

Electronic Voting: Integrity vs Anonymity

Ayca Begum Tascioglu, ID:2020531

Submitted to Prof. Nicola Laurenti

for Information Security Lesson Literature Review Essay Assignment

Abstract

This paper focuses on the electronic voting systems its infrastructure; investigates the privacy, integrity and verifiability principles.

Introduction

In electronic voting systems, privacy, integrity, and verifiability can be aimed at. Even though there is no certain model to compare electronic voting systems with traditional paper-based voting, voting processes such as counting, or recounting the votes can be performed in a more transparent and quicker way. It can be said that even the verifiability can be strengthened by the electronic voting systems since the problem part, the teller can be realized and can be fixed easily. Despite the fact that the effect of the electronic voting systems on democracy cannot be underestimated, there should be a sensitive balance in electronic voting systems in between anonymity and integrity. If the anonymity is strengthened then it will increase the privacy of the voter yet can damage the integrity since providing the voter's vote will be harder. If the integrity is increased that the counting is publicly revealed, then the privacy will be weakened. In order to set the balance between these principles, many of the different models are proposed. In this paper, end-to-end auditable voting systems will be discussed with the RSA and digital signature system.

Electronic Voting Systems

In every voting system, integrity, privacy, and verifiability principles should be guaranteed [1]. Integrity is the correctness of the information received, in this case, the voter's vote should be tallied correctly. Privacy is the use of the information received by the sender, but this information should be only used by the desired transmitter, in this case, a voter's vote should be received by only the transmitter; anyone cannot be able to link the vote and the voter. There should not be any information about the voter be revealed with the ballot. The transmitter can identify the voter with a digital receipt yet if this receipt is found by someone else, the founder should not be able to receive any information from this receipt. Lastly, verifiability is confirming the linkage between inputs and corresponding outputs; there should not be a different result in case of recounting of the votes, the system's output, the result of voting should be the same in every recounting. However, if the votes are counted and revealed publicly in the way that each voter can verify their vote, there will be perfect verifiability and perfect integrity but the system has zero privacy in that case [1]. As a result of that, there will be major problems such as selling votes would be emerged if the system cannot

provide anonymity. Some of the cryptographic voting systems are focused on guaranteeing the privacy, verifiability, and integrity principles together, hence they use some techniques such as dividing the counting and revealing process to multiple intermediate layers with mixed nets. These systems also use RSA, Rivest-Shamir-Adleman cryptosystem, however, if the attacker has enough computational power, RSA can be evaluated as a non-secure system.

For the correctness, to ensure that the voting procedure is held properly, we should be able to show that voter is anonymous which means that there is no way for a stranger to understand which party that voter voted, also, the correctness of that all votes are tallied and counted correctly should be granted. In that way, we need to prove both anonymity and privacy principles together. The voter should be anonymous yet the voter should also be sure that his/her vote is counted and affect the result, if anonymity cannot be guaranteed then selling vote will be a problem, freedom of the voter cannot be secured; if the privacy principle cannot be guaranteed then there will be no trust on the result of the election. In an election system, individual verifiability, which means voters are able to see what they voted, and their vote is counted and affected the result correctly, and universal verifiability that anyone can verify that the result of the election is correct [2]. In case to verify voter their vote is tallied correctly, digital signature revealed receipts can be used [3]. For the basic perception of a traditional voting system, all legitimate users should be listed, and when a voter voted, the system should not give them a right for another vote; a voter should only vote once for an election. By providing such control over the participants of the election, the digital signature is used. Digital signatures provide voter's authentication, it gives information about that the message is coming from the original or not [4].

Asymmetric Authentication and Integrity Protection

Electronic voting systems are based on an asymmetric encryption model since there are two different keys, one is the public key and one is the private key. In the general model of the asymmetric authentication and integrity protocol, the attacker and the desired receiver can have the public key. Signing the user input message is the same as symmetric encryption yet, the verification part is different in asymmetric encryption. RSA (Rivest-Shamir-Adleman) cryptosystem, which is a computational security system, it is possible to leak information if the attacker has enough computational power; RSA is also a one-way function that carries easy to compute but hard to invert principle [5]. In the light of that information, in RSA, even though it is easy to encrypt the message, it is hard to derive the original input message from the encrypted version of the message.

To provide integrity, privacy, and verifiability principles, anonymous channels, blind signatures, and homomorphic encryption can be used [2]. As Chaum stated about the anonymous channel, the message will be encrypted with a public key and also with a private key, the holder of the private key only be able to decrypt the message, and by the public key, the content can be reached [6]. The decryption procedure is similar to onion routing, the message is carried with layers, and only layers can have the private key of the previous layer. Also, the blind signature is a mechanism that is similar to digital signature yet in the blind signature mechanism, the information is not be revealed while in the encryption process; the blind signature mechanism is for ensuring that the layers between the voter and the final teller only can reveal the outer envelope of the vote, not the inner; in each layer, the teller takes a signed vote with a private key of the previous teller, encrypts it with a private key of its own, and sends to the next layer. Moreover, in each bench, the votes are mixed

[3]. For instance, when the third voter voted, their vote can be counted in 579th order in the first teller, and at the next teller, it can be counted on fifth-order, orders are uniform numbers to increase anonymity. Homomorphic encryption allows tellers to do calculations on the encrypted data, rather than fully decrypting it. The checking of tellers follows zero-knowledge protocol [3]. At each level, the result of the mix of ballots is published on the website yet, the only known value by everyone is the vote count; no linkage between the vote and voter should be revealed. Also, it is possible to check if votes are counted correctly. With these middle reveals, it is easier to detect whether there is a wrong behavior of any teller, if there is, recounting after that specific teller can be also eased.

Digital receipts can also be a useful technique to prove to voters that their vote is tallied, these receipts can grant voters to view their vote is correctly included/tallied, even after the voting phase [3]. Using digital receipts also need the following requirements:

- Nobody other than the voter can link the vote and the voter; linkage between the vote and the voter should be secret
- The receipt should be created in a way that no other person can link the voter and the vote, in that case selling votes can be avoided; voters should be free to decide their own vote only
- The voter should be able to revise, correct, and change their ballot
- The voter should be ensured that their vote is correctly tallied [3]

With digital receipts, voters can be able to verify their vote is tallied via the website [7]. Creating these receipts varies between different approaches. To exemplify, the ballot system of Prêt à Voter, the candidate list will be randomly printed in the ballots and will be destroyed at the end of the marking phase. In such ways, the risk of selling vote is decreased, because the returned receipt does not give any information about the selection of the voter. In the ThreeBallot voting system, three ballots together are aimed to give meaningful information about the vote; voters only can keep only one receipt which does not include the candidate list [8]. However, it is proved that the ThreeBallot voting system could not satisfy in decreasing the risk of the attacker to find voter's choice.

Voting Phase

First of all, a ballot image should be created. As mentioned, in a voting system that creates receipts, ballot images can be varied to increase privacy. In Prêt à Voter Approach which is also a voter-verifiable voting system, gives voters the ballots with the randomized candidate list, after the vote is marked, the candidate list in the ballot will be destroyed [7]. In that way, no other person other than the voter will be able to read and understand the receipt. As stated in the paper [3], ballots can be created in a way that has two layers, which have information bits diagonally. In the below image, there are four choices to vote for.

```

[[['0', '0'], ['0', '0'], ['0', '1'], ['0', '1'], ['1', '1'], ['1', '1'], ['0', '1'], ['0', '1']]]
In [2]: runfile('/Users/Ayca/Desktop/ElectronicVoting/votecast.py', wdir='/Users/Ayca/Desktop/ElectronicVoting')
Initial: [[['0', '0'], ['0', '0'], ['0', '1'], ['0', '1'], ['1', '1'], ['1', '1'], ['0', '1'], ['0', '1']]]
Vote:2
[[['♥', '♥'], ['♥', '♥'], ['♥', '♠'], ['♥', '♠'], ['♠', '♥'], ['♥', '♠'], ['♥', '♠'], ['♥', '♠']]]
[[['♥', '♥'], ['♥', '♠'], ['♠', '♥'], ['♥', '♠']]]
In [3]:

```

Figure 1: Ballot Image Visualization

Initial ballot can be represented with matrix where information bits are colored in yellow.

Candidate 1		Candidate 2		Candidate 3		Candidate 4	
0	0	0	0	1	1	0	1

Figure 2: Initial Ballot Visualization without Encryption and Information Bits

Candidate 1		Candidate 2		Candidate 3		Candidate 4	
0	0	0	1	1	1	0	1
0	0	0	1	1	1	0	1

Figure 3: Initial Ballot Visualization Completed with Information Bits

After the voter performs their selection, the information bits of the selected candidate will be reversed. To exemplify, if the selection is Candidate 2, information bits in the Candidate 2 will be changed as follows:

Candidate 1		Candidate 2		Candidate 3		Candidate 4	
0	0	0	0	1	1	0	1
0	0	1	1	1	1	0	1

Figure 4: The Ballot after the Voter Marked Their Selection

The voter is able to decide to change their vote, in that case, a new ballot will be provided, if the voter is sure about their final vote and display their given vote correctly, they can continue the further process. The voter will decide which layer they want to keep, the other layer will be destroyed. Each layer has the serial number and information about the encryption. Assuming that the voter decided to keep the upper layer, they will leave with the upper layer as follows (the ballot also has the serial number and further encryption information); ballot also can be presented with other symbols rather than 0 and 1:









Candidate 1		Candidate 2		Candidate 3		Candidate 4	
							

Figure 5: The Selected Layer of the Ballot with Encrypted Vote

These ballot receipts can be used to increase voter confidence that their vote is correctly tallied since they can check it with third-party organizations, or the government's website. After encrypting phase, the bench of votes is transmitted to tellers; in each teller, the destructed part of the vote can be reconstructed on behalf of the encryption information, such as which layer is kept and the information bits. Furthermore, for increasing anonymity, votes are mixed then transmitted to the next teller. Each teller first decrypts the ballot with the private key of the previous teller's key, then reveal the result of the bench, sign the message with its own private key and provide next teller in the unordered ballots.

Conclusion

Electronic voting systems are aimed to satisfy privacy, integrity, and verifiability. There are several electronic voting models are discussed in history to satisfy these principles. Integrity and privacy are the principles that may be problematic since they can affect each other negatively. The models which are discussed in this paper are aimed to increase all of these principles together. In the light of the information above, there are different techniques used to provide these principles. First of all, the multiple ballot system increases verifiability with the receipt which is kept by the voter, the voter will be able to verify that their vote is counted correctly and the election result will not change in case of recounting. Also, encryption of the given receipt increases the anonymity of the voter since any other person rather than the voter is able to know the voter's vote. Secondly, after the voter left the booth, the group of votes is sent to the tellers, whose mechanism is similar to onion routing. By using an anonymous channel and RSA crypto-system, votes can be revealed in the middle stages without the decryption phase; because the envelopes are signed with two different keys. In that way, both verifiability and integrity can be increased. Lastly, mix net structure allows the system to randomize the order of ballots in each intermediate stage, which also increases privacy. In a conclusion, we can say that by using an electronic voting system, we can get closer to perfect privacy, integrity, and verifiability.

References

- [1] B. Hosp and P. L. Vora, “An information-theoretic model of voting systems,” *Mathematical and Computer Modelling*, 17-Jun-2008. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0895717708001775>. [Accessed: 13-Feb-2021].
- [2] L. Langer, H. Jonker, and W. Pieters, “Anonymity and Verifiability in Voting: Understanding (Un)Linkability,” 2010. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-17650-0_21. [Accessed: 15-Feb-2021].
- [3] D. Chaum, J. Graaf, P. Y. A. Ryan, and P. L. Vora, “Secret Ballot Elections with Unconditional Integrity,” 2007. [Online]. Available: <https://eprint.iacr.org/2007/270.pdf>. [Accessed: 14-Feb-2021].
- [4] M. Kamat, S. Ibrahim, M. Salleh, and S. R. A. Aziz, “Secure E-Voting with Blind Signature,” 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings., 2003. [Online]. Available: https://www.academia.edu/8369645/Secure_Evoting_with_blind_signature. [Accessed: 15-Feb-2021].
- [5] N. Laurenti, “Physical Layer Secrecy” presented to Information Security class to University of Padova, PD, IT, 2020 [PowerPoint Slides]. Available: https://elearning.dei.unipd.it/pluginfile.php/646334/mod_resource/content/1/PHYsecrecy.pdf
- [6] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *ACM Digital Library*, Feb-1981. [Online]. Available: <https://dl.acm.org/doi/10.1145/358549.358563>. [Accessed: 15-Feb-2021].
- [7] P. Y. A. Ryan, S. Schneider, and V. Teague, “End-to-End Verifiability in Voting Systems, from Theory to ...,” May-2015. [Online]. Available: <https://orbilu.uni.lu/bitstream/10993/25430/1/End-to-End%20Verifiability%20in%20Voting%20Systems%2c%20from%20Theory%20to%20Practice.pdf>. [Accessed: 16-Feb-2021].
- [8] K. Henry, D. R. Stinson, and J. Sui, “The Effectiveness of Receipt-Based Attacks on ThreeBallot,” Dec-2009. [Online]. Available: <https://cs.uwaterloo.ca/~dstinson/papers/ThreeBallot-Jan.30.pdf>. [Accessed: 16-Feb-2021].