Analyzing and Improving Eligibility Verifiability of the Proposed Belgian Remote Voting System

Jan Willemson[0000−0002−6290−2099]

Cybernetica, Narva mnt 20, 51009 Tartu, Estonia
jan.willemson@cyber.ee

Abstract. This paper discusses a recent hybrid paper-electronic voting system proposal put forward for Belgian elections. We point to some problems in the proposal, and consider addition of blind signatures as one possible approach to dealing with the identified shortcomings. We discuss the concomitant updates from both the protocol and electoral processes point of view, arguing that our proposal would strike a better balance between different requirements. To the best of our knowledge, this is also the first proposal to use blind signatures in a paper-based voting system.

Keywords: Remote voting · eligibility verification · blind signatures

1 Introduction

In our current increasingly mobile world, it becomes harder and harder to get all the eligible voters to physical polling stations for the act of voting on a single day [27]. The recent COVID-19 outburst has only added to this problem [9]. Hence, there is a definite need for reliable remote voting options.

Two main approaches are available for this. The more established way is to send the ballots in via physical mail. For example in the 2020 U.S. presidential elections, 43% of the voters cast their ballot by mail – a number twice as high as four years earlier. Even though the COVID pandemic was definitely a major factor, the trend towards increasing voting by mail has been observed for years in the U.S. [10].

As an alternative, several countries like Switzerland [14], Estonia [12], Norway [25], Australia [8], France [6], etc. have had elections with vote casting options over Internet.

Both of these approaches have their pros and cons. Internet voting can offer reliable vote transmission and efficient tallying procedures. On the other hand, it has been criticized for implementation complexity, concentrating many risks into the central components, being hard to verify by an average citizen, etc. [15, 24, 21]

Postal voting can be implemented without relying on any digital equipment on the client side, hence being easy to understand, use and trust by the voter. On the other hand, it is very hard to ensure authenticity and privacy of the voters,

the postal channel is vulnerable to both integrity and confidentiality attacks, etc. [17, 4]

Thus, it is natural to ask whether we could get the best of the both worlds without sacrificing too much in terms of residual risks. And indeed, several digital-paper hybrid schemes have been proposed in the literature [4, 3, 10, 20]. Of course, building such a hybrid system requires trade-offs, and balancing different requirements may lead to several possible equilibria.

In this paper, we are going to take a closer look at a recent proposal presented by a team of Belgian researchers with the aim of being implemented for postal voting in Belgium [1, 2, 11]. The advantage of this proposal over the previous purely academic papers is that it comes with technical implementation details much better laid out. Belgium also has a national electronic identity system which opens up new opportunities in terms of voter authentication and eligibility verification.

We note that the current version of the paper has been shortened due to space limitations, but interested readers can have access to the full version at [28]. The main difference between the current and the full version is a review and analysis of previously proposed hybrid schemes, more specifically the Benaloh-Ryan-Teague scheme [4], STROBE [3], RemoteVote and SAFE Vote by Crimmins *et al.* [10], and the scheme by McMurtry *et al.* [20]. Remarkably, none of the proposals explicitly deals with eligibility verification, even though it is one of the core components of end-to-end verifiability.

Crimmins *et al.* claim in [10] that STROBE, RemoteVote and SAFE Vote all provide the eligibility verification property, but do not specify how exactly. The only explanation given is a reference to 'existing procedural controls' in a footnote, possibly hinting at the standard methods used in postal voting like double envelopes.

Note, however, that double envelope system is a legacy adopted not because of its excellent properties, but because historically there has not been a better alternative. For instance it does not really protect vote secrecy against a malicious actor while the vote is in transit; thus we question the ballot secrecy claims made in Table 1 of [10]. This is a good example that one can not leave any part of the system unspecified while proposing a new voting scheme as implementation details of one component may harm the desired properties of others.

2 The proposed Belgian remote voting system

The system proposed for Belgium relies on verification codes that have to be recorded by the voter in order to perform the verification later [1, 2, 11]. More precisely, the voter is provided with three sheets (see Figure 1). The selection sheet lists all the candidates together with the preference marking spots. The code sheet presents short codes for both of the options of voting for or against a particular candidate. Finally, the note sheet is meant for the voter to write down the codes corresponding to her selections in order to later check against

the codes published on the bulletin board. As the code sheet provides a receipt of voting, it is meant to be destroyed after the vote has been cast.

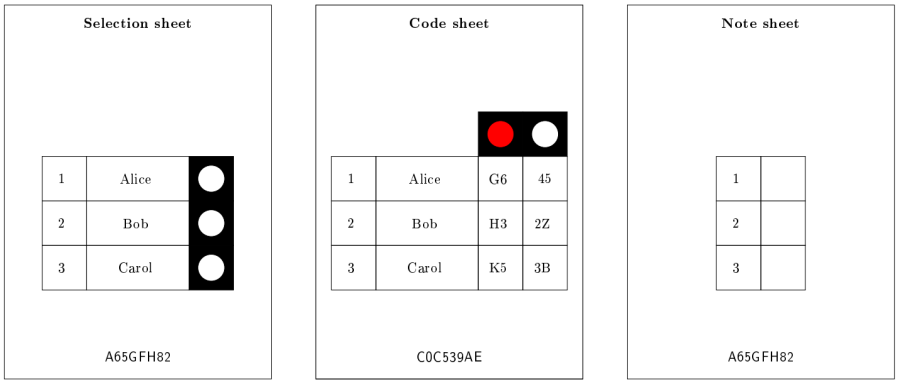

Fig. 1. Ballot, code and note sheet for the proposed Belgian postal voting system [1, 2, 11]

What makes the case of the proposed Belgian system especially interesting is the existence of a well-established national electronic identity (eID) infrastructure. It means that voter authentication can be performed much more reliably, potentially also improving eligibility verification in the case of postal voting.

In the beginning of the process, the voter logs onto the voting server by using her eID. The server checks eligibility and prepares the voting sheets specifically for this voter. Each sheet will carry a random 128-bit voter-specific code k, enabling the tallying authority to authenticate the vote even without relying on an outer, signed envelope. This allows, in principle, to drop the outer envelope altogether, thus potentially increasing postal vote secrecy during the vote transmission.

In Belgium, the selection sheets can be pretty large as they need to accommodate all the candidates. However, the voter can only vote for the candidates of one party. Thus, as a compromise, in case of electronically prepared ballots, it is proposed that the candidates of one party are displayed on one A4 paper, and the voter would need to mail in only the sheet corresponding to the party of her choice.

It has been left unspecified in the system description [1] whether the voter can only print out the sheet she needs for her party of choice, or whether she should print out all the generated sheets. The subtle issue here is keeping the vote secret from the voter's computer. If the voter would choose to print the candidate list of only one party, a malicious device would learn her party preference.

There are a few ways to look at the issue. On one hand, voter's device definitely is one of the easiest-to-attack components in the whole system, especially

when it comes to vote secrecy. Even if the system provides vote integrity verification mechanisms, it is hard to give strong guarantees that the vote has not been leaked from the used digital device. The best known mechanism to achieve such guarantees would be code voting, but it comes with usability trade-offs [19] and we do not consider such systems in this paper.

A usual approach to this problem is not to target vote secrecy at all in remote settings, and aim at a weaker property of coercion resistance instead (see e.g. [18] for an overview of different proposed approaches to achieve it). Since the Belgian system has been presented as the first step of transition towards Internet voting, there will be a moment in the future when the voters will use their computing devices to prepare and cast votes. Thus we argue that leaking one's vote to the computer is a practical trade-off that will need to be accepted at some point anyway.

We note that in the Belgian system as it is described in [1], the voter has to trust her computer also in regards to vote integrity. It is foreseen that the voter can contact the ballot preparation server and check that the code k is a valid one, but it is not guaranteed to be unique. If an attacker is able to compromise several voter devices, he can make these devices to use the same (valid!) k for all the ballots issued through them. This problem would only be noticed in the tallying phase and the system description [1] does not specify what to do in this case. However, there are little alternatives to invalidating all the votes sharing the same k, as the tallying authority can not distinguish the k-sharing-attack from a ballot box stuffing attempt. This efficiently results in disenfranchising all the voters who cast these votes.

We may try to detect multiple verification attempts made to the same code k, but it is unclear what to do in case of successful detection. The voter may legitimately want to verify the code several times from different devices as she does not necessarily trust a single device. Also, most of the voters would probably not bother verifying the code at all, and thus such a detection mechanism would likely be inefficient.

We also note that checking the value of k for validity may pose a usability issue. The system description [1] discusses embedding k on the ballot sheets both in an OCR font and in the form of a QR code, recommending the former to support human readability. In both cases, the voter would need a device capable of scanning the representation of k, which in the current practice means having a smartphone, a tablet computer or alike. In any case the success of scanning depends on the user skills, quality of the camera, lighting conditions, etc.

3 Eligibility assurance with blind signatures

The root of the problem enabling reuse of the values for k is that these values depend neither on the voter, nor the vote. Of course we do not want to print the voter's digital signature on the ballot instead as this would undermine vote secrecy. Luckily, there exists a good alternative available in the form of blind signatures.

Blind signatures were first introduced by Chaum in 1982 in the context of implementing untraceable payment systems [7]. In 1992, Fujioka *et al.* proposed using this primitive to achieve vote-secrecy-preserving authentication of a ballot by blindly signing it with the authority's key [13].

The construction of Fujioka *et al.* is a very generic one, with a number of improvements proposed throughout the years (see e.g. [23] for a good overview on the topic). Blind signatures have been used also in practical e-voting schemes; recently e.g. in Russia [26]. However, their practical applicability to postal voting has been very limited. This can be explained by a diverse set of assumptions that one would need in order for make such a solution to be useful and work.

On one hand, in order to make use of blind signatures, a relatively advanced digital infrastructure is required. The voters need a reliable means for authenticating themselves to the signing authority, accompanied with a method to do something with the returned signature. On the other hand, even though a digital identification infrastructure is assumed, the society should still look to improve remote paper vote casting, rather than going for Internet voting right away.

Both of these aspects are present in Belgium, and hence considering the blind signatures for authenticity and eligibility assurance is interesting in this case.

Of course, we would need to use the voter's computer as a ballot marking device and trust it for vote secrecy. However, as discussed in Section 2, this is a trade-off that is probably required sooner or later anyway.

Thus, we propose setting up a generic blind signature scheme as an addition to the proposed Belgian postal voting system. For that, we will assume the authority A who maintains the list of eligible voters, possesses a public-private blind signature key pair, and publishes the corresponding public key.

After the voter has used her computer to fill in the ballot, it is first masked for blind signing. The voter then authenticates herself to A who verifies her eligibility. If this verification succeeds, A issues the blind signature. Next, the voter's computer removes the blinding and displays the obtained signature directly on the ballot, e.g. as a QR code. The resulting sheet can then be printed out and cast as a regular postal ballot.

Before mailing it off, this scheme allows the voter to check well-formedness of the ballot and the signature of A. First of all, note that the Belgian ballot can be encoded rather efficiently. There are less than 256 parties running, so one byte is enough to encode the party choice. For each candidate of this party, one bit needs to be encoded. Depending on the length of the the party list, one may need a few dozens of bits. Adding the metadata concerning the election event, the encoding should comfortably fit into 256 bits.

This means that we can put the padded encoding of the vote directly under the signature without hashing it. Thus, a mobile verification app can be developed that can decode the whole vote together with A's signature from the QR code, check the signature and display the decoded vote content to the voter. The voter can then visually match the result to what has been printed out on the ballot in the traditional human-readable way. This ensures the voter that the vote has indeed been correctly signed by A without intermediate manipulation.

Machine-readable votes also allow for a more efficient tallying process by scanning the QR codes. It is not even necessary to visually inspect all the postal ballots for correspondence to the human readable part if a proper statistical post-election audit process like risk-limiting audit is implemented. Note that a statistical post-election audit as part of the tallying procedures implicitly also protects the voters who did not bother downloading and using the mobile verification app.

As the ballot is signed with the authority's signature to prove eligibility, there is no need for the outer, voter-identifying envelope, and the ballot can be mailed anonymously. This removes one of the major privacy problems of postal voting that anyone can study the envelopes in transit and reveal how the postal voters voted. At the same time, blind signatures printed on the ballots ensure eligibility of the voters and also protect ballot integrity.

On the other hand, extra measures are then needed at the polling station on the election day. If a person who has cast a postal vote comes to the polling station and wants to cast a vote, a respective mechanism is needed to avoid double voting.

In case of a standard double envelope postal voting system (see e.g. [16]), envelopes can be kept sealed until the regular polling station votes are also cast. Double envelopes belonging to the voters who submitted in-person votes can then be discarded without opening.

In case of anonymously sent postal votes this approach would not work. Instead, the voter needs to be stopped at the polling station before she gets a chance to submit a vote. For that, polling stations workers need access to A's database of voters who have requested signing their postal votes. This is technically non-trivial, but doable. A similar system has been in use in Estonia since 2021 Parliamentary elections to enable cancelling electronic votes with paper ones in a polling station [12].

Note that the problem of double voting is also present in the proposed Belgian system as described in [1], and even on a bit more serious level. In principle, the ballot preparation server can keep a list of the voters who have requested a ballot, but it can not tell if the ballot has actually been completed. If requesting a blank ballot would be registered as the voter having used her voting rights, this may end in disenfranchising the voter e.g. in the case she fails submitting her postal vote and attempts voting in a polling station.

In case of our proposal, the voter only requests the authority's signature *after* having filled the ballot in. Of course, we still do not know whether the signed ballot was actually mailed or not. However, we argue that there is a potential legal difference between just requesting a blank ballot and asking for the authority's confirmation once it has been filled. In the latter case it is easier to call the act of voting completed and rule against the voter in case of a possible dispute between disenfranchisement *vs.* double voting.

Using the voter's computer as a ballot marking device also allows for a more efficient printing procedure. There is no reason to print all the sheets corresponding to the parties the voter did not want to vote for. Of course, this is mainly

a result of our trade-off with secrecy of the vote from the voter's computer. On the other hand, it also gives a significant environmental effect as the number of otherwise unused sheets of paper would be multiplied by the number of postal voters.

Note also that we do not need to print the code sheet at all. Instead, we can directly generate and print the filled note sheet. This is good both from the usability and security points of view. Usability benefits are clear as the voter is not required to copy any random codes by hand. Security benefit comes from the observation that the code sheet is actually a receipt that the voter can use intentionally or under coercion to prove how she voted.

The original system description [1] requires the voter to destroy this sheet, but we argue that relying on such a measure to achieve privacy properties is not a good security design principle. Users can in general only be expected to give a minimal amount of effort to achieve the functional goals, i.e. casting one's vote in our case. If the code sheet remains lying around, it can cause unexpected privacy problems which are better avoided if possible.

4 Discussion

Verifiability properties of standard double envelope postal voting are rather weak. There is typically no Cast as Intended verification, and instead of Counted as Cast there is a weaker property of Counted as Collected [5]. We argue that if such a system would be proposed today, it would not be accepted as not satisfying elementary requirements, especially as postal voting protocols offering better properties are available now [4, 29, 3, 20, 10, 1].

However, eligibility verification remains a challenge for all these proposals, and this problem is inherently related to the available infrastructure. When we want to enable e.g. Cast as Intended verification, we need to enhance the capabilities of the verifier, i.e. the voter. When postal voting was introduced for the soldiers fighting in the U.S. Civil War, there was no way of getting convenient and fast feedback about the fate of the vote [22]. But nowadays we have omnipresent Internet access, enabling such feedback.

A similar situation also occurs for eligibility checking. However, now the primary verification agent is the election organizer who needs to decide whether the vote came from a legitimate voter, and whether it is a double vote or not. The ballot can carry some sort of an identifier (like a social security number), or the outer envelope may carry a signature, but neither of them can be considered a strong form of identification in the third decade of the 21st century.

In order to provide better eligibility verification properties, a respective infrastructure is required. With electronic identity mechanisms being introduced in many countries, this infrastructure is becoming readily available. It is only natural to use it to secure remote voting, both in electronic and mail-in settings.

The most straightforward way of integrating an eID into a remote voting scheme would be signing the vote. In case of electronic voting it is easy to encrypt the vote in order to protect its confidentiality. For postal voting, however, there

is an implicit expectation that the paper representation of the vote should be human-readable. This makes direct signing with voter's eID impossible.

On the other hand, blind signature on an anonymous paper vote is still very much an option. Of course, a corrupt signing authority may attempt to sign the votes for ineligible voters. As a solution, we can require the blind signing requests to be signed by the voters. If in the end of the voting period the number of authority-signed votes in the digital ballot box exceeds the number of voter-signed requests then we know that the authority has cheated. As an alternative, signing authority can be implemented in a distributed manner in order to avoid relying on just one trusted party.

We also note that while the idea of using blind signatures in a remote voting setting is not novel, their application to paper-based voting systems is to the best of our knowledge.

5 Conclusions

Cryptographically-enhanced postal voting is a recent and exciting research area. It has a potential to provide a remote voting solution with better authentication and integrity properties compared to regular postal voting. At the same time, it can also avoid some of the problems with remote electronic vote casting as the main vote carrying medium would still be paper.

In this article we reviewed several recent schemes, concentrating on the system proposed by Belgian researchers as an intermediate step towards Internet voting. It adds end-to-end verification capabilities to the postal votes and can even be used to send the filled ballots in anonymously.

The proposal is very rich in implementation details compared to previous purely academic papers. It is also very realistic in terms of the trade-offs required between usability, verifiability and privacy properties of the system.

However, we were still able to point out several problems in this paper. The biggest issue is the need to trust the voter's computer not to disenfranchise the voter by maliciously re-using the random authentication token k.

In order to mitigate this problem, we proposed implementing a generic blind signature scheme instead of using the random token. It turns out that such a solution also has other benefits; for example it enables easier tallying and vote correctness verification by the voter.

The downside of our proposal is the need to use the voter's PC as a ballot preparation device, hence trusting the device not to breach vote secrecy. However, we argue that this is a reasonable trade-off that will need to be accepted at some point anyway. At the same time we reduce the need for paper printouts. This improves both the environmental footprint and coercion-resistance properties of the scheme.

The Belgian postal voting scheme is still in the early stages of research, and we hope that this paper has made a small contribution towards its future success.

Acknowledgments

The paper has been supported by the Estonian Research Council under the grant number PRG920.

References

1. Étude sur la possibilité d'introduire le vote Internet en Belgique (2021), https://elections.fgov.be/informations-generales/etude-sur-la-possibilite-dintroduire-le-vote-internet-en-belgique
2. Abeels, T.: Postal Voting. Master's thesis, Ecole polytechnique de Louvain, Université catholique de Louvain, (2021), http://hdl.handle.net/2078.1/thesis:33143
3. Benaloh, J.: STROBE-Voting: Send Two, Receive One Ballot Encoding. In: E-Vote-ID 2021, Proceedings. LNCS, vol. 12900, pp. 33–46. Springer (2021)
4. Benaloh, J., Ryan, P.Y.A., Teague, V.: Verifiable postal voting. In: Security Protocols XXI - 21st International Workshop, Cambridge, UK, March 19-20, 2013, Revised Selected Papers. LNCS, vol. 8263, pp. 54–65. Springer (2013)
5. Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y.A., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public Evidence from Secret Ballots. In: E-Vote-ID 2017, Proceedings. LNCS, vol. 10615, pp. 84–109. Springer (2017). https://doi.org/10.1007/978-3-319-68687-5_6
6. Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D., Walter, J.: An Analysis of the Security and Privacy Issues of the Neovote Online Voting System. In: E-Vote-ID 2022, Proceedings. LNCS, vol. 13553, pp. 1–18. Springer (2022). https://doi.org/10.1007/978-3-031-15911-4_1
7. Chaum, D.: Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) CRYPTO '82. pp. 199–203. Plenum Press, New York (1982). https://doi.org/10.1007/978-1-4757-0602-4_18
8. Conway, A., Teague, V.: iVote Issues: Assessment of potential impacts on the 2021 NSW local government elections. In: Proceedings of E-Vote-ID 2022. pp. 42–52 (2022)
9. Cotti, C., Engelhardt, B., Foster, J., Nesson, E., Niekamp, P.: The relationship between in-person voting and COVID-19: Evidence from the Wisconsin primary. Contemporary economic policy **39**(4), 760–777 (2021)
10. Crimmins, B.L., Rhea, M., Halderman, J.A.: Remotevote and SAFE vote: Towards usable end-to-end verification for vote-by-mail. In: FC 2022 International Workshops - CoDecFin, DeFi, Voting, Revised Selected Papers. LNCS, vol. 13412, pp. 391–406. Springer (2022). https://doi.org/10.1007/978-3-031-32415-4_27
11. Devillez, H.: Secure postal voting. In: Proceedings of E-Vote-ID 2022. pp. 140–143 (2022), https://dspace.ut.ee/handle/10062/84432
12. Ehin, P., Solvak, M., Willemson, J., Vinkel, P.: Internet voting in Estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly **39**(4), 101718 (2022). https://doi.org/https://doi.org/10.1016/j.giq.2022.101718
13. Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Proceedings. LNCS, vol. 718, pp. 244–251. Springer (1992). https://doi.org/10.1007/3-540-57220-1_66

14. Haines, T., Pereira, O., Teague, V.: Running the Race: A Swiss Voting Story. In: E-Vote-ID 2022, Proceedings. LNCS, vol. 13553, pp. 53–69. Springer (2022). https://doi.org/10.1007/978-3-031-15911-4_4
15. Halderman, J.A.: Practical attacks on real-world e-voting. In: Real-World Electronic Voting, pp. 159–186. Auerbach Publications (2016)
16. Killer, C., Stiller, B.: The Swiss Postal Voting Process and Its System and Security Analysis. In: E-Vote-ID 2019, Proceedings. LNCS, vol. 11759, pp. 134–149. Springer (2019). https://doi.org/10.1007/978-3-030-30625-0_9
17. Krimmer, R., Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In: EGOV 2005. Schriftenreihe Informatik, vol. 13, pp. 225–232. Universitätsverlag Rudolf Trauner, Linz, Austria (2005)
18. Krips, K., Willemson, J.: On Practical Aspects of Coercion-Resistant Remote Voting Systems. In: E-Vote-ID 2019, Proceedings. LNCS, vol. 11759, pp. 216–232. Springer (2019). https://doi.org/10.1007/978-3-030-30625-0_14
19. Marky, K., Schmitz, M., Lange, F., Mühlhäuser, M.: Usability of Code Voting Modalities. In: Conference on Human Factors in Computing Systems, CHI 2019. ACM (2019). https://doi.org/10.1145/3290607.3312971
20. McMurtry, E., Boyen, X., Culnane, C., Gjøsteen, K., Haines, T., Teague, V.: Towards Verifiable Remote Voting with Paper Assurance (2021). https://doi.org/10.48550/ARXIV.2111.04210
21. Park, S., Specter, M., Narula, N., Rivest, R.L.: Going from bad to worse: from internet voting to blockchain voting. Journal of Cybersecurity **7**(1), 1–15 (2021)
22. Rotondi, J.P.: Vote-by-mail programs date back to the civil war (2020), `https://www.history.com/news/vote-by-mail-soldiers-war`
23. Schmid, M., Grünert, A.: Blind Signatures and Blind Signature E-Voting Protocols (2008), University of Applied Science Biel, Switzerland, `https://www.e-voting-cc.ch/images/pdf/blindsignatures.pdf`
24. Simons, B.: Why Internet Voting is Dangerous. Geo. L. Tech. Rev. **4**, 543–563 (2019)
25. Stenerud, I.S.G., Bull, C.: When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting. In: EVOTE 2012. LNI, vol. P-205, pp. 21–33. GI (2012), `https://dl.gi.de/20.500.12116/18219`
26. Vakarjuk, J., Snetkov, N., Willemson, J.: Russian Federal Remote E-voting Scheme of 2021 – Protocol Description and Analysis. In: EICC 2022. pp. 29–35. ACM (2022). https://doi.org/10.1145/3528580.3528586
27. Willemson, J.: Bits or paper: Which should get to carry your vote? J. Inf. Secur. Appl. **38**, 124–131 (2018). https://doi.org/10.1016/j.jisa.2017.11.007
28. Willemson, J.: Analyzing and Improving Eligibility Verifiability of the Proposed Belgian Remote Voting System. CoRR **abs/2305.09411** (2023). https://doi.org/10.48550/arXiv.2305.09411
29. Zagórski, F., Carback, R., Chaum, D., Clark, J., Essex, A., Vora, P.L.: Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. In: ACNS 2013, Proceedings. LNCS, vol. 7954, pp. 441–457. Springer (2013). https://doi.org/10.1007/978-3-642-38980-1_28