International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp 7391-7394

End-to-End Cryptography: Spreading Democracy

Mohammed Awad[1] and Ernst L. Leiss[2]
[1] American University of Ras Al Khaimah, RAK, UAE
E-mail: mohammed.awad@aurak.ac.ae
[2] University of Houston, Houston, TX, USA

Abstract
Due to concerns related to the security and privacy of conventional and electronic voting systems as well as the shortcomings of some verification methods, such as Voter Verified Paper Audit Trails (VVPATs), an alternative approach known as End-to-End (E2E) voter verifiable system was proposed. E2E systems rely on cryptography to provide voters and the public with both secrecy and accuracy, two fundamental requirements of the electoral process that conventional voting systems (including paper ballots) failed to assure. While the use of cryptography introduces several advantages over conventional voting methods, cryptographic voting systems have various limitations of their own. In this paper, we will briefly analyze two of the proposed E2E voting systems. We then address some of the existing limitations that may stand in the way of their implementation.

Keywords: E-Government. Digital divide. E-Voting. Cryptography

INTRODUCTION

With conventional voting systems and e-Voting machines, voters are unable to verify personally that the ballot box is handled properly on election day. In fact, with such voting systems, election security depends strongly on a predefined sequence of procedures referred to as the chain of custody, in which the voter has only a very small role.
Figure 1 illustrates the verification steps in a voting system that relies on the chain of custody. In such a system, each step must be verified in order to consider the system secure [1]. These steps include testing the source code and verifying it was installed properly, properly supervised during the elections, physically secured afterwards, and accurately tallied in a secure environment at the end of the day.
There are several drawbacks to the chain of custody approach. For example, voter participation in this chain is very limited. The voter has no other alternative than to trust the machine, the election authorities, and that only eligible ballots will make it to the final tally. Another concern with this approach is the difficulty of detecting mistakes, and if any mistake is detected, recovery is even more difficult. In this situation, rerunning the elections might seem to be the safest way to handle any intentional or unintentional error. Note that the use of Voter Verified Audit Trails (VVATs) slightly reduces the reliance on this chain [1].

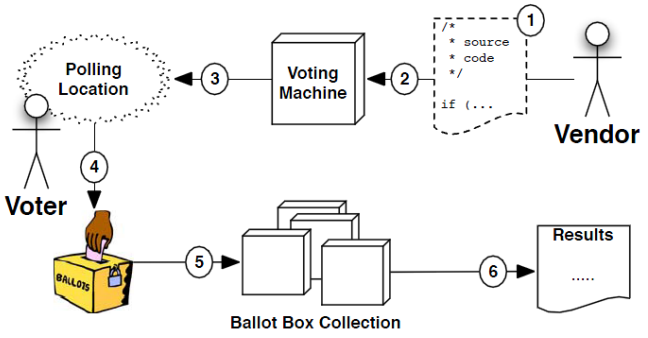

Figure 1: Chain of Custody Voting [1]

The use of cryptography in election systems aims at reducing the reliance on the chain of custody. It also aims at involving the voter more closely in the voting process. In other words, cryptographic voting systems intend to provide the voter with the assurance that his vote was stored as cast and counted as stored, yet assure ballot secrecy by not allowing the voter to proveto a third party how he voted. The concept that the voter can be sure that his vote was cast as intended and recorded as cast is referred to as direct verifiability [9].
End-to-end verifiability (E2E) is usually achieved by giving the voter an encrypted receipt of his vote. The voter can use this receipt to check whether his vote made it to the final tally by comparing it to a published web bulletin that contains the voter list and the encrypted cast ballots. The public can also check thisweb bulletin to ensure that the list consists only of registered voters; this benefit is referred to as universal verifiability [9].
In this paper, we will describe two E2E cryptographic voting systems, namely Prêt à Voter [11] and Punchscan[6]. These systems are meant to be used in a supervised voting environment. As we will show, these designs use cryptography to ensure ballot secrecy; however, the accuracy will be assured by using statistical methods. We will also point out the limitations of such schemes and discuss possible improvements. Even though cryptography can be a complicated topic for voters, these designs try to simplify the voting process while applying cryptography in the verification and auditing phases [2].

PRÊT À VOTER

Prêt à Voter is a voter verifiable voting system that was first presented by Peter Ryan in 2005 who had worked previously on verifiable cryptographic schemes with David Chaum[11].

Since then variant modifications and enhancement were proposed to the scheme by Ryan and other cryptographers [8],[12]. The key idea of Prêt à Voter is to encode the candidates list via randomization. The candidates in each race will appear in a different (random) order on each ballot. Unlike DREs that use cryptography to encode the voter's selections, this scheme encodes the ballot format.
Figures 2 shows two different ballots in the same race [11]. The candidates in each ballot are randomly ordered. After the voter marks the right half (RH) next to his candidate of choice and detaches and discards the left half (LH), no one will be able to figure out whom he voted for. Figure 3 is the right half (RH) of the ballot, which will serve as an encoded vote [11]. Note that at the bottom right of each ballot there is a unique cryptographic value, which will be used to decrypt the ballot. This is the ballot's multi-layer cryptographic value, which will be referred to as the ballot onion and denoted by Θ.

Candidates	Your vote
Obelix	
Idefix	
Asterix	
Panoramix	
	$7rJ94K$
Destroy	Retain

Candidates	Your vote
Asterix	
Idefix	
Panoramix	
Obelix	
	$N5077t3$
Destroy	Retain

Figure 2: Example of two a Prêt à Voter ballots in the same race[11]

Your Vote
X
$7rJ94K$
Retain

Figure 3: The right half of one of the ballots in Figure 2[11]

PUNCHSCAN

Another E2E verifiable voting system is Punchscan, which was proposed by David Chaum. This system relies on cryptography to ensure election secrecy. Not unlike Prêt à Voter, Punchscan is a precinct based optical-scan system. In this system, election officials count and tabulate the votes in private. However, it allows the voters and the public to verify election accuracy by enabling them to pre and post audit the integrity of the electoral process [6].

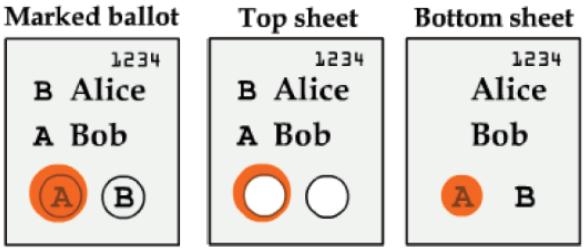

Figure 4: A Punchscan ballot consists of two overlaying sheets (top and bottom)

Typically, a Punchscan ballot consists of two separate sheets overlaying each other. The top sheet displays a list of the candidate names with a symbol next to each candidate and a number of holes (correlating to the number of candidates). The bottom sheet has the same list of candidates, yet rather than holes, symbols are located underneath candidate names. When these two sheets are positioned, one on top of the other, the symbols on the bottom sheet can be seen through the holes on the top sheet [6].
In order to cast a vote, the voter finds the symbol next to his candidate of choice and marks the matching symbol shown via the holes. Punchscan utilizes a marker similar to the bingo-style dauber. Such a marker would leave a disk of ink on the paper when pressed against it. The dauber's mark is much larger than the hole itself, marking both sheets of the ballot at the same time [10].
The order of the symbols on the top and bottom sheets of a ballot is random and independent. An example of a marked Punchscan ballot is shown in Figure 4[6]. In this race there are two candidates: Alice and Bob; thus, there are four possible combinations of ballots. These combinations can be represented in {top/bottom} pairs as follows: {A/B, A/B}, {A/B, B/A}, {B/A, A/B}, {B/A, B/A}. Figure 5 shows all the possible sheets and the resulting possible combinations of a race ballot between Alice and Bob [10].[1] For example, the ballot in Figure 5 will be referred to as {B/A, A/B}. Notice that the candidate names on all the ballots will be displayed in the same order (usually alphabetical); however, the symbols are randomly generated.

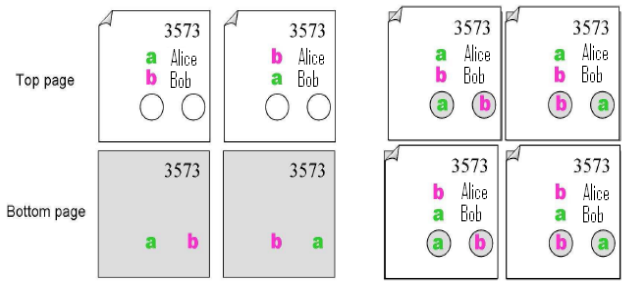

Figure 5: Each Punchscan ballot has four possible combinations (in a race between two candidates)

[1] Figure 5 is a variant of a figure in [10].

Because of the randomness of the symbols, both sheets of the ballot are needed to reveal the voter's choice [10]. A separate sheet of the ballot (top or bottom) will serve as an encrypted vote and will be used to provide E2E verifiability, as we will explain further on. As shown in Figure 4, each ballot has a unique serial number, which is used to decrypt the sheet and reconstruct the ballot. Just as in Prêt à Voter, a threshold number of election officials is needed to perform the reconstruction operation.

LIMITATIONS

Despite the various features provided by verified cryptography, a few limitations discourage adopting it:

Complexity

The complex nature of cryptographic protocols represents a huge mental barrier to adopting this technology, an issue of which most cryptographers are aware. As we have shown previously, E2E schemes try to simplify the cryptography used; however, a certain amount of complexity is still unavoidable [3, 4].

Usability might be another concern of these systems. Many of the cryptographic ballots ask the voter to perform several steps (even after the ballot casting), which can be a burden to the voters.

Reliance on Auditors

Cryptographic systems require auditing the ballots before and after the electoral process. Some requirements exist to ensure that the auditors are from different political parties; however, the auditors must be accorded a high level of trust. While this can be the same case for other voting systems, the main aim behind the use of cryptography is to reduce the reliance on third parties [9].

In addition to auditors, some cryptographic schemes [1] suggest the addition of helper organizations at polling stations; these private parties can provide the voter with several receipt verification services such as checking the digital signature, checking the bulletin board, and performing universal verification.

Additional Steps

Despite reducing the number of steps in the chain of custody approach, we point out that there are some new steps of verification that need to be enforced. For example, a mechanism needs to be put in place to make sure that the voter cannot leave the polling station with the part of his ballot that was supposed to be destroyed. Another mechanism is needed to ensure that the pre-election audited ballots are not going to be in the final tally, and that no one can create duplicates of them to coerce people to vote.

Homomorphism Restrictions

Most of the protocols used in voter verifiable systems rely on variations of homomorphic encryption. Unfortunately, such an encryption does not allow for write-in candidates (a legal requirement in US elections) [9]. Additionally, many of these schemes rely on randomizing the candidates order from one ballot to another; this can be an issue in some jurisdictions that require all voting options to appear in a set order.

New Threats

The main idea behind providing a receipt is to allow the voter to verify that his ballot made it to the final tally without the voter being able to prove to anyone else how he voted, thus eliminating coercion and vote selling and buying, which is also referred to as "receipt freeness" [1]. However, several studies have shown that verifiable voting systems are not completely coercion-resistant, and that by using these receipts, adversaries can launch new attacks such as random voting, pattern voting (the Italian attack), and contract voting [5, 6].

In random voting [7], the adversary tells the voter which position to mark, regardless of the order of candidates on the ballot, thus producing a random vote. The coercer can achieve that by threatening to punish the voters or by tempting them with a reward. Random voting can be effective in areas where the majority of voters do not support the adversary's candidate of choice. This threat can be eliminated if the election authorities design a ballot with a separate sheet (and a separate cryptographic key) for each candidate, an approach that might result in more cumbersome elections.

In pattern voting [7], the attacker provides the voters with a distinctive set of mark positions as a guideline for the voters to follow (or in some cases to avoid). The coercer can verify (by checking the voter receipt) whether or not the voter followed his instructions. For this attack to be feasible, the ballot should contain several races to enable the attacker to create his own unique set of marks. This threat can be eliminated if the election authorities generate separate ballots for each race.

CONCLUSION

End-to-end verifiable voting schemes involve statistical auditing tools, which is an improvement to election integrity. It is safe to assume that there is a very high probability of detecting any integrity attack. While flipping a few votes may go undetected, these attacks will eventually be caught during the auditing phase. Additionally, E2E assures the integrity of the electoral process by involving the voters in the auditing process through encrypted receipts. However, these receipts generate new threats that traditional voting systems are not prone to, such as pattern voting, random voting, and contract voting. When it comes to confidentiality and denial-of-service attacks, E2E schemes do not offer a tangible improvement against them (in comparison to conventional voting methods). Mainly, end-to-end cryptographic voting schemes tend to use threshold cryptographic keys (or a cryptographic key). Notice that in such a scheme, if the election officials conspire they can easily invade a voter's privacy. Generally, E2E schemes have the potential to overcome the conflict between voter privacy and secrecy; however, as we have shown in this paper, they have several limitations of their own to overcome.

ACKNOWLEDGMENT

Partial support under NSF grant DGE 1433817 is acknowledged.

REFERENCES

[1] Adida, B.:Advances in Cryptographic Voting Systems. Doctoral thesis. Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (2006).

[2] Awad, M.:Using Cryptography and Enhanced Verification to Safeguard Electronic Voting. Doctoral thesis. Department of Computer Science, University of Houston, Houston, TX (2011).

[3] Awad M.,Leiss,E. L.: End-to-End Cryptography: Potentials and Limitations. The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). IEEE Xplore Digital Library. IEEE Catalog No: CFP13811-ART. ISBN: 978-1-908320-20-9. London (2013)

[4] Awad M.,Leiss,E. L.: Cryptography and Democracy: Providing Assurance to Voters. Central and East European E|GOV Days 2014.eGovernment: Driver or Stumbling Block for European Integration. ISBN: 978-3-85403-300-4. Budapest (2014)

[5] Clark, J., Hengartner, U., Larson, K.: Not-So Hidden Information: Optimal Contracts for Undue Influence in E2E Voting Systems. In Proceedings VOTE-ID, 1-17 (2009).

[6] Fisher, K., Carback, R., Sherman, A.:Punchscan: Introduction and System Definition of a High-Integrity Election System. In Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 06). Cambridge, UK (2006)

[7] Kelsey, J., Regenscheid, A., Moran, T.,Chaum, D.: Hacking Paper: Some Random Attacks on Paper-Based E2E Systems. Frontiers of Electronic Voting.Dagstuhl Seminar Proceedings (2008)

[8] Küsters, R., Truderung, T., Vogt, A.: Improving and Simplifying a Variant of Prêt â Voter. Proceedings VOTE-ID (2009)

[9] McGaley, M.: E-voting: an Immature Technology in a Critical Context. Unpublished doctoral thesis. National University of Ireland (2008). Retrieved May 20, 2014, from http://www.cs.nuim.ie/~mmcgaley/

[10] Popoveniuc, S.,Hosp B.: An introduction to Punchscan. In Proceedings of Workshop on Trustworthy Elections 2006 (2006). Retrieved June 10, 2013, from http://punchscan.org/papers/popoveniuc_hosp_punchscan_introduction.pdf

[11] Ryan, P. Y. A.:The Computer Ate my Vote. Technical Report CS-TR-988. University of New Castle upon Tyne (2007). Retrieved April 13, 2012, from www.dagstuhl.de/Materials/Files/07/07091/07091.RyanPeter.Paper.pdf

[12] Ryan, P. Y. A., Teague, V.: Ballot Permutations in Prêt à Voter. In EVT/WOTE'09 Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections (2009). Retrieved May 25, 2014, from http://www.usenix.org/event/evtwote09/tech/full_papers/ryan.pdf