Administrative and Public Verifiability: Can We Have Both?

Josh Benaloh
Microsoft Research

June 30, 2008

Abstract

Administrative verifiability gives election officials the means to protect against certain kinds of errors and fraud. This is typically accomplished with tools like paper audit trails that enable manual recounts and spot checks. Public verifiability uses cryptographic and related tools to enable any member of the public to independently fully verify the accuracy of an election tally. Although public verifiability is technically a higher standard, its complexity makes it unappealing for many. This raises the question of whether it is possible to achieve public verifiability without sacrificing the traditional administrative verifiability tools in common use.

This paper introduces*verified optical scan* — a simple design wherein both administrative and public verifiability are possible and the two are tightly linked to achieve consistent results.

1 Introduction

Accurate tallies are crucial to the electoral process, but they are effectively impossible to ensure. In virtually every election scenario, there exists various sets of actors who can prevent an election from concluding with an accurate tally. In lieu of guaranteed accuracy, we generally substitute some flavor of verifiability. We add checks and balances and perform audits to detect irregularities, identify bad actors, and correct errors when possible. In this way, we add a measure of verifiability to obtain some confidence that if there is malfeasance, we will know it. The questions then revolve around what assumptions are made on the verification, what can be verified, and what sets of actors can circumvent verification.

Traditional verification is based predominantly upon redundancy. Paper ballots are handled only in the presence of multiple witnesses and can be independently recounted. Election equipment is produced by vendors and then certified by independent testing labs. These are examples of what can be called *administrative verifiability* in which the verification capability is enjoyed by officially designated entities and provides protection against many errors as well as most corruption by individuals. In contrast, *public verifiability* enables any individual to verify the accuracy of a tally — regardless of any conspiracies of any size.

In the abstract, public verifiability is a stronger property than administrative verifiability. Not only does public verifiability extend auditing capabilities beyond those few appointed by election administrators, but it also resists malfeasance by coalitions who are supposed to be checking each other. In practice, however, the known techniques that enable public verification are not entirely satisfactory: although they can detect errors and fraud, they usually can do little to correct them; they are often subject to massive denial of service attacks; in most cases they rely upon cryptographic assumptions which, if breeched, could lead to widespread compromise of voter privacy; and they use methodologies which are not well understood, and therefore generally not well trusted, by the public. For these reasons, it is desirable to not forgo the benefits of administrative verifiability which is generally better understood and can, in at least some cases, correct errors and resist widespread attacks.

A natural question is whether administrative and public verifiability can be obtained simultaneously. This would provide the reliability and understandability benefits of common election methods while providing the added accuracy and confidence that can come from public verification techniques. The one detraction of existing publicly verifiable schemes that cannot be mitigated by a pairing with a traditional scheme is the potential risk of a massive privacy compromise, but the cryptographic techniques that would be used here are well established and used in many other scenarios such as the world banking system; and the consequences of a financial system collapse could be argued to be worse than those entailed by loss of voter privacy. (Note that with many of the available cryptographic tallying systems, even the worst case scenario of a complete compromise of the cryptosystem would *not* compromise the accuracy of an election — only the privacy of the votes.)

The principal problem of creating a hybrid system is synchronization. If an election produces an administrative outcome that does not match the publicly-verified outcome, then confidence will be shaken and little good will be served. For these reasons, a simple parallel system in which two sets of votes are cast without any effort to maintain synchronization is undesirable. Instead, a single system offering both administrative tools with good failure recovery and the capability of public verification is preferred.

2 Dual Alternatives

One simple approach to dual (administrative and public) verifiability is to augment a traditional DRE device with the means to provide a verifiable receipt which can be used by voters to track their (encrypted) votes. [Bena07] provides a detailed description of how this can be done. A tight linkage between the administrative and publicly verified tallies can be achieved, but the benefits are severely limited by the fact that the administrative verifiability of traditional DREs is quite weak. It seems likely that a single skilled rogue insider could corrupt tallying software, and numerous studies (eg. [Cali07]) have shown that the independent testing process has not been very effective at detecting irregularities. The “fix” of adding paper audit trails to DREs has been seen to create its own problems including the creation of new privacy risks (especially when the paper maintains the order in which ballots were cast) and questionable effectiveness (since voters seem to do a poor job of verifying the integrity of the paper audit trail).

Optical scan systems have gained favor in recent years because they provide fairly good administrative verifiability. Scantegrity [Scan07] is a system which augments optical scan ballots with letter codes which can be recorded by voters and used as receipts. There are, however, some drawbacks including the requirement that ballots be individualized with distinct letter codes (this complicates the printing process and creates potential privacy concerns), the need for voters to manually record letter codes to form receipts, and a cumbersome challenge process that requires administrative intervention.

3 Verified Optical Scan

The *Verified Optical Scan* system described herein (*VOS* or *VOpScan* for those who like short names) creates a simple dual-verification system with all of the advantages of ordinary optical scan systems. Sets of identical optical scan ballots — such as those in common use today — can be marked either manually or by a specialized ballot marking device.[1] The public verifiability is then enabled by augmenting precinct-based optical scanners with a few additional features that would likely be more economical than, for instance, augmentation of DREs with paper printers (in part because there would typically be fewer optical scanners required per precinct than DREs).

3.1 The *Ideal* Implementation

Ideally, an optical scanner would include a small display, a simple input mechanism that allows a voter to answer "yes" or "no" to a question presented on the display, a small paper printer to provide voters with receipts, and the capability to print directly on ballot pages. Except for the ability to print on ballots themselves, many precinct optical scanners already have these capabilities — although they are currently intended only for administrative purposes such a printing vote totals at the end of balloting. As shall be seen later, the ability to print directly on ballots offers several benefits — even in traditional scenarios without public verifiability. One additional capability that is standard on precinct optical scanners is the ability to read the contents of a ballot and then make a decision as to whether to retain the ballot or return it to the voter. (This capability allows scanners to process a ballot and conditionally return the ballot to a voter in order to correct errors like overvotes.)

Once a voter has completed the marking of a ballot, the voter would feed the ballot into the scanner. The scanner would read the ballot and create an encrypted version of the ballot contents[2] and then print a paper receipt consisting of this encrypted value together with the scanner's serial number, a monotonically increasing ballot sequence number, the date and time, and a short (20-25 character) cryptographic hash of this data to facilitate an easy human consistency check.[3] If desired, the display would offer the voter the opportunity to review the selections as read by the scanner.

Once the paper encryption is printed (and after any possible review of the displayed ballot contents has been completed), the display would offer the voter a simple question — "Do you wish to cast this ballot?" (If no display is available, the voter can indicate a choice by pressing one of two labeled buttons.) If the voter opts to cast the ballot, a digital signature is added to the paper receipt indicating that the ballot has been accepted and cast, and the receipt is given to the voter. In addition, the scanner's interpretation of the ballot contents is printed on the ballot and the ballot is then dropped into the scanner's set of retained ballots. Note that printing the vote selections (as interpreted by the scanner) should not pose any privacy concerns, since the voter's selections are already marked on the same ballot.

If the voter opts *not* to cast the ballot, then the voter is asked a second question — "Do you wish to modify this ballot?". If the voter answers "yes", then the ballot is returned to the voter together with the already printed encrypted receipt. If the voter answers "no", then the word 'VOID" is printed on the ballot and the ballot is returned to the voter. Verifiable decryption data and a different digital signature are added to the receipt, and the receipt is given to the voter. This will serve as challenge ballot to help ensure that the scanner is behaving properly.

At the end of balloting, the scanner can report totals exactly as in current usage. When desired, the set of paper ballots can also be

[1] Ballot marking devices have been suggested as a method of enhancing usability and accessibility of optical scan systems while reducing errors and ambiguities that may be caused by partial or irregular markings.

[2] The details of the encryption method would be determined by the back-end verifiable tallying system and are independent of this work.

[3] Ideally, this paper receipt is printed face down or behind an opaque screen to prevent a coercion attack in which a voter is coerced into taking actions based upon the encrypted value.

counted manually — again as in current usage. However, a simple public verification channel has been added to the system. The scanner can provide the full set of encrypted receipts given to voters, and these receipts can be posted to media such as web sites and local newspapers. Any data that would be included on a paper receipt should also be posted with the set of encrypted ballots, so consistency of encryptions, verifiable decryption data, and thumbprint computations could be verified by observers. Any one of a variety of back-end verifiable tallying systems (including [Chau81], [DLM82], [CoFi85], [Bena87], [PIK93], [BeTu94], [SaKi95], [CGS97], [BJR01], [FuSa01], [Neff01], [GZBJJ02], [JJR02], [Grot03], [Chau04], [Furu04], [Chau05], [CRS05], [PBD05], and [Bena06]) can be employed to show that these encrypted receipts represent the same tally that was produced and reported by more traditional means.

This new verification channel answers the question being asked more and more by voters, "How do I know my vote was counted?" (see, for instance, the recent opinion piece in *USA Today]/* [Bart08]) It also can allay concerns over mis-calibrated or mis-configured scanners. Even the most conscientious of voters need do nothing more than check that their vote thumbprints are accurately posted, and there is no requirement that voters do even this. Effective auditing is achieved if only a small fraction of voters check their receipts.

Under normal circumstances, there's no reason or opportunity for the verified tally to differ from the tally reported by the scanner. The encrypted ballot set is produced from the data read by the scanner and this data can be stored by the scanner together with the raw tally data that it already stores. Indeed, any discrepancy between the raw tally produced by a scanner and the verified tally produced from the published encrypted votes is an immediate indication of either incorrect operation of the scanner or incorrect reporting of the scanners output, and in any such cases the paper ballots can be used to discern the true tally. The benefit of the new verified tally is that it provides a new auditing path beyond manual auditing by election officials. Voters can check that their receipts are accurately posted, and they or their surrogates can perform a full audit to verify that the encrypted ballots that have been posted match the announced tally.

There may, of course, be discrepancies between the electronic tallies and any subsequent manual tally of the paper ballots. This can result, for instance, from paper marking ambiguities or scanner mis-configuration or mis-calibration, but these potential discrepancies are no different than those that can occur when using optical scanning equipment today. The new process, however, gives a new check beyond manual auditing by election officials. Any ballot that is *not* cast serves as a challenge that a voter or inspector can use to check whether or not ballots are being properly scanned. This gives any individual who cares to do so the opportunity to audit the process without placing additional burdens upon voters who do not wish to be bothered. In addition, the printed ballot interpretations allow any discrepancies between an electronic count and a manual count to be immediately isolated and scrutinized. Thus, instead of having a publicly verified count which is over-ridden by a manual recount without explanation, it would be possible to display any ballots which were interpreted differently by the electronic and manual counts and enable careful (perhaps even public) review of such discrepancies.

3.2 Provisions for Reduced Scanner Capabilities

The scenario described above seems to offer the best properties, but in some instances some of these capabilities may not be available on an optical scanner. However, mitigations are possible.

For instance, if for some reason a paper receipt is not available (either because of a paper jam, lack of paper, or lack of a printer), the cryptographic thumbprint of the receipt data can be presented to the voter on the scanner display. Voters who care to do so can copy this 20-25 character thumbprint by hand for use as a receipt. As long as a printer is available, the lack of a display can be accommodated by providing voters with two buttons with labels like "Cast Ballot" and 'Do Not Cast Ballot".

The most likely mitigation would be to accommodate the lack of an ability to print on ballots since this capability is not commonly available as an integral component of current optical scanning devices. This printing capability serves two roles: printing the scanner's interpretation of a ballot's contents and printing "VOID" to prevent an opened ballot from being subsequently cast. Printing of a ballot's contents offers a new and attractive mechanism for reconciling manual and electronic counts, but this mechanism is generally unavailable today and there are still benefits to adding public verifiability without providing for this kind of reconciliation. There is therefore no need to mitigate against the unavailability of this feature.

The ability to "VOID" a ballot, however, is integral to an effective verification process. If the scanner does not have the ability to void a ballot, a voter could challenge a ballot and receive a decryption of its encrypted receipt and then immediately cast the same ballot. A nearby coercer could observe the voter's actions and use the receipt to confirm the voter's selections on the ballot that was subsequently cast. This threat can be mitigated by the assistance of a poll-worker. A voter should not be able to both keep a decrypted receipt and re-cast the ballot which generated the receipt. One option would be for a poll-worker to mediate any returned ballots and verbally ask whether or not the voter wishes to modify the ballot. If the voter opts to modify the ballot, the decrypted receipt should be destroyed (or better yet, not be printed at all). If the voter chooses to not modify the ballot, the poll-worked can can manually mark a "VOID" box on the ballot and then return this ballot to the voter together with the decrypted receipt (or have the decrypted receipt printed at that time). Another option would be to enforce a delay so that any returned ballot would be returned directly to the voter, but the voter would be required to return to a ballot marking station and take sufficient time to make changes before the ballot can be re-cast.

3.3 Write-in Votes

As is typical with optical scan systems, when write-in voting is available to voters the ballot contains an "other" or 'write-in" option. Voters would mark this option as they would any other candidate and then write-in the name of the desired candidate. Both the administrative and public tallies would contain the number of write-in votes for any office, and the allocation of these votes would be managed manually. While it would be possible for the encryption of the ballot to contain an entire ballot image rather than just the selected candidates, this would be inefficient and would present opportunities for coercion.

3.4 Inspections

It is desirable for voters, unofficial observers, and official inspectors to all be able to cast challenge votes and receive decrypted receipts. However the system described herein makes it difficult for anyone other than legitimate voters to do so. If non-voters are to be able to issue challenge votes, a mechanism must be provided to allow them to do so without allowing them to instead cast their ballots. Since the scanner should be unable to differentiate an ordinary ballot from a challenge ballot until after it has printed the ballot's encryption, the process for both cases must be the same up to this point. One option would be for a poll-worker to accompany the challenger to the scanner and physically prevent the cast button option from being selected. Another option would be to scan or photograph the challenge ballot on another device before the challenger uses the scanner — this would allow the vote to be subtracted from totals if it were to be cast.

Additional options would alter the normal voting process. For instance, valid voters could each be given a token that must be inserted into the scanner to complete the vote casting process. Alternately a poll-worker could be assigned to staff the scanner and mediate each ballot-casting decision.

The first option, in which challenge voters are accompanied by poll-workers, seems to be the most practical; but other options should be explored depending on the details of the environment.

4 Properties and Threats

In most respects, Verified Optical Scan shares the properties of traditional optical scan voting. These include retention of voter-generated paper ballots that can be independently audited and used in case of hardware or software failures. There are substantial additional benefits accrued from the verified tally channel, but the new channel introduces some new threats as well.

4.1 New Benefits

Independent Public Auditing The public verification channel allows voters and even passive observers to validate the accuracy of the tally with a simple independent audit. While the development of independent auditing tools may require expertise, their use does not. Individuals who conduct independent audits would be free to use tools from any source or sources they wish — they would *not* be obligated to place their trust in designated election officials. Furthermore, an individual could employ verification tools from multiple independent sources and thereby avoid placing trust in any single entity or enabling any single point of failure. In the extreme, individuals could even build their own verification tools and not delegate any trust whatsoever.

One concern might be that independent audits could produce different results, but this is easily reconciled. Independent audits do *not* produce their own tallies. They only validate (or fail to validate) the tally produced by election officials. Validation failures would be specific. Rather than simply asserting that a validation has failed, tools would be able to isolate any alleged failures and focus attention on specific arithmetic operations. Since the official "proof" of a tally would be nothing more than a sequence of arithmetic operations, the essence of a validation failure would consist of an assertion that an arithmetic claim is false: *"Step 389 of the proof asserts that 2+2=5, and this is not correct."* A claimed validation failure that cannot point directly to a specific arithmetic fallacy can be dismissed.

Elimination of Conspiratorial Fraud Another benefit of the public verification channel is that it prevents well-placed coalitions from altering tallies without detection. While various redundancy checks are intended to prevent any one individual from undetectably corrupting an election tally, many small sets of people could easily manipulate the tally by, for instance, agreeing to replace one set of marked ballots with another. With public verification, any individual would be able to detect a fraudulent tally — even if everyone else has conspired against that individual. (Of course, in this extreme case, there may be little that an individual can do once fraud has been detected; but this is a far more significant issue when a group that has no representation as poll workers or election officials suspects fraud.)

Detection of Scanner Registration Errors Yet another benefit of public verification is the ability to detect *and correct* optical scanning errors that may cause a ballot to be mis-read. Improper scanner calibration has been cited as being responsible for many tallying errors. An important component of public verification is that voters have an opportunity to see how a ballot is being read by a scanner and can retain copies of mis-read ballots together with commitments from scanners of how these ballots were read. Any such ballots would remain uncast and not impinge on voter privacy, but they would provide strong evidence of the need for targeted manual recounts wherever scanners have been demonstrated to be faulty.

4.2 New Threats

Cryptographic Compromise In the unlikely event that the underlying cryptosystem is compromised, the contents of the encrypted ballots could be revealed. While this would not impact the accuracy of the election tally, it would compromise voter privacy. A weak or corrupted pseudo-random number generator is a special variety of cryptographic failure that could also compromise voter privacy.

Coercion The ballot verification process creates several potential opportunities for coercion. Mere fear of cryptographic compromise could keep some voters from voting their conscience, but there are more direct threats that should be mitigated. If a voter is allowed to reject a ballot and then immediately resubmit and cast the same ballot, then the plaintext receipt from the rejected ballot would act as a plaintext receipt for the cast ballot. For this reason, it is best to mark any rejected ballot as no longer eligible for casting; in lieu of this, there should at least be a short waiting period to give opportunities for changes to be made before a ballot can be resubmitted.

Another avenue for coercion is enabled if a coercer can be physically seen by a voter at the time the voter is to decide whether or not a ballot is to be cast. At the decision point, the coercer could signal the voter which option is to be taken. A coerced voter could not safely cast an uninfluenced ballot because upon attempting to cast such a ballot, the voter might receive a signal from the coercer indicating that the ballot should become a challenge ballot and be revealed rather than being cast. Although this threat seems to require a lot of effort, polling stations should be organized so that voters and others cannot linger behind the scanner where they can easily be seen by voters using the scanner.

Ballot Insertion Since posted encrypted ballots are not directly associated with named voters, there is the potential for illegitimate ballots to be added to the set. As with traditional auditing mechanisms, there should be no more ballots in the system then there are legitimate voters who cast ballots. Additional ballots constitute an immediate indication of election fraud. The list of participating voters is a matter of public record,[4] so observers can easily check that the number of posted ballots does not exceed the number of voters who cast ballots; and false claims of voter participation can be evaluated by standard public means.

Ballot Deletion It is possible that a voter could cast a ballot and receive a legitimate receipt but not have that ballot appear amongst the public posting of encrypted ballots. However, every legitimate receipt is signed by the scanner that issued it. Thus failure to post a valid receipt is an immediate indication of a system failure.

It is also possible for a voter to cast a ballot but to receive an illegitimate receipt (for instance, a receipt for which the signature doesn't verify). The voter would know that the scanner has behaved improperly, but this may not be evident to a third-party. Appropriate testing of scanners should minimize the likelihood of illegitimate receipts being created inadvertently. Instances of malicious failure would be subject to forensic testing to determine, for instance, whether the printed receipt actually came from the scanner or was produced elsewhere in an attempt to discredit the scanner.

Ballot Substitution Substitution of an illegitimate ballot for a legitimate one entails

[4] In many instances, the list of participating voters is only "semi-public" to protect voters against stalking, but is made available to those who are deemed to not pose threats to individual voters.

removal of a legitimate ballot, and any such ballot deletion is mitigated by the use of a digital signature as described above.

Duplicate Votes The accuracy of the verified tally could be compromised if identical receipts are given to two or more different voters and if only one copy of such a receipt were to be published. This is why each receipt should include a scanner identification number, a ballot sequence number, and the date and time of issue — making any vote duplication attacks very likely to be caught. Including this information on a ballot receipt and posting it should not create a privacy threat since the raw vote selections are only included in encrypted form.

5 Partial Implementation

The public verification channel of Verified Optical Scanning consists of two primary components: a mechanism for enabling voters to ensure that their votes are being properly recorded and a mechanism which allows anyone to verify that the recorded votes are properly tallied. It is possible to obtain some benefits with lower complexity and risk by implementing only the first of the two components. The mechanism that allows voters to check that their votes are being accurately read by an optical scanner could be implemented without any cryptographic back-end. This would enable the detection and correction of scanner registration errors while avoiding some of the complications and threats imposed by the implementation of a full public verification system. If scanners allowed voters to review their votes on a display only, then few if any additional threats are introduced, but voters will not be able to retain tangible evidence of errant scanners. If scanners print paper receipts, then documentation of errors can be provided to voters, but coercion threats (such as those described above where a coercer signals a voter whether or not a particular ballot is to be cast or retained) must be mitigated. One design for paper receipts could be for a scanner to always print a plaintext paper receipt of any ballot that it reads and then, depending on the request from the voter, either return both the original ballot and the receipt to the voter or retain both the original ballot and the receipt.

Once a mechanism has been put in place to enable voters to check that their votes are being accurately recorded, it is a relatively small step to full public verifiability. Thus, it might well be reasonable to consider a phased implementation in which simple verification capabilities are first added to precinct-based optical scanners and, if and when desired, full public verification capabilities are added subsequently.

6 Conclusions

Verifiability in the context of elections is not a simple binary concept. There are many kinds of verification that enable different sets of people to verify different things under different assumptions. This work has contrasted traditional *administrative* verification, in which select entities are able to mitigate some specific threats, with *public* verifiability which allows any individual to audit against virtually any kind of tally fraud, but introduces new complications and potential threats to privacy.

Verified Optical Scan is introduced as a mechanism which retains essentially all of the comprehensibility and administrative verifiability benefits of traditional optical scan technology while adding capabilities that enable public verifiability and ensure a tight integration between the administrative and publicly verifiable tallies.

Acknowledgements

The author would like to thank Ari Feldman and several anonymous reviewers for many helpful comments and suggestions.

References

[Bart08] **Barton, B.** "Will my vote be counted?" *USA Today Opinion.* (March 27, 2008). See http://blogs.usatoday.com/oped/2008/03/will-my-vote-be.html.

[Bena06] **Benaloh, J.** "Simple Verifiable Elections" *Proceedings of the 2006 Electronic Voting Technology Workshop.* Vancouver, BC (Aug. 2006). Available at http://usenix.org/events/evt2006/tech/.

[Bena07] **Benaloh, J.** "Ballot Casting Assurance via Voter-Initiated Poll Station Auditing" *Proceedings of the 2007 Electronic Voting Technology Workshop.* Boston, MA (Aug. 2007). Available at http://usenix.org/events/evt2007/tech/.

[Bena87] **Benaloh, J.** "Verifiable Secret-Ballot Elections." *Yale University Ph.D. Thesis YALEU/DCS/TR-561.* New Haven, CT (Dec. 1987).

[BeTu94] **Benaloh, J.** and **Tuinstra, D.** "Receipt-Free Secret-Ballot Elections" *Proceedings of the* 26th *ACM Symposium on Theory of Computing.* Montreal, PQ (May 1994) 544–553.

[BJR01] **Bruck, S.**, **Jefferson, D.**, and **Rivest, R.** "A Modular VotingArchitecture ("Frogs")." *Workshop on Theory of Elections.* Tomales Bay, CA (Aug. 2001).

[Cali07] "California Top-to-Bottom Review". Available at http://www.sos.ca.gov/elections/elections_vsr.htm.

[Chau04] **Chaum, D.** "Secret-Ballot Receipts: True Voter-Verifiable Elections." *IEEE Security & Privacy 2* 1, (Feb. 2004), 38–47.

[Chau05] **Chaum, D.** "Recent Results in Electronic Voting." *Fronteers in Electronic Elections.* Milan, Italy (Sep. 2005).

[Chau81] **Chaum, D.** "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." *Communications of the ACM 24,* 2, (Feb. 1981), 84–88.

[CGS97] **Cramer, R.**, **Gennaro, R.**, and **Schoenmakers, B.** "A Secure and Optimally Efficient Multi-Authority Election Scheme." *Proceedings of Eurocrypt '97.* Konstanz, Germany (May 1997) 103–118.

[CoFi85] **Cohen (now Benaloh), J.** and **Fischer, M.** "A Robust and Verifiable Cryptographically Secure Election Scheme." *Proceedings of the* 26th *IEEE Symposium on Foundations of Computer Science.* Portland, OR (Oct. 1985), 372–382.

[CRS05] **Chaum, D.**, **Ryan, P. Y. A.**, and **Schneider, S.** "A Practical Voter-Verifiable Election Scheme." *Proceedings of European Symposium on Research in Computer Security.* Milan, Italy (Sep 2005) 118–139.

[DLM82] **De Millo, R.**, **Lynch, N.**, and **Merritt, M.** "Cryptographic Protocols." *Proceedings of the* 14th *ACM Symposium on Theory of Computing.* San Francisco, CA (May 1982), 383–400.

[Furu04] **Furukawa, J.** "Efficient, Verifiable Shuffle Decryption and

Its Requirement of Unlinkability." *Proceedings of PKC 2004.* Singapore (Mar. 2004) 319–332.

[FuSa01] **Furukawa, J.** and **Sako, K.** "An Efficient Scheme for Proving a Shuffle." *Proceedings of Crypto 2001.* Santa Barbara, CA (Aug. 2001) 368–387.

[Grot03] **Groth, J.** "A Verifiable Secret Shuffle of Homomorphic Encryptions." *Proceedings of PKC 2003.* Miami, FL (Jan. 2003) 145–160.

[GZBJJ02] **Golle, P.**, **Zhong, S.**, **Boneh, D.**, **Jakobsson, M.**, and **Juels, A.** "Optimistic Mixing for Exit-Polls." *Proceedings of Asiacrypt 2002.* Queenstown, New Zealand (Dec. 2002) 451–465.

[JJR02] **Jakobsson, M.**, **Juels, A.**, and **Rivest, R.** "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking." *Proceedings of the 2002 USENIX Security Symposium.* San Francisco, CA (Aug. 2002), 339–353.

[Neff01] **Neff, C.A.** "A Verifiable Secret Shuffle and its Application to E-Voting." *Proceedings of the ACM Conference on Computer and Communications Security.* Philadelphia, PA (Nov. 2001), 116–125.

[PBD05] **Peng, K.**, **Boyd, C.**, and **Dawson, E.** "Simple and Efficient Shuffling with Provable Correctness and ZK Privacy." *Proceedings of Crypto 2005.* Santa Barbara, CA (Aug. 2005) 188–204.

[PIK93] **Park, C.**, **Itoh, K.**, and **Kurosawa, K.** "Efficient Anonymous Channel and All/Nothing Election Scheme." *Proceedings of Eurocrypt '93.* Lofthus, Norway (May 1993), 248–259.

[SaKi95] **Sako, K.** and **Kilian, J.** "Receipt-Free Mix-Type Voting Scheme." *Proceedings of Eurocrypt '95.* St. Malo, France (May 1995) 394–403.

[Scan07] "Scantegrity" See http://www.scantegrity.org.