Coercion-Resistant Hybrid Voting Systems

Abstract

This paper proposes hybrid voting systems as a solution for the vote buying and voter coercion problem of electronic voting systems. The key idea is to allow voters to revoke and overrule their electronic votes at the polling station. We analyze the potential and pitfalls of such revocation procedures and give concrete recommendations on how to build a hybrid system offering coercion-resistance based on this feature. Our solution may be of interest to governments which aim at integrating paper-based and electronic voting systems rather than replacing the former by the latter.

1 Introduction

In consideration of the complexity and manyfold vulnerabilities of today's computers and networks, most governments pursue a cautious strategy in introducing electronic means into processes that are so fundamental for running their democracy. Their reservation is particularly distinctive if the technology involves components that are not under their control. The number of countries experimenting with electronic voting over the Internet is therefore still marginal. Estonia and Switzerland, two of the few pioneering countries in Internet elections and referendums (we shall use the general term *voting*), follow the strategy to slowly increase the number of electronic votes over the years [Die02]. The idea behind keeping this shift at a slow pace is to limit the risk and consequences of fraud in the early stage of the respective project. The legitimacy of such concerns has been demonstrated by the negative e-voting experience in the Netherlands, where all nationwide e-voting activities have been stopped in 2007, after the vulnerability of the deployed system had been exposed in public [Loe08]. In the foreseeable future, traditional and electronic voting systems are therefore expected to live side by side for quite some time.

Running two or more different voting systems in parallel requires some care. For example, it must be excluded that voters manage to cast more than one vote, for instance one in each subsystem. The respective systems in Estonia and Switzerland have their own mechanisms to avoid this. The Swiss Canton and Republic of Geneva, for example, issues a voting card that contains a scratch-off panel with a hidden PIN to access the electronic system [CWS06]. Voters that

know their PIN can cast their vote electronically. However, a voter needs to show an untouched scratch-off panel to get access to the ballot-box or voting booth at the polling-station.

Another problem of running more than one voting system in parallel is the fact that the overall voting system is at most as secure as each of its subsystems. If we consider traditional paper-based systems as almost perfectly secure, the security of the overall voting system is directly determined by the security of its electronic subsystem. Every possible weakness of the electronic system automatically poses a security threat to the overall voting system. If for instance the electronic system issues a receipt to the voters that allows them to prove a coercer or vote-buyer how they voted, the overall voting system is subject to fraud. Indeed, *receipt-freeness* and *coercion-resistance* are two of the most difficult properties to achieve in electronic voting systems [BT94, JCJ05, DKR06].

In this paper, we introduce the concept of a *hybrid voting system*, which is more than just running a traditional paper-based and an electronic voting system in parallel. The idea is to exploit the properties of the paper-based voting infrastructure to overturn the weaknesses of the electronic system. In particular, we suggest a *vote revocation* mechanism, which allows voters to overrule their electronic votes by casting an additional paper vote at the polling station. The idea is thus similar to the "re-voting" feature of the Estonian Internet voting system, in which voters can to cast multiple votes electronically, but such that only the last vote is taken into account [MM06]. The principle and possible benefits of counting only the "last ballot" has first been mentioned in [Skr02]. It is our proposed counter-measure against the vote buying and voter coercion problem, which is difficult to avoid in pure e-voting systems.

To motivate and define our concept of a hybrid voting system, we start in Section 2 with a general discussion of the vote buying and voter coercion problem in electronic voting systems. Then we present our understanding of a hybrid voting system and explain why they offer coercion-resistance. In Section 3, we give concrete recommendations of how to build a hybrid system with the vote revocation feature. To make our analysis as generic as possible, we first develop a classification of different e-voting systems by looking at the properties of the underlying electronic ballot-boxes. We will argue that a hybrid system that prevents vote buying and voter coercion can always be constructed, if the enclosed electronic voting system guarantees that each voter can unambiguously identify his vote in the electronic ballot-box. In Section 4, we summarize the main conclusions of our analysis and refer to some of the open problems.

2 Hybrid Voting Systems

New voting mechanisms will not find acceptance unless they evidently preserve the security level of traditional paper-based voting. This requirement is inherently difficult to fulfill with e-voting systems, and it seems that it is not fulfilled

to a satisfactory degree by many of the proposed models or existing systems. Two serious types of fraud that are particularly difficult to prevent and which are largely scalable in electronic systems are *vote buying* and *voter coercion*. In the first part of this section, we describe the challenge of building trustworthy e-voting systems that inherently prevent such types of fraud. Then we show how hybrid voting systems may offer voters a means of voting electronically while keeping the possibilities of such types of fraud as scarce as in traditional paper-based systems.

2.1 Vote Buying and Voter Coercion

Whether or not a system has actually implemented required security features is not necessarily transparent to the voters. If they feel that their votes may not even reach the final tally, they might fully restrain from voting electronically and tend to cast their votes in the traditional way, a means of casting votes still likely to be available in the near future. By doing so, they witness the vote reaching the body of the possibly transparent ballot-box. Some countries even allow voters to attend the tallying procedure and thus to witness the consideration of their votes in the final outcome. To establish a similar level of voters' trust in e-voting systems, it is imperative to give them access to some information that confirms the correct casting of their votes in a convincing way. This confirmation is meant to provide *individual verifiability*, a precondition to trustworthiness of voting systems. The existence of such a confirmation may thus seem like a feature, but since it will generally also convince any third party that a particular vote was cast, it disallows voters to deceive others about their votes. Such information is thus called a voter's *receipt* [BT94]. Its existence is a violation of the voter's privacy, because it opens doors to the following two types of fraud, in which the adversary gets the voter to vote in a prescribed way [Skr02].

Vote Buying. The voter will be rewarded by the *vote buyer* for voting in a particular manner. To receive the reward, the voter may actively co-operate with the vote buyer, e.g. by deviating from the normal voting procedure to construct a receipt.

Voter Coercion. The voter is put under pressure or threatened by a *coercer* for voting in a particular manner. Here, the voter may only consent to co-operate with the vote buyer as long as the threat is perceived as real.

Note that both forms of exploiting a voting system are largely scalable in an electronic environment. A vote buyer could simply set up a web site explaining the conditions for making easy money, while a coercer could easily post his threats to thousands of voters. In both cases, the attack is only interesting to potential adversaries as long as voters are able to prove them how they voted. Without a receipt, a corrupted voter could simply lie about the vote cast, i.e., the motivation of an adversary even launching such an attack in the first place is likely to be as low as with paper-based votes.

Clearly, it must be a primary objective to establish an e-voting system that is immune to all sorts of vote buying and voter coercion attacks, including those in which the adversary gets the voter to abstain from voting or to vote at random. Systems blessed with that immunity are called *coercion-resistant* [JCJ05, DKR06]. Note that coercion-resistance is stronger than mere *receipt-freeness* [BT94, JV06], which alone does not prevent adversaries from getting voters to abstain from voting. In the literature, there are many suggestions for receipt-free or coercion-resistant systems, but most of them rely on unrealistic technical assumptions such as untappable communication channels [BT94, Oka97, HS00, MBC01, LBD+03, DKR06, XS06, MN06, CLW08].

2.2 Hybrid Systems

A hybrid voting system offers every voter the choice between either casting a vote electronically or casting a traditional paper vote at the polling station. The key to undermining the possibility of exploiting the electronic subsystem for the above-mentioned types of fraud is to allow the voters to revoke their electronic votes at the polling station. Revocation can be followed by casting the vote of personal choice in the traditional way, i.e., inside the (presumably) coercion-free environment of the polling station. Clearly, the revocation mechanism must be designed in a way that an adversary can not find out which votes have been revoked. In Section 3, we will propose two different solutions to that problem. Both solutions include three different ballot-boxes: the α-*box* for the electronic votes, the β-*box* for the vote revocations, and the γ-*box* for the paper votes. The final outcome Σ of the voting can then be calculated as

$$\Sigma = \alpha - \beta + \gamma,$$

where α, β, γ denote the individual results of the respective ballot-boxes.[1] This model with three ballot-boxes is illustrated in Figure 1. Depending on the revocation mechanism, the β-box may contain revocations either in electronic form or on paper. Clearly, each vote in the β-box must reflect the corresponding vote from the α-box.

Coercion-Resistance. In a hybrid system with a vote revocation procedure, even if an adversary is contently convinced that the voter cast the electronic vote as told, there is still the possibility that the vote will be overruled by the voter's personal choice and thus not be considered in the final tally. Only by witnessing the voter entering the polling station, it becomes apparent to the coercer that the voter's intention is most likely to revoke the vote. However, monitoring the entrance of a polling station is not easily scalable to a large number of corrupted voters. Furthermore, since the possibility of hindering voters from going to the

[1] We do not further specify here whether the ballot-boxes contain simple yes/no-votes or more complicated 1-out-of-n or k-out-of-n selections. In the latter cases, $\Sigma = \alpha - \beta + \gamma$ must be applied component-wise to each of the n options.

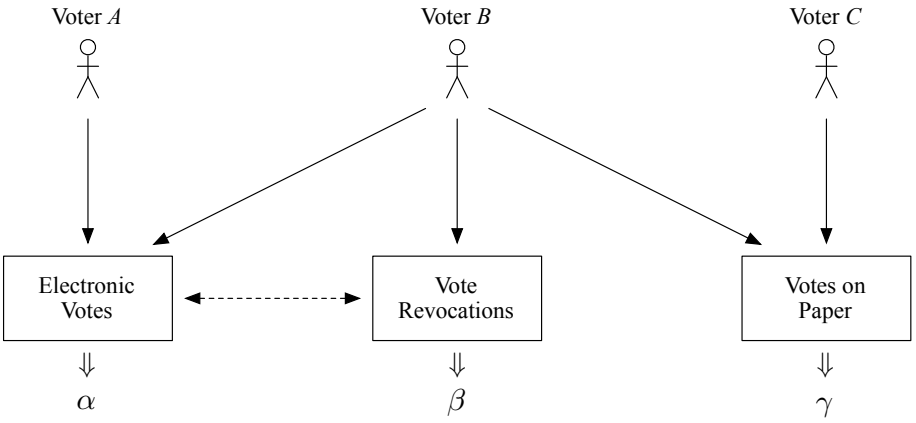

Figure 1: Three types of ballot-boxes and voters in a hybrid voting system: Voter A votes electronically; Voter B first votes electronically, but then overrules it by a paper vote; Voter C votes on paper.

polling station is also given in traditional, well-accepted paper-based systems, it does not prevent hybrid systems from reaching the same level of coercion-resistance as their traditional counterparts.

We conclude that if adversaries must assume that corrupted voters will usually revoke their votes, a hybrid system is clearly coercion-resistant: an attack would simply seem too expensive. We believe that it is possible for governments to invoke that perception among adversaries, for instance by explicitly allowing voters to co-operate with vote buyers and coercers, however only as long as they revoke their biased vote.

Prerequisites. Remarkably, pure electronic voting systems and the electronic subsystems of hybrid voting systems do not necessarily share the same prerequisites. For example, the great challenge of removing receipts from pure e-voting systems does no longer apply to the electronic components of a hybrid voting system. Not that receipts are only admitted, their guaranteed presence may even be a prerequisite in the design of a hybrid system. One of the proposed methods in Section 3 requires such *guaranteed receipts*. In general, we are less restrictive by imposing the following two key prerequisites for the e-voting component of a hybrid voting system.

1. The system guarantees the presence of a *vote identifier*, to ensure that the voters can identify the votes in the α-box that were generated using their credentials. Receipts are special cases of such vote identifiers.
2. The system provides some mechanism that allows voting officials at the polling station to check whether or not a registered voter has already cast an electronic vote.

Note that in general the guaranteed existence of a vote identifier (1st prerequisite) is insufficient for the voting officials to verify whether someone has cast an electronic vote or not (2nd prerequisite). Because if such an identifier is secret to the voter, then the existence of the electronic vote could be concealed by simply withholding the identifier. Similarly, the existence of a mechanism to check if somebody has already voted electronically (2nd prerequisite) is in general not enough to identify that person's vote in the α-box (1st prerequisite), because the system may provide a list of voters that is completely disconnected from the list of votes.

In the absence of a receipt, the first prerequisite can be met by leaving the encrypted vote attached to information that publicly identifies the voter. In order to preserve the voters' privacy, the individual votes clearly may never be decrypted in this case, not even at the time of tallying. Instead, homomorphic methods for tallying exist, where only the result of the tally needs to be decrypted [CGS97, HS00]. By applying this method, even the second requirement is inherently met. We thus conclude that the prerequisites we impose on the electronic subsystem of a hybrid system do not form obstacles that are particularly hard to overcome.

3 Vote Revocations in Hybrid Systems

We now consider construction of a coercion-resistant hybrid voting system. To prevent vote buying and voter coercion, we need to define a secure vote revocation mechanism that allows voters to update their electronic votes at the polling station. For the solution presented in this section, we assume that the electronic subsystem provides the two key prerequisites discussed at the end of the previous section. We assume thus the existence of an electronic ballot-box, in which the electronic votes are collected (the α-box). Additionally, we suppose that the traditional voting infrastructure satisfies the following three minimal requirements.

1. The traditional voting infrastructure consists of a polling station, where the paper votes of registered voters are anonymously collected in a physical ballot-box (the γ-box).
2. The traditional voting procedure at the polling station (checking the identity of voters, opening the ballot-box, counting the votes, etc.) is sufficiently secure, in particular coercion-resistant, and the group of voting officials is reliable and trustworthy.
3. The official voting period at the polling station chronologically succeeds the electronic voting period.

To understand the applicability of the proposed vote revocation procedures, we first need to get an overview of the different types of electronic ballot-boxes in e-

voting systems. The result of this discussion in Subsection 3.1 is a classification of e-voting systems, from which two fundamentally different situations emerge. For each of these cases, we propose in Subsection 3.2 a corresponding vote revocation procedure that fits into the proposed counting scheme of a hybrid system.

3.1 Classification of E-Voting Systems

A common core component of all existing e-voting systems is an *electronic ballot-box*, in which votes are collected during the voting period. One can think of it as a database with two basic operations for adding new entries and reading its content. To ensure the availability and the correctness of these operations, and to guarantee the integrity and consistency of the database, a variety of security measures need to be implemented. Some of these measures aim at avoiding so-called single points of failure, i.e., critical components capable of causing the entire system to fail.

Depending on the chosen configuration and properties of the electronic ballot-box and the structure of its entries, different e-voting systems emerge. In the remainder of this subsection, we will make a distinction between black box and bulletin board systems, anonymous and non-anonymous boards, identifiable and non-identifiable board entries, and the presence or absence of a receipt. In Figure 2, we give a first overview of this classification and indicate where vote revocations are possible.

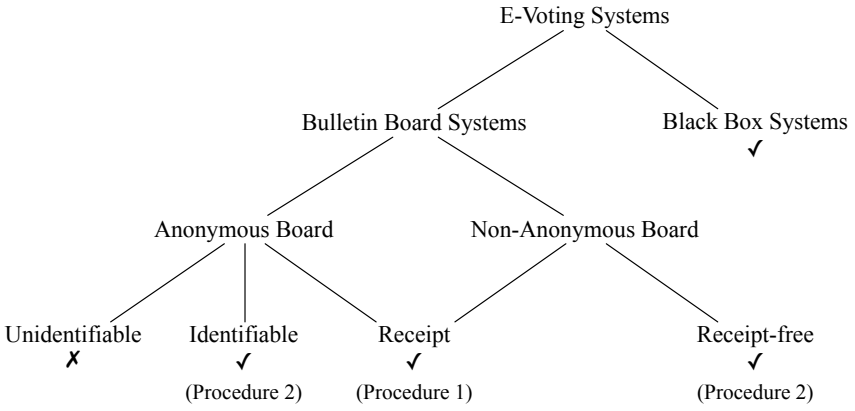

Figure 2: Classification of existing e-voting systems with different types of electronic ballot-boxes. The check marks indicate where vote revocations are possible.

Black Box vs. Bulletin Board Systems. E-voting systems mainly differ in the type of database access they provide. There are two extreme cases, one

in which the access is restricted to a few authorized persons only, and one in which everybody can add new entries to the database and read its content (while deleting entries is always prohibited). E-voting systems of the first category are sometimes called *black box voting systems* [HA03, KKW06]. They are very popular in commercial solutions and in political e-voting projects. An advantage of black box systems is that from a cryptographic point of view, they are relatively simple to understand and implement. On the other hand, they are often criticized as not providing enough transparency, i.e., neither providing individual verifiability, nor allowing the outcome to be publicly verified.

The second major category comprises systems with a public *bulletin board*, through which all cast votes are visible to everybody [Pet05]. To ensure the secrecy of the votes and the fairness of the voting process, the board's entries need to be encrypted (at least during the official voting period). The purpose of the public board is to allow all voters to verify the inclusion of their votes in the electronic ballot-box and the correctness of the counting. Most system proposals in the academic e-voting literature are based on such bulletin boards.

Anonymous vs. Non-Anonymuous Boards. In bulletin board systems, there are two opposed sub-categories, each defined by whether the entries on the board are anonymous or not. In the case of anonymous boards, there must be an additional mechanism to exclude votes from unauthorized voters or multiple votes from the same voter. Examples of such mechanisms are *mix nets* [Cha81] or *blind signatures* [Cha82]. If the board entries are not anonymous, for example if they contain a unique voter ID that attributes them unambiguously to the respective voters, there must be a mechanism that prevents the decryption of single votes. Systems of that type are usually based on *homomorphic encryption schemes* with a shared public key [CGS97, HS00]. Clearly, in those systems, the publicly known voter ID serves as the vote identifier.

Vote Identifiers vs. Receipts. Another distinguishing feature of bulletin board systems concerns the board entries themselves. There are three basic types: those which can be identified and disclosed with a receipt, those which can only be identified with a vote identifier (but not disclosed), and those which are completely unidentifiable. In the case of a non-anonymous board, where the identification of the votes is given intrinsically, only two types of board entries remain, those with a receipt and those without. These cases are depicted at the bottom of the tree shown in Figure 2.

3.2 Vote Revocation

In the classification tree of the previous subsection, four cases are tagged with a check mark and one is crossed out. The cross means that the case of an anonymous board with unidentifiable board entries is not compatible with any vote revocation procedure. The missing vote identifier makes it impossible to

either remove the vote from the electronic ballot-box or to subtract it from the final tally. Note that by explicitly requiring the existence of vote identifiers at the end of Section 3, we have ruled out this case from the beginning.

In black box systems, it is possible to install a vote revocation mechanism as long as the electronic votes in the ballot-box remain identifiable. Due to the lack of transparency offered by such systems, the correct application of a potential revocation mechanism can not be verified by the public. We therefore leave revocations using a black box approach undiscussed.

Procedure 1: Revocations on Paper. The first procedure we propose assumes that every voter owns a receipt for his vote in the α-box. It does not matter whether the board is anonymous or not, but it is crucial that the voter (and not the coercer or vote buyer alone) is in possession of the receipt. The payoff of this restriction is a revocation procedure that particularly appeals by its simplicity.

The following points define the procedure. We start off when the voter at the polling station is about to revoke the electronic vote in the α-box (we assume that the voting officials have already successfully checked the voter's identity and right to vote).

1. The voter uses the receipt to locate the encrpyted vote in the α-box and reveal it towards the voting officials.
2. The voting officials prepare a revocation paper ballot containing the same vote and hand it over to the voter.
3. The voting officials verifiy that the voter drops the revocation paper ballot into the β-box.
4. The voter is granted access to the γ-box to cast the final paper vote.

In this procedure, the β-box is thus a physical ballot-box similar to the γ-box. At the end of the official voting period, it is opened and tallied according to the same procedure.

Note that in the scheme as it is proposed, it is crucial to assume that the voting officials will not allow the voters to cast a paper ballot that differs from their electronic votes in the α-box. If not all voting officials are fully trustworthy, then several voting officials should be involved in each step of the procedure. In other words, before the voter gets access to the γ-box, a sufficient number of voting officials would have to give their approval, for instance by signing the revocation ballot. Thus, we merely need to assume that among the group of involved voting officials, there is at least one that would refuse the signature to an incorrect revocation ballot.

A drawback of this procedure is the fact that the content of the electronic vote must be revealed to the voting officials. One could argue that this violates the

anonymity of the vote, because in a simple yes/no-type of voting, one could guess that revoking a yes-vote implies that the update will be a no-vote, and vice versa. But since such conclusions will always remain speculative, i.e. it can not be excluded that the original and the updated votes are identical, we think that this is an unpleasant but acceptable side effect.

Note, that by requiring instead of avoiding a receipt, we sharply depart from the mainstream approach of taking additional measures to make electronic voting systems receipt-free. Yet, the following procedure shows how vote revocations can be realized even without receipts.

Procedure 2: Electronic Revocations. Let the e-voting component of the hybrid system now be a system that provides a mere vote identifier, not necessarily a receipt. The idea then is to leave the votes encrypted throughout the whole revocation procedure. To guarantee to anonymity of the those who decide to revoke their votes, and thus to ensure the overall system to remain coercion-resistant, we define the β-box as an anonymous bulletin board onto which re-encryptions of the original votes are posted. The adversary is then unable to make out which votes from the α-box have been revoked. The electronic voting environment must therefore comply with the following requirements.

- The β-box must be an anonymous bulletin board.
- The encryption scheme used to generate the encrypted votes in the α-box must allow re-encryption[2] and the generation of a non-transferable proof of correct re-encryption.[3]

The following points define the procedure.

1. The voter generates a re-encryption of the encrypted vote in the α-box.
2. A corresponding non-transferable proof of correct re-encryption is generated, designated to the voting officials at the polling station. Optionally, this step can be done remotely in a non-interactive manner, given the existence of trusted software.
3. The voter approaches the voting officials and uses the vote identifier to identify the encrypted vote in the α-box.

[2] Let $w = E(v, r)$ be the encrypted vote, where E is a randomized encryption function with randomization factor r. Then $w' = R(w, r')$ denotes the re-encryption of w, such that the decryptions of w and w' are identical, i.e., $v = D(w) = D(w')$.

[3] A proof of correct re-encryption allows a prover to convince a verifier that w' is indeed a re-encryption $R(w, r')$ of w, without revealing the randomization factor r'. A proof constructed as an *interactive* Σ-*protocol* is inherently non-transferable, i.e., only the involved verifier will be convinced of its correctness [BG92]. Corresponding non-interactive protocols are transferable, but there is a general way of extending them to be convincing to a designated verifier only [JSI96].

4. The voter hands the re-encryption and the corresponding non-transferable proof over the voting officials.

5. If the proof is accepted, the voting officials post the re-encrypted vote to the β-box.

6. The voter is granted access to the γ-box to cast the final paper vote.

The β-box is tallied according to the procedure defined for the α-box.

Similar to the previous procedure, we can enhance it by requiring a sufficient number of voting officials to approve the voter's re-encryption: A voter would only be granted access to the γ-box once a sufficient number of voting officials have posted their electronic signature of the re-encryption to the bulletin board.

Clearly, the randomization factor the voter used for his re-encryption serves him as a receipt; He can always prove to an adversary that he has revoked his electronic vote. However, he will never be interested in doing so. On the other hand, the receipt does not help at proving to an adversary that he did *not* revoke his vote. It thus does not reduce the security level of the overall system.

4 Conclusion

Governments around the world intend to offer their citizens e-voting as a comfortable way to express their political preferences. Yet, it seems that the traditional paper-based schemes are not likely to disappear for quite some decades. Defining procedures to intergrate both means of casting votes to an overall voting system clearly poses an inherent necessity. We propose our understanding of hybrid voting systems as a solution to this challenge. By introducing the anonymous β-box and by exploiting the traditional polling station as a protective environment, we allow voters to revoke their electronically casted votes. We argue why such an approach yields coercion-resistance, even if the electronic subsystem were indeed subject to coercion when disallowing revocation at the polling station. In a hybrid system, we are therefore given the freedom to have the e-voting subsystem grant receipts to satisfy individual verifiability, without introducing the risk of vote buying or voter coercion. Thus, hybrid voting systems offer voters trustworthy, coercion-resistant e-voting.

References

[BG92] M. Bellare and O. Goldreich. On defining proofs of knowledge. In E. F. Brickell, editor, *CRYPTO'92, 12th Annual International Cryptology Conference on Advances in Cryptology*, LNCS 740, pages 390–420, Santa Barbara, USA, 1992.

[BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In *STOC'94, 26th Annual ACM Symposium on Theory of Computing*, pages 544–553, Montréal, Canada, 1994.

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. *European Transactions on Telecommunications*, 8(5):481–490, 1997.

[Cha81] D. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[Cha82] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO'82, 2nd International Cryptology Conference*, pages 199–203, Santa Barbara, USA, 1982.

[CLW08] S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In *NDSS'08, 15th Network and Distributed System Security Symposium*, pages 81–94, San Diego, USA, 2008.

[CWS06] M. Chevallier, M. Warynski, and A. Sandoz. Success factors of Geneva's e-voting system. *Electronic Journal of e-Government*, 4(2), 2006.

[Die02] Die Bundesbehörden der Schweizerischen Eidgenossenschaft. Bericht über den vote électronique: Chancen, risiken und machbarkeit elektronischer ausübung politischer rechte. *Bundesblatt*, 154(5):645–700, 2002.

[DKR06] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *CSFW'06: 19th IEEE workshop on Computer Security Foundations*, pages 28–42, Venice, Italy, 2006.

[HA03] B. Harris and D. Allen. *Black Box Voting: Ballot Tampering in the 21st Century*. Plan Nine Publishing, 2003.

[HS00] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, *EUROCRYPT'00, International Conference on the Theory and Applications of Cryptographic Techniques*, LNCS 1807, pages 539–556, Bruges, Belgium, 2000.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In V. Atluri, S. De Capitani di Vimercati, and R. Dingledine, editors, *WPES'05, 4th ACM Workshop on Privacy in the Electronic Society*, pages 61–70, Alexandria, USA, 2005.

[JSI96] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In U. Maurer, editor, *EUROCRYPT'96, International Conference on the Theory and Application of Cryptographic Techniques*, LNCS 1070, pages 143–154, Saragossa, Spain, 1996.

[JV06] H. L. Jonker and E. P. Vink. Formalizing receipt-freeness. In *ISC'06, 9th Information Security Conference*, LNCS 4176, pages 476–488, Samos, Greece, 2006.

[KKW06] A. Kiayias, M. Korman, and D. Walluck. An internet voting system supporting user privacy. In *ACSAC'06, 22nd Annual Computer Security Applications Conference*, pages 165–174, Miami Beach, USA, 2006.

[LBD+03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, *ICISC'03, 6th International Conference on Information Security and Cryptology*, LNCS 2971, pages 245–258, Seoul, Korea, 2003.

[Loe08] L. Loeber. E-voting in the Netherlands: from general acceptance to general doubt in two years. In R. Krimmer and R. Grimm, editors, *3nd International Workshop on Electronic Voting*, Lecture Notes in Informatics, pages 21–30, Bregenz, Austria, 2008. Gesellschaft für Informatik E.V.

[MBC01] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In B. Schmid, K. Stanoevska-Slabeva, and V. Tschammer, editors, *I3E'01, 1st IFIP Conference on towards the E-Society*, volume 202, pages 683–694, 2001.

[MM06] Ü. Madise and T. Martens. E-voting in Estonia 2005: The first practice of country-wide binding internet voting in the world. In R. Krimmer, editor, *2nd International Workshop on Electronic Voting*, number P-86 in Lecture Notes in Informatics, pages 15–26, Bregenz, Austria, 2006. Gesellschaft für Informatik E.V.

[MN06] T. Moran and M. Naor. Receipt-free universally-verifiable voting with everlasting privacy. In C. Dwork, editor, *CRYPTO'06, 26th Annual International Cryptology Conference on Advances in Cryptology*, LNCS 4117, pages 373–392, Santa Barbara, USA, 2006.

[Oka97] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, *5th International Security Protocols Workshop*, LNCS 1361, pages 25–35, Paris, France, 1997.

[Pet05] R. A. Peters. A secure bulletin board. Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, The Netherlands, 2005.

[Skr02] J. Skripsky. Minimal models for receipt-free voting. Semester project, ETH Zürich, 2002.

[XS06] Z. Xia and S. Schneider. A new receipt-free e-voting scheme based on blind signature. In *WOTE'06, IAVoSS Workshop on Trustworthy Elections*, pages 127–135, Cambridge, U.K., 2006.