to recount the results manually [15]. Scanners are just possible due to the recent evolution in scanning systems and computers in general. Before these systems were introduced, punch card voting systems were invented. Those systems were used extensively in the US until 2014. Instead of making a cross on a paper to cast a vote, the voter inserts a punch card, which is basically a table printed on a piece of paper, into a template, that contains holes next to the candidates name. To vote for a candidate, the voter uses a needle like tool to make a hole into the punch card at the position that refers to the candidate. The punch cards are then collected in a box. They are then counted using special machines that are able to read the punch cards through detecting the holes. As the votes are recorded on paper, this system allows for recounts on different counting machines or even

Figure 1: The ”Votomatic”, a widely used punch card system [21]

by hand to verify the results. Though it is hard for the voter to verify that he voted for the candidate he intended to[21]. Despite the fact that it is possible to verify, it is impossible for humans to detect when the machine fails to count as it is hard for humans to read the punch cards. All in all paper ballot voting ensures private voting as it is impossible to identify the owner of a specific ballot as it does not contain any information about the voter. While the voter can't verify that his vote was actually counted, he can verify that all the votes, including his own, went into the ballot box and were counted later, so if the counting is public he can make sure that the election was fair. While a single person might only verify the results of one polling station, a group of people can verify the whole system. As every fraud detected would become public, these systems can be verified completely and if the voter casted his vote at the polling station he can be sure that his vote was casted. That this works in practise is shown by an incident that became public that happened in local county elections in Germany. To enable disabled people to participate in the election, they were allowed to sign a contract that transmitted their voting right to someone else. The defrauder signed fake contracts in the name of others. He then received about 150 ballots that he filled with his own name. However the fraud was detected when the ballot owners arrived at the polling station and noticed, that their vote was already handed in. This shows that this voting system allows to detect some types of fraud[3].

All in all, paper ballots allow a lot of people to participate and the system is quite bulletproof in detecting fraud, however the increased accessibility achieved with mail voting also increases the risk that votes are influenced.

And while using scanning machines reduced the time and effort needed for an election, a punch card or a paper ballot still needs to be printed for every voter and verifying the voter is still required. This means that the voting is still expensive. To reduce the cost, voting machines were invented to replace paper ballots.

4 Voting machines

Voting machines were invented in the early 19th century [9] and are aimed to reduce the number of volunteers and the time it takes to count the votes. Various systems were invented since then. The earliest systems were simple mechanical counters known as lever machines. They had a counter for each candidate and a button which increased the counter when pressed by a voter. Mechanisms locked the buttons after a button was pressed so that every voter could only vote once [10, page 5]. While those machines were relatively easy to use for voters, as they only required a button press, they did not fully replace the voting officials as an identity check of the voter was still required. Additionally the polling station personnel still had to sum up the votes of every machine. The biggest disadvantage of those voting machines is however that no one could guarantee that mechanical failures would not happen. As voting machines usually keep their results secret, a voter cannot verify that his vote was indeed recorded[10, page 3]. Early systems also had no ability to recount the result which disqualifies lever machines to be used in votings.

4.1 Direct-recording voting machines

The next stage of inventions are called direct-recording electronic voting machines (DRE's) which aimed to replace all the paper and manual counting needed using techniques previously mentioned. A DRE is basically a computer which has a special User Interface for elections, and is also counted as E-Voting. They are widely used today in various countries, including the USA and Brazil [7]. In opposite to voting with machines or via paper ballots the DRE's can guide the voter through the voting process. Therefore spoiled ballots (either intentionally or unintentionally) are prevented. Recent DRE's also provide additional input methods so that disabled people can also vote. The votes are stored inside the memory of the DRE and are either displayed

to the local election officer or directly sent to the voting authority after or even during the election [5]. However this simplification also has its downsides: While this makes elections very easy and fast to process and count, there are a lot of attacking vectors in this kind of systems. The voting machines, the connection to the election servers and the election servers itself need to be secured, which requires a lot of technical expertise. And if someone finds a way to circumvent the security measures taken there is no way to notice it, as the DRE's provide no way for the voter to verify that its vote was casted. Not to mention that its impossible to verify that all votes are counted up correctly. After the use of DRE's of the company Nedap during elections in the Netherlands and in Germany, various huge design mistakes were found. To secure the internal computer against manipulation, it was surrounded by a metal case and locked with a key. That key however was the same for all devices making it easy to replicate. To then manipulate the election, the internal computer was set into its maintenance mode using a hardcoded password ”GEHEIM” (eng.: ”SECRET”). An attacker would then be able to completely override the systems software[16]. After these issues went public, voting machines were immediately forbidden in both countries[11][20]. Similar problems were found in the DRE's that are used in the US federal elections, which shows that unsafe voting machines are common [13]. All in all voting machines reduce the work involved in an election and enable more people to vote. However the use of voting machines makes it unable for the voter to even verify that his vote was cast. Mechanical failures and digital attacks were already proven multiple times which increases the concerns against voting machine based elections. And they still require the voters to go to the next polling station. To allow people to vote from nearly everywhere, Remote E-Voting was developed.

5 Remote E - Voting

The term Remote E-Voting describes a voting, where voters can vote via the Internet. That makes E-Voting quite easy from the voter's perspective. Instead of visiting the next polling station which takes time and might be difficult due to physical disabilities, people can vote from everywhere around the world. The only requirements are a functioning computer or tablet or mobile phone, an Internet connection, which exists nearly everywhere today, and a

way to verify themselves, which is usually possible with a code sent to every eligible voter, or in some countries the ID card provides this functionality. However that might exclude people without an Internet connection from the ballot.

5.1 A matter of trust

As many cases already showed, Internet ballots can be tampered with in a lot of ways, and its hard to detect such frauds. This happened in France, Norway, Finland and Canada were tests with on-line voting were canceled because of security concerns [12][14][6][8]. To make fraud impossible, the system involved to cast votes needs to provide technical countermeasures against such attacks. For that, skilled developers are needed as well as a lot of infrastructure, which not every community can afford. However that might still be cheaper than printing paper ballots and organizing the polling stations personnel. Even if the system is as secure as possible, people still mistrust the Internet. Data leaks and breaches are in the news every day, so people may won't believe, that cryptography can be uncrackable. And while most E-voting strategies allow every person to verify the voting results with checksums and hashes, it requires a good technological understanding to do so. While people understand how their paper ballot is counted, voting via Internet seems to be magic. Therefore most E-Voting solutions focus on being understandable rather than providing absolute security.

5.2 Is the Internet stable enough?

As stated above, remote E-Voting requires an Internet connection. That does not seem to be bad as an Internet connection is nearly available everywhere. However someone could attack the connection to prevent a certain group of voters from voting. While a physical attack, such as cutting the Internet cable is risky as one needs to do that in person, so called Distributed Denial of Service attacks can be started from computers all over the world. In most cases it is impossible to find the individual that started the attack. To attack the voting system, the computer network of an attacker would send thousands of requests to the voting servers. These then get busy and are unable to respond to the voters requests. While such DDOS attacks cannot target a certain group of voters, they do affect every voter which allows an attacker to

prevent the voting to be carried out. One way to mitigate these kind of attacks is to request the Internet service provider to block the attackers connection. But that may affect innocents that share the same IP address. Another way would be to set up more servers than the attacker is able to attack. While this is quite effective it also increases the cost as more servers need to be bought and maintained.

5.3 Can we trust our computers?

On a modern computer programs can be installed and run in parallel. The operating system ensures that the programs data is strictly separated and limits the rights of installed programs. Before it grants certain rights to a program it prompts the user to validate this. While this could create a secure basis for running applications and servers for carrying out a voting, the system is to complex to run without problems in reality. Small mistakes done by the programmers can cause the security mechanisms to fail, which allows malware to run on the computer without the user noticing. Even if there are no known attacking vectors, a malicious program could still mask itself as a useful application and simply request the rights from the user. The possibility of attacks does not only apply to E-Voting but also applies to online banking and many other systems. Therefore the voter is very likely to be aware of such risks and is taking countermeasures like installing an anti virus program. Some remote E-Voting systems also address these attacks by separating the process onto multiple devices so that the different devices verify each other, so that manipulation can be detected. The probability that the malware infects all devices is very unlikely. Therefore remote E-Voting can not be totally secure as it relies on the voters computers and the providers network security and stability. However as more and more things get connected to the Internet, one could argue that this is a known risk for society that is not directly related to E-Voting. The only country that actually implemented remote E-Voting successfully is Estonia.

5.4 Case study: Estonia

In Estonia, E-Voting was first tested in 2005. Since then it was successfully used in multiple elections in local, parliament and EU elections for more than 10 years. The success was only possible as Estonia also adopted e-

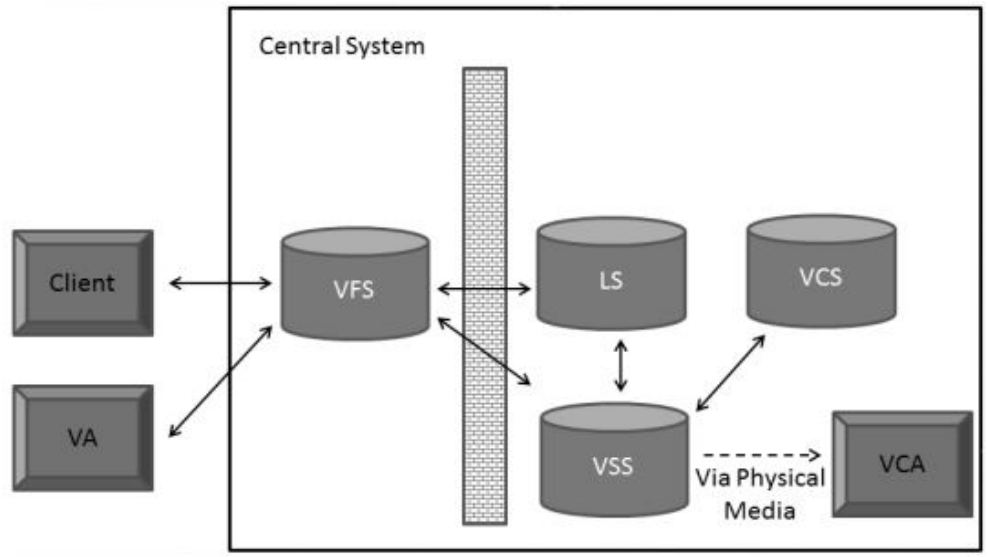

Figure 2: Estonian voting system architectural overview [2, Figure 1]

governance very early. That means that most official forms and paperwork can be filled in online. Estonia also introduced a digital ID card in 2002 that allows to verify their owners and allows them to cryptographically sign documents using a 2048 bit RSA key pair, which is an asymmetric encryption that is considered safe until today. This ID Card is mandatory for the remote voting as it allows the citizens to authenticate themselves against the voting servers. The signing function is also necessary as it prevents the ballot from being manipulated while being sent over the Internet. Every citizen over the age of 15 is required to have this ID card, therefore requiring the ID card for the elections does not exclude valid voters. It is even in use at the public transport in Estonia's bigger cities, where the ID card replaces paper based tickets. This high acceptance of the ID-card makes E-voting possible. To prevent fraud, the ID card requires a PIN before it authenticates its owner, or signs a certificate (in the sense of a digital signature) for him. The Estonian election system was designed with simplicity in mind, it should be similar to the paper ballot based elections[2, page 1 - 3]. The voter uses two seperate programs for processing the election, the *Client* used for voting and the *Verification Application (VA)* to verify the voting results. They were split up into two programs that only run on different operating systems to prevent fraud. The *vote forwarding server (VFS)* adds another security layer between the world wide web and the voting servers and provides public data related to the election, including candidates and the public key of the *vote counting application (VCA)*. It redirects all the votes received to the *vote storage server (VSS)* which stores the votes, ver-

ifies the voters identity by requesting the *validity confirmation server (VCS)* and removes duplicate and wrong votes. The server however cannot access the users votes, as they are still encrypted. When the election period ended, the *VSS* then removes the voters identity from the ballots. These now anonymous and still encrypted votes are then physically transfered to the final VCA which holds the private RSA key the votes are encrypted with, so it is able to decrypt and count them. The separate *log server (LS)* collects log data from the other servers to detect system failures and frauds and is thus able to verify the elections integrity.

Through this system, none of the servers can connect a voter to his vote. While the VSS knows all the voters who have voted, it does not know their vote as the vote is encrypted. The VCA is able to decrypt the votes, however it does not know the users related to the votes as they were removed by the VSS. Therefore, the users vote stays private unless both servers have been compromised. As they are under strict observation of the electoral committee, this is rather unlikely to happen without being detected. To fraud the election, only the VCS needs to be taken over as manipulating it allows the defrauder to influence the counted result.

The biggest security concern however seems to be the users device, as not every user has a technical knowledge and might not detect that malware is running on his device. The malware could simply sign a different vote than the voter wanted. To prevent this, the client stores a number in the ballot and displays it to the user. He can then enter that code into his mobile devices VA, which then contacts the servers and checks that the vote related to that number really elected the right candidate. As it is very unlikely that both the mobile device and the desktop computer the client runs on get infected by malware from the same author, it allows for a secure verification that the vote was sent to the VSS. However one still needs to trust the software published by the government[2, page 5 - 9].

A group of researchers found rather huge bugs in the servers software that would have allowed an attacker to compromise the whole system. Those bugs were then fixed. However it shows that the 'rather unlikely' cases described above can actually happen. While such attacks have not yet been detected, there is no guarantee that they do not exist. This insecurity was criticized by many researchers[2, page 10, 11]. To ensure that code is free of bugs, it is a common practice to do code reviews by independent experts, called audit,

or to publish the source code so that everyone can search for mistakes. After being criticized that such reviews were not done [17], the source code was published on-line [4].

While only 1.9% of the voters used Internet voting when it was introduced, nearly one third of the voters voted via Internet in the recent elections. In the parliamentary elections 2011, only one vote was corrupted, which shows that the system is indeed working in a huge scale [2, page 12]. While this shows that Remote E-Voting is indeed working in reality, the Estonian system is far from perfect. That one needs to trust the voting server administrators and that fraud is 'unlikely' to happen does not satisfy cryptographers.

5.5 Cryptographers dreams

The ultimate election protocols exist already, at least their authors say so. However while these systems are secured and verifiable using cryptographic techniques, it is hard for non-cryptographers, which means big parts of the society, to understand, trust and work with these systems. Therefore the general public mistrusts them, even if they are without any possibility to attack or fraud the election. Therefore the recent development in the cryptographers community is to ensure that the protocols are also understandable to everyone.

5.6 A sample protocol using homomorphic encryption

Xukai Zou, Huian Li, Feng Li, Wei Peng and Yan Sui present such a system in their paper "Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election". They claim that counting the final results *"is simply modular addition and can be performed by everyone"* which ensures that the voting is totally transparent for everyone [23, page 2].

Assumptions To schedule the voting, this scheme needs at least two so called "collectors" that are part of different parties involved in the election to make sure that they won't exchange secret informations with each other. The collectors control each other, so if a collector tries to manipulate the election the other will notice and can start a repetition of the voting. They also propose that elections with bigger groups of voters are split up into smaller groups of a few thousand voters, because the computation involved is increasing exponentially with the number of voters, so splitting the voters will also split up

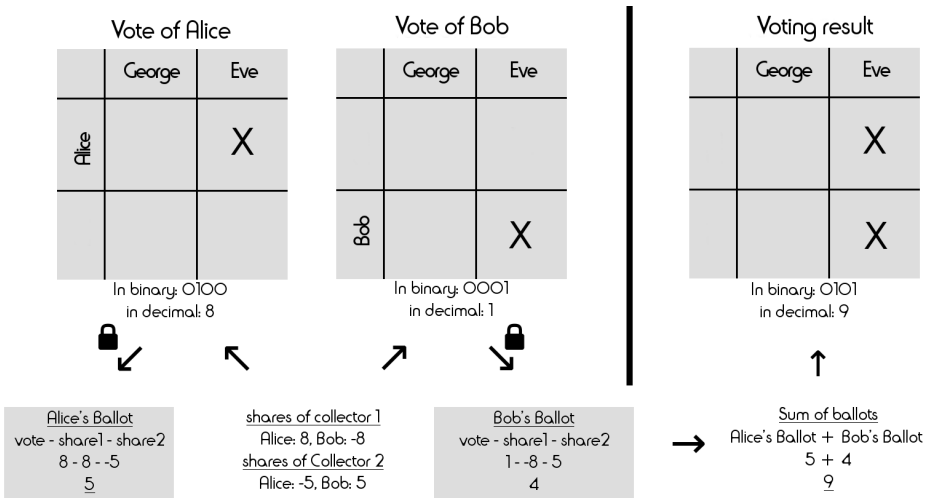

Figure 3: Scheme of the proposed voting system

the computation time needed from one long computation into multiple smaller, which allows them to be done in parallel. The authors claim that while a honest voter that only casts one vote is anonymous while voters involved in fraud can be identified. [23, page 24]

How it works Each of the collectors generates a secret number called share for each voter so that the sum of shares is 0. The voter connects to every of the collectors, they verify each others identity somehow and set up a secret channel. The collector then sends the voters share and the list of candidates to the voter. All collectors send the same list. The voter then generates a unique row number (so that no no other voter uses it) ranging from 1 to the number of voters. This uniqueness check uses multiple rounds of generating a number and checking the results until all voters got a unique one. The client then cast the vote through building a table of binary values with a column for each candidate and a row for each voter. It then sets every value to zero except the one at the column of the candidate he wants to elect and at the row his row number refers to. He can then turn the table into a number by reading it from left to right, row by row as a binary number. While that number still directly contains the voters choice, the voter hides his choice by simply subtracting all the shares the collectors offered from that number. This number, which seems to be completely random now, is send back to the collectors. The collector cannot calculate the vote out of it as he does not know the shares the voter received from the other collectors. Therefore it is mandatory that the collectors keep the generated shares private from each other. The collectors can

now make every voters number public and everyone, including the collectors, can sum up the values now. As the sum of shares is zero, summing up all the numbers actually erases all the random numbers added by the voters and the final sum only contains the voter's vote. This behavior is called homomorphic encryption. The final sum can then be written into a table again, reversing the procedure done when casting the vote. It can now be validated that every row (that refers to a voter) only contains one 1, so that every voter only voted once. To get the final results one simply needs to sum up the 1s in a certain column to get the result for the relating candidate[23, page 4 to 7, 10 to 13]. While everyone is able to verify that table the authors' assumption that everyone can do this is a bit overestimated. While their examples show simple calculations with 3-digit numbers, these examples assume 4 voters and 2 candidates. For a few thousand voters the numbers grow to a size which only computers can handle accurately. That is the reason why they propose to publish the calculations live, with every addition in a single row so that everyone can check a few calculations and check that its own ballot is included, so that the whole calculation was verified part-by-part by at least one person. More importantly, everyone with a software implementing this protocol could download all votes and do the calculation on its own. Even though every single vote is verifiable, no one can actually relate the row number to a certain voter, not even the collectors can. And as long as the collectors keep their shares private, no one can turn the encrypted votes published into the private vote the voter casted. The only way to break the encryption would be that the majority of voters colludes with a collector or that all collectors exchange their shares, which would allow the collectors to decrypt the encrypted ballots. But this assumes that the collectors from different parties collaborate, and if that happens something is very wrong in the democracy already, so in a working democracy one can assume that this is nearly impossible to happen. However voters could cause trouble by voting in the row of another person, multiple times or not at all. That could create two different outcomes: In most cases during summing up one can detect a wrong vote and can exclude it (which requires a bit more calculations, left away for brevity). In some very rare cases when two votes equally collide (two wrong voters vote for each other) this can't be detected. However then there is no benefit for the fraudsters whatsoever. If a certain voter did not provide his vote in time, the collectors could exclude it from the calculation by publishing the shares related to that ballot. A fake ballot could

then be generated for it. Through that, voters can be excluded from the election. However this requires all the collectors to participate which ensures that this step does not influence the outcome but is only used to make the results accessible[23, page 12 to 18].

The perfect voting system? The authors' claim that actually everyone can understand what is going on is definitely exaggerated as the addition is not that simple. However a large group of people can actually verify the whole system, so fraud can definitely be detected. However the authors explicitly exclude *"attacks [...] targeting at general computers or network systems"*. So they assume a perfect Internet connection between all of the voters and the collectors without failures and connection loss. The assumption that a few thousand voters keep their devices running with an Internet connection until they decided for a unique row for each user is not prepared for failures of all kinds. A power failure, Internet connection breakdowns, computer crashes or hardware failures or even dumb voters shutting down their computer can cause the whole election to fail. Therefore the protocol proposed is working nicely in theory, however it definitely fails in reality. The authors admit that their system for generating the unique row numbers is not perfect, and propose alternative methods to be invented in the future. If that problem is solved it could indeed work as claimed, enabling a completely secure, verifiable voting that ensures privacy[23, page 24].

6 Conclusion

Voting is one of the cores of democracy. Frequent elections ensure that the actions the government takes are backed by the people. They are therefore mandatory for a stable government. Voting systems that use paper ballots are used worldwide for more than hundred years. Since then no serious weakness was discovered. However those elections require a huge amount of work, money and personnel and they require each participant to go to the next polling station, which limits the frequency of elections. To increase the number of elections, they need to be cheaper, simpler and faster. To achieve this, voting machines were developed. However they are often insecure and provide no benefit for the majority of voters whatsoever. E-Voting seems to be a better solution. Voting via Internet is easy, fast and cheap. But while a lot

of countries experimented with E-Voting in recent years, most of these experiments were declined because the governments failed to introduce a secure E-Voting system, which is quite hard to achieve. Estonia is the only country where E-Voting seems to be working without problems during larger elections. The main reason why it works is that Estonia was also the first country that adopted E-Government. E-Voting would not be possible without the E-ID. Until other countries reach this state of digitalization it will take a few years. The Estonian E-Voting model is simple but definitely not secure. That the votes are counted correctly is in the hands of the administrator who could manipulate the votes. However there are indeed alternative cryptographic schemes that allow for totally secure, private and fair votings. But none of them has been tested in practice yet even less so on a large scale. Therefore it remains to be seen whether E-Voting is an enrichment for democratic societies, but it is very likely going to be.

References

[1] *Bundestagswahl 2017*. Der Bundeswahlleiter, Statistisches Bundesamt. URL: https://www.bundeswahlleiter.de/bundestagswahlen/2017/ergebnisse/bund-99.html (visited on 01/24/2018).

[2] Dylan Clarke and Tarvi Martens. "E-voting in Estonia". In: (). URL: https://arxiv.org/pdf/1606.08654 (visited on 01/10/2018).

[3] *Details zur Briefwahlaffäre in Stendal*. MDR. URL: https://www.mdr.de/investigativ/briefwahl-affaere-stendal-wahlbetrug-100.html (visited on 02/03/2018).

[4] *Estonian State Electoral Office's Github Profile*. Estonian State Electoral Office. URL: https://github.com/vvk-ehk/ivxv (visited on 02/09/2018).

[5] *ExpressVote XL*. ESS HEADQUARTERS. URL: https://www.essvote.com/products/12/51/universal-voting-system/expressvote-xl/.

[6] *Finnish e-voting results annulled, municipalities to hold new elections*. Electronic Frontier Finland, 2009. URL: https://effi.org/blog/2009-04-09-EVoting-Supreme-Admin-Court.html (visited on 02/19/2018).

[7] *How Brazil has put an 'e' in vote*. BBC, Aug. 1, 2008. URL: http://news.bbc.co.uk/2/hi/7644751.stm (visited on 02/19/2018).

[8] *Internet voting pilot to be discontinued*. Norway's Ministry of Local Government and Modernisation, June 25, 2014. URL: https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/ (visited on 02/19/2018).

[9] Douglas W. Jones. *A Brief Illustrated History of Voting*. URL: http://homepage.divms.uiowa.edu/~jones/voting/pictures/ (visited on 02/19/2018).

[10] Douglas W. Jones. "Early Requirements for Mechanical Voting Systems". In: (). URL: http://homepage.divms.uiowa.edu/~jones/voting/ReVote09history.pdf (visited on 02/01/2018).

[11] André Kramer. "Nedap freut sich über das 'Aus für Nedap-Wahlcomputer'". In: (June 9, 2007). URL: https://www.heise.de/newsticker/meldung/Nedap-freut-sich-ueber-das-Aus-fuer-Nedap-Wahlcomputer-187464.html (visited on 02/03/2018).

[12] John Lichfield. “Fake votes mar France’s first electronic election”. In: (June 3, 2013). URL: http://www.independent.co.uk/news/world/europe/fake-votes-mar-france-s-first-electronic-election-8641345.html (visited on 02/19/2018).

[13] Adam Lusher. “Hackers breached defences of US voting machines in less than 90 minutes”. In: (July 31, 2017). URL: http://www.independent.co.uk/news/world/americas/us-politics/us-election-hacking-russia-russian-hackers-cyberattack-donald-trump-voting-machines-def-con-a7868536.html (visited on 02/19/2018).

[14] Leslie MacKinnon. *Elections Canada drops plan for online voting due to cuts*. URL: http://www.cbc.ca/news/politics/elections-canada-drops-plan-for-online-voting-due-to-cuts-1.1346268.

[15] Tim Meisburger. *Korean Elections: A Model of Best Practice*. Apr. 20, 2016. URL: https://asiafoundation.org/2016/04/20/korean-elections-a-model-of-best-practice/ (visited on 02/11/2018).

[16] *Nedap/Groenendaal ES3B voting computer a security analysis*. URL: http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf (visited on 02/03/2018).

[17] Barbara Simons. *Report on the Estonian voting system*. Sept. 3, 2011. URL: https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/ (visited on 02/09/2018).

[18] *Tatkräftiger Einsatz: etwa 650.000 Wahlhelferinnen und Wahlhelfer bei der Bundestagswahl 2017*. Der Bundeswahlleiter, Statistisches Bundesamt. URL: https://www.bundeswahlleiter.de/info/presse/mitteilungen/bundestagswahl-2017/18_17_wahlhelfer.html (visited on 01/24/2018).

[19] *Universal Declaration of Human Rights*. United Nations, Sept. 10, 1948. URL: http://www.un.org/en/universal-declaration-human-rights/ (visited on 02/03/2018).

[20] *Verwendung von Wahlcomputern bei der Bundestagswahl 2005 verfassungswidrig*. Bundesverfassungsgericht. URL: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019.html (visited on 02/03/2018).

[21] *Votomatic*. Verified Voting Foundation, Inc. URL: https://www.verifiedvoting.org/resources/voting-equipment/ess/votamatic/ (visited on 02/01/2018).

[22] *Wahlkostenerstattung*. Der Bundeswahlleiter, Statistisches Bundesamt. URL: https://www.bundeswahlleiter.de/service/glossar/w/wahlkostenerstattung.html#id-0 (visited on 01/24/2018).

[23] Xukai Zou et al. “Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election”. In: *Cryptography* 1.2 (2017).