2017 International Conference on Information Technology Systems and Innovation (ICITSI)
Bandung, October 23 – 24, 2017
ISBN: 978-1-5386-3100-3

Verifiability Notion in e-Voting Based On Modified ThreeBallot System

Teguh Nurhadi Suharsono, Kuspriyanto, Budi Rahardjo
School of Electrical Engineering And Informatics
Bandung Technology Institute
Bandung, Indonesia
teguhns21@gmail.com, kuspriyanto@yahoo.com, rahard@gmail.com

Fazmah Arif Yulianto
School of Electrical Engineering And Informatics
Bandung Technology Institute
School of Computing, Telkom University
Bandung, Indonesia
fazmah.arif@gmail.com

Abstract—**The need to manage the voting process more efficiently, more flexible access, and faster results setting make e-voting systems a promising alternative. ThreeBallot was proposed to overcome the contradiction among some e-voting requirements, i.e. anonymity, privacy, and verifiability. Verifiability is an electronic voting system should provide a method to verify that the system works as expected. The verification of the original ThreeBallot method we call partial verification, because the voter only has a 1/3 belief that his voice exists and does not change. By making some modifications and additions to the ThreeBallot system, a system which allows for full verification is made (it is assured that three parts of the ballot do exist and remain unchanged). Unfortunately, by using original ThreeBallot, voter has only partial confidence in verifying his/her vote. We propose a modified ThreeBallot-based e-voting system to provide full verification without sacrificing either anonymity or privacy for verifiability notion.**

Keywords—verifiability, anonymity, e-voting, full verification, partial verification, privacy, modified ThreeBallot

I. Introduction

The need for more efficient organization and management of voting process, more flexible access for voters, and faster voting result publication, makes electronic voting as one of the most promising solution.

In order to ensure certainty of choice, then the voting stage is divided into four main [1] namely;

1. Registration, the process of registration of participants voting in accordance with applicable regulations;
2. The validation, data validation process involves voters, to get the voters eligible to vote and to avoid duplication of data;
3. The collection, which is a process of collecting voters to vote;
4. Tallying, processes related to vote counting.

Concerning what have been stated by Fujioka et al. [2], Cranor and Cytron [1], Salini and Kanmani [*3*], Wu et al. [4], and Adeshina and Ojo [5], there are specific and important requirements which usually emerged when we talk about e-voting system, some of them are: eligibility, anonymity, privacy, accuracy, verifiability, fairness, dispute-freeness, and auditability. It is usually considered that there exist some contradictions among those requirements, for example: between anonymity, privacy, and verifiability. It is not easy to fulfill these three requirements at a same time. Anonymity means nobody (or nothing) can trace the relationship between a particular vote and who cast it (we call him/her 'the voter'). We define privacy as a condition in which there is no voter possess enough evidence to show and to prove his/her vote to anyone else. Verifiability requires that every voter should be able to check whether his/her vote is actually recorded correctly and the system has count it correctly.

Based on Cranor and Cytron [1] states that the e-voting should have parameters that can be used as a guideline. Statement known as the Golden Rules of e-voting, which includes:

1. Accuracy: selection does not change, noise can not be eliminated and the vote defects are not counted.
2. Invulnerability: just who is entitled to vote and voting only once.
3. Privacy: unknown selection and choice of vote can not be proved.
4. Verifiability: the results of calculations can be re-verified.

Based on Guasch Castell'o [6], verifiability is an electronic voting system should provide a method to verify that the system works as expected. Voters must be able to verify their voting results according to their choice and be taken into account in the vote counting process. The auditor shall be able to verify that all votes by eligible voters may be included in the vote count. Verifiability is aimed at ensuring the correctness of the votes cast by the electorate.

Implementation of voting technology will not necessarily be well received by the public. It is highly influenced by the level of public confidence in the quality of voting technology is used. Based on Cranor and Cytron [1] shows that the verifiability is one parameter in e-voting, so verifiability is the most dominant in improving the quality of the technology of voting. With the parameter verifiability, providing confidence and trust to the voter that the voting system used will provide protection to both the votes cast and the voters themselves [7]. Relating to data security, the e-voting system data security can be divided into two parts, namely: security associated with a ballot (starting from the stage of voting until the stage of counting), and verification by the voter to ensure the contents of the ballot has not changed and has been counted correctly [8].

The next part of this paper briefly describe the partial verification which supported by ThreeBallot system. The third part contains our proposal to modify and enhance the ThreeBallot-based e-voting system in order to provide full verification. The fourth part of this paper explains how to do full verification without sacrificing either anonymity or privacy.

II. THREEBALLOT AND PARTIAL VERIFICATION

In 2006 Ronald L. Rivest proposed ThreeBallot [9] to provide anonymity, privacy, and verifiability in voting system. The ballots itself contain no information which can be used to trace back the voter who cast the particular vote. Voters bring home the receipt of their vote so that they can verify their own vote in some later time. Receipt is a copy of just one ballot(among three ones that the voter casted into the ballot box). Just having one single ballot, the voter has no enough evidence to show and prove his/her true vote. By this reason, it is said that the system maintain privacy of voters and votes. ThreeBallot originally designed to be used in paper-based voting system, even though the idea can also be used in electronic-based voting system, as proposed by Santin et al. [10].

The system is composed of several entities, namely: registration agent, voting console, voting manager, electronic ballot box, and electronic election bulletin board. To be able to vote, voters initially contact the registration agent to obtain credentials. The registration agent interacts with the voting manager to get the ballot ID and then uses it to generate the credentials that will be given to voters. After going through the authentication process, voters use the voting console to include their choice. While the voting manager keeps the selection in electronic ballot box, voting console gives the receipt to the voters. When the voting period ends, the electoral authority and election representatives begin the counting phase. The results of the count are published via electronic election bulletin board.

Prior to displaying in the voting console, the voting manager gives the initials to three ballots (one for each candidate row in the randomly selected column). To indicate his choice, the selector only needs to add one more mark to the empty column in the selected row of candidates. As a receipt, voters may choose any ballot. Once encrypted using the election representative's public key, the three ballots are then stored in three different repositories (electronic ballot boxes) to remove the connection between the ballots.

The vote counting phase can be started when the election representative inserts his private key to decrypt all the ballots. The vote count is displayed on the bulletin board so voters can also verify.

The ThreeBallot technique is aimed at securing the secrecy of voters' choice and privileges, facilities for verification, and eliminating voter opportunities to show the content of their choice to others. Rivest originally designed ThreeBallot for use on paper-based voting systems [9].

One key principle that ThreeBallot uses is "vote by rows and cast by columns" [9]. The ballot used consists of three separate columns. Each part (column) of the ballot is composed of two parts, namely: selected area and identity area (in the form of random and unique code per column).

There are several rules for using the ballot, including: (1) To select a candidate, mark the exact two circles in the line corresponding to the candidate. There are no restrictions on which columns to mark. (2) To not select a candidate, mark the exact one. There are no restrictions on which columns to mark. (3) For each row there must be at least one marked circle. Ballots will not be accepted if there are lines left blank. (4) There should be no row of three circles marked. Ballot will not be accepted if there is a fully charged line.

After going through the process of checking the validity of the filling, voters may choose one part (column) of the ballot to be copied and brought as a receipt. Three parts of the ballot are then separated and inserted into the ballot box. After the voting period ends, all ballots will be scanned and the data is displayed on the bulletin board for public viewing. Voters can also check if the ballot is listed on the bulletin board by comparing the unique code printed on the receipt they own.

The calculation of the final result can be done as usual, noting that the actual number of votes earned by each candidate is the amount earned from the counting of all the voting cards minus the number of voters entering the vote.

During verification process, a voter searches bulletin board (by him/herself or assisted by trusted one) for a ballot which has the same ID as his/her own receipt. When he/she found the matched ballot, actually he/she only has 1/3 confidence that his/her vote is correctly recorded in the system. There is no way that he/she knows either his/her other two ballots are also correctly recorded or not. This is what we call ‘partial verification.

Having only 1/3 of the vote as a receipt, the voter does not have enough evidence to show the content of his choice to the other party. This will reduce the chances of a vote selling.

III. PROPOSED SYSTEM

Beside partial verification mentioned before, we need full verification to make sure that all three ballots are exist in system's record and recorded correctly as it is casted by the voter. To do that, we need to modify and enhance the ThreeBallot system. As we intent to make a stronger verification, we should be careful not to decrease the anonymity and privacy aspects below the acceptable level. Overall architecture of the proposed e-voting system is depicted in Figure 1. This system designed with assumption that it will be used to vote for a single winner and each voter votes only for one candidate.

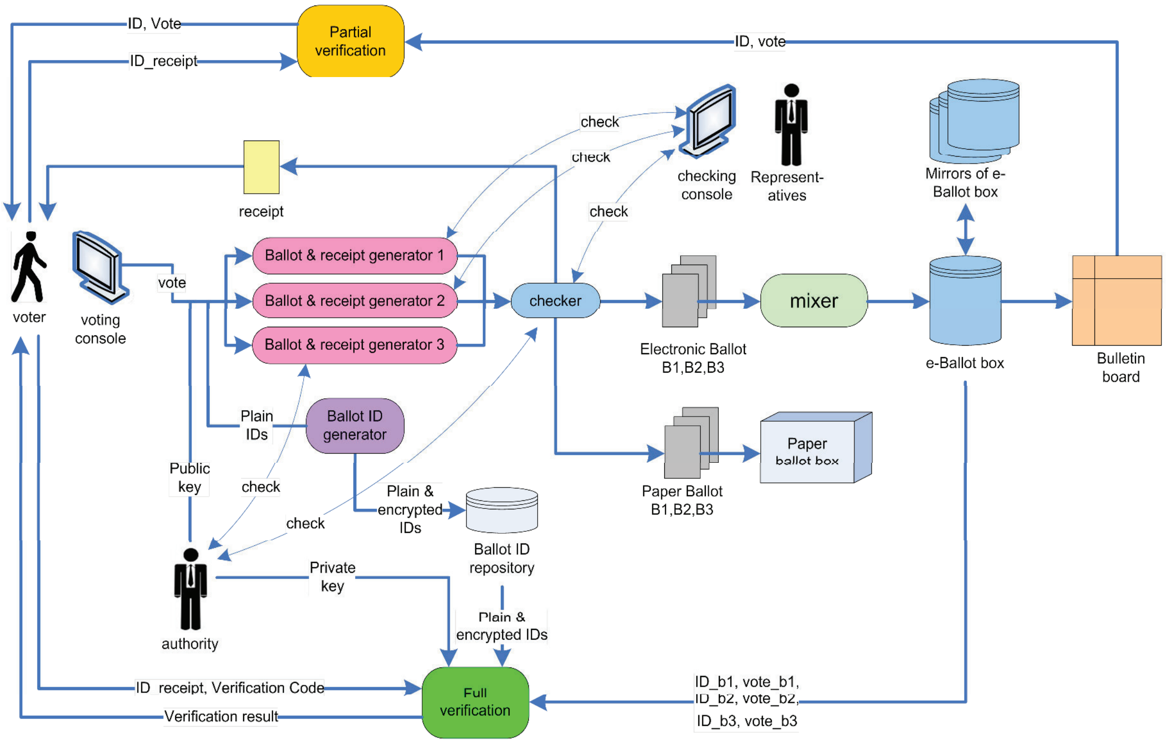


Figure 1. Architecture of the Proposed e-Voting System

After passing the eligibility checking, voter uses voting console (touch screen) to cast his/her vote. Based on this vote, system then generates three electronic ballots, three paper ballots, and one paper receipt. Every ballot has its own randomly generated unique identity (ballot ID). System fills the voting region in each ballot with random pattern as long as it is exactly representing the vote. Figure 2 gives the example of paper ballot generated by the system.

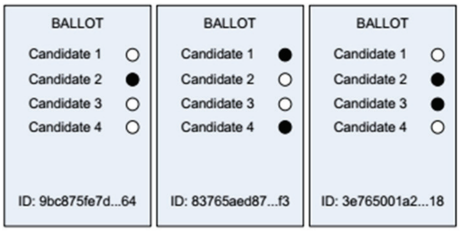


Figure 2. Example of generated ballot, filled randomly to express vote for candidate 2

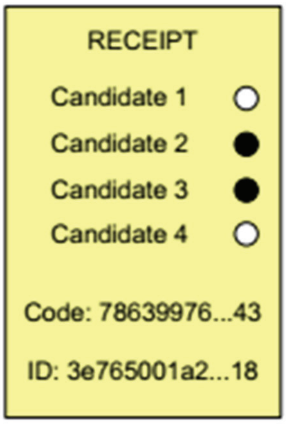
All of paper ballots will be inserted into paper ballot box. The ballot box will be opened and the ballots counted manually only in the case where there is indication of fraud or incorrect operation of electronic ballot recording and/or counting. Meanwhile, electronic ballots are generated and each of them represented as tuple (ID,C1,V1,…,Cn,Vn), where ID is a unique ballot ID, Cn is a unique code for candidate-N, and Vn contains the vote status for candidate-N (filled or empty).

Before goes to electronic ballot box, the three tuples must went through a mixer to randomize the location of their recording inside the ballot box database. It should be done to eliminate the clue of relationship between those three ballots. If they are recorded in sequential order, it is very easy to guess which ballot set constitute one original vote. All data written to e-ballot box also simultaneously backed up into the mirrors. Bulletin board contains information regarding all ballots have been recorded by the system. Public has direct and open access to this bulletin board.

Receipt is generated as a result of voter's free choice in selecting which ballot (among those three) to be copied. Along with the exact copy of selected ballot, verification code also printed on the receipt. This code will be used during the fullverification process. One possible formula to generate the code is as follows:

Code = XOR(hash(tuple_ballot1),hash(tuple_ballot2), hash(tuple_ballot3)) (1)

Hash function returns the digest of each ballot tuple. To maintain the anonymity, we omit the sequence number of each ballot. Because of the commutative and associative properties of exclusive OR operator, we don’t have to worry about the sequence. Figure 3 gives an example of receipt related to complete ballot in Figure 2.



RECEIPT

Candidate 1 ○

Candidate 2 ●

Candidate 3 ●

Candidate 4 ○

Code: 78639976...43

ID: 3e765001a2...18

Figure 3. Example of receipt

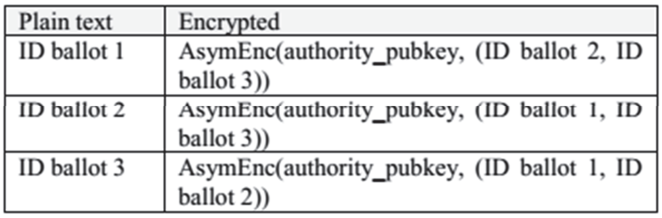
To improve the reliability of ballot and receipt generator process, we propose three redundancy of ballot and receipt generators. The three identical processes receive the same inputs (vote, 3 ballot IDs, and authority’s public key). In parallel, they generate 3 tuple ballots and verification code. Outputs from those three modules checked by the checker module. If they are identical, then electronic ballots will continue to mixer module, paper ballots and the receipt will then be printed. On the contrary, if the results are not the same it is an indication of fraud or improper operation of ballot and receipt generator. What will be the next action depends on the pre-defined voting procedure, ranged from just repeat the generation processes up to halting the voting process to run a thorough investigation and recovery actions.

Before and during voting session, all voting representatives (including witnesses from each candidate and independent observers) have right and access to do sampling checks whenever they need to make sure that two ballot and receipt generators (number 1 and number 2) and the checker moduleare operating correctly. Representative uses a checking console to ask the generators to generate three tuple (ballots) and a receipt, based on ID and vote which chosen freely by representative him/herself. The results from generators are then compared with the expected results (pre-computed by the representative using the same algorithm which claimed been used by the generators). The same technique can be used to the checker module. On the other hand, voting authority may also check the other ballot and receipt generator (number 3) and the checker module.

IV. FULL VERIFICATION

To do full verification, we need three related ballots which came from a same original vote. This is why we have to record the relation between those three ballots in a secure way. After generating IDs for three ballots, there will be three new entries in ballot ID repository. Each entry consist of two parts: nonencrypted part, and encrypted part (using asymmetric algorithm and authority’s public key). The system need to save all three ballots because it is not allowed to record which ballot has been chosen by the voter to copy as a receipt. Table 1 illustrates the three related entries in ballot ID repository.

Table I. Illustration of related entries in ballot ID repository



Plain text	Encrypted
ID ballot 1	AsymEnc(authority_pubkey, (ID ballot 2, ID ballot 3))
ID ballot 2	AsymEnc(authority_pubkey, (ID ballot 1, ID ballot 3))
ID ballot 3	AsymEnc(authority_pubkey, (ID ballot 1, ID ballot 2))

Ballot IDs can be generated in pure random resulting the highest anonymity level, or we can use k-anonymity approach as devised by Matthijs R. Koot [11]. By using k-anonymity, some digits will be treated as Quasi ID in a way that the anonymity set equal to k. Number of digits and what kind of information to be used as quasi ID depends on the need of anonymity level and votes compilation granularity level. If there is a need to count the votes at province level then we can use two digits as a province code. As a result, we have anonymity set size equals to the number of eligible voters in that particular province. The more digits being used as quasi ID, usually the smaller anonymity set size will be.

As in the original ThreeBallot system, voter who wishes to do a partial verification will access the bulletin board to search for ballot which ID matched with ID written on the receipt. When the intended ballot found, voter can check whether the ballot content is equal with the receipt content or not. If those two are equal, the voter has 1/3 confidence that his/her vote is correctly recorded.

Beside the information written on the receipt, full verification process also need approval from voting authority. Authority approves the process by providing authority’s private key. Concerning the use of private key, full verification process better be executed off-line (not through open communication network/ Internet) and on-site (in full controlled secure environment, authority office is good choice). Using ID on the receipt, one can query the ballot ID repository to find all ballot parts related to that particular receipt. One ID matched with receipt ID will be found in plaintext, while two other IDs still in encrypted form. Authority’s private key is needed to decrypt those two IDs.

The three related IDs are then used to find three ballot tuple in e-ballot box. Next, digest will be computed from the complete ballot using same formula as the one to compute the verification code (Formula 1). If the digest matched the verification code written on the receipt, we can conclude that all ballot parts are correctly recorded. To simplify the process, receipt ID and verification code could be printed in 2D or 3D barcode.

In contrast, if any ballot part was missing or the digest doesn’t match with the verification code, then voter may claim an objection to voting authority. What will happen next depends on the pre-defined rule of the voting itself.

Full verification processes only the digest of the ballot, not the content of the vote. It is to make sure that the privacy of the vote still maintained safely. If the ballot and receipt generator, checker module, and full verification module work as it should be, then no one else can learn what the actual vote of individual voter is, even if that someone successfully possesses the receipt. He/she can only know whether the ballot is fully and correctly recorded in the system or not.

V. Evaluation

As proposed in the original ThreeBallot system, voters intent on partial verification can directly access the bulletin board to search for the ballot portion whose ID is the same as the ID listed on the receipt. If the ballot portion is found, the selector can check whether the contents of the choice in the ballot section are the same as the ones listed on the receipt. If both are the same, then the electorate may have a belief of up to 1/3 that his choice is actually recorded in the system and has not changed.

Full verification in addition to requiring information that is in the receipt, also need to get approval from the administrator. This agreement is realized with the administrator's private key usage. Because it involves a private key, this full verification process should be done off-line (not via an Internet public data communication channel) and on-site (conducted in an official place controlled by the voting organizer). By using the ID written on the receipt, a search can be done on the repository of ballot ID until it gets the ID of all the ballot sections associated with the receipt. One ID that exactly matches the ID of the receipt will be obtained in plaintext, while the other two ID parts of the ballot are still encrypted. The two IDs are then decrypted using the administrator's private key.

Next three IDs are used to search for three tuple ballots in the e-ballot box. Once obtained, a calculation is done to obtain a 'fingerprint' from a complete ballot. The counting formula is the same as that used to generate the verification code on the receipt (formula 1). The fingerprint is then compared to the existing verification code on the receipt. If the same, then it can be concluded that all parts of ballot are actually stored in the system and its content is the same as when the ballot was first made. If any ballot portion not found in the ballot box or fingerprint is not the same as the verification code, then the voter may file an objection claim to the voting organizer. The next action depends on the voting rules. In some cases it may lead to the necessity of re-voting.

In the full verification process, what is compared is the fingerprint of the entire contents of the ballot (not the contents of the ballot it directly). This is done to keep the privacy of one's choice. If the ballot & receipt generator module and the full verification module work correctly and honestly, then no other party can know the content of a person's choice, even if the other party succeeds in obtaining the receipt of a voter. He can only know that ballots are stored completely and correctly in the system.

To facilitate entry into the system when performing full verification, the receipt and verification codes may be listed on the receipt in the form of a barcode or QRCode.

Based on the evaluation of the original threeballot method with the modified threeballot, it appears that in the verification process, actually when the voter (independently or assisted by others) finds the ballot on the bulletin board whose ID is the same as the ID on his receptor, he has only 1/3 that his voice exists and does not change. He can not be sure that the other two parts of ballot really exist and also do not change. Verification of the original ThreeBallot method we call partial verification. By making some modifications and additions to the ThreeBallot system, a system that makes full verification possible (ensures that three parts of the ballot do exist and remain unchanged). This is done while keeping the aspect of anonymity and privacy not decreasing (or at least only slightly less).

VI. Conclusion

Using ThreeBallot original system, voters can independently verify their votes partially. We have modified ThreeBallot to provide full verification, while at the same time still keep the anonymity and privacy aspect of e-voting system. Full verification can only be done by voters with approval of the voting authority.

References

[1] L. F. Cranor and R. K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet," in *Proceedings of the Hawai`i International Conference on System Sciences*, Wailea, Hawai`i, USA, 1997.

[2] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme For Large Scale Elections," in *Advances in Cryptology - AUSCRYPT ’92*, Gold Coast, Queensland, Australia, 1992.

[3] P. Salini and S. Kanmani, "Application of Model Oriented Security Requirements Engineering Framework for secure E-Voting," in *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, 2012, pp. 1–6.

[4] Z.-Y. Wu, J.-C. Wu, S.-C. Lin, and C. Wang, "An electronic voting mechanism for fighting bribery and coercion," *J. Netw. Comput. Appl.*, vol. 40, pp. 139–150, Apr. 2014.

[5] S. A. Adeshina and A. Ojo, "Design imperatives for e-voting as a socio technical system," in *201411th International Conference on Electronics, Computer and Computation (ICECCO)*, 2014, pp. 1–4.

[6] C. S. Guasch, *Individual verifiability in electronic voting*.: Universitat Polit`ecnica de Catalunya, 2016.

[7] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," in *25th IEEE Symposium on Security and Privacy (S&P)*, 2004, pp. 38–47.

[8] M. J. Moayed, A. A. A. Ghani, and R. Mahmod, "A Survey on Cryptography Algorithms in Security of Voting System Approaches," in *International Conference on Computational Sciences and Its Applications, ICCSA '08*, 2008, pp. 190–200.

[9] R. L. Rivest, "The ThreeBallot Voting System," in *Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology*, 01-Oct-2006.

[10] A. O. Santin, R. G. Costa, and C. A. Maziero, "A Three-Ballot-Based Secure Electronic Voting System," *IEEE Secur. Priv*, vol. 6, no. 3, pp. 14–21, May 2008.

[11] M. R. Koot, *Measuring and predicting anonymity*. Amsterdam: University of Amsterdam, 2012.