

Dual-Authentication Scheme Design in Electronic Voting System

Cheng-Yi Wu, Wu-Chuan Yang, Ming-Haw Jing

Department of Information Engineering

I-Shou University

No.1, Sec. 1, Syuecheng Rd., Dashu Township, Kaohsiung County 840, Taiwan

Abstract. Electronic voting system offers a more efficient and accurate election way than the traditional election. However, the voters do not trust the electronic machine in many important occasions. To increase voter confidence, we propose a dual-authentication scheme. Voters can check and verify the entire election process and results by our scheme. This article combines VVPAT with a new scheme based on confirmation code to achieve the goal of dual-authentication in e-voting system.

Keywords: Electronic Voting, Two-dimensional barcode, QR Code, VVPAT

1. Introduction

To increase voter confidence, the conception of VVPAT (or VVPRS) [1] was proposed. It provides a paper record to let voter verify their vote records. In the United States presidential election of 2008, many states had adopted the DRE with VVPAT to be the voting system [2]. The other well-known voting system is End-to-End (E2E) voting system. It allows voters to verify that their ballots are processed correctly, and let voters can make sure that their votes are counted as intended from cast to the end. In 2008, D.Chaum etc. proposed the Scantegrity [3] and Scantegrity II [4] voting system to enhance the existing optical scan optical system. And in the Scantegrity II voting system, it proposed the confirmation code to satisfy the E2E mechanism.

Because e-voting is not taken effect in Taiwan, we hope to develop a secure and practical system to reduce the dispute of e-voting. In contrast with the traditional paper ballot, QR code could provide an efficient way to preserve the paper ballot in a smaller size. When the election dispute happened, QR code could be used to recount valid votes very efficiently. Consequently, we select QR code to be the major paper audit trail. In this article we take advantage of VVPAT to develop our design scheme, and use QR code to store the required ballot information. When QR code printed, voter can check the content of QR code by using webcam to real-time decode. In order to let voter can verify their vote whether is recorded correctly, we proposed a new scheme based on the confirmation code of Scantegrity II. Our new scheme is designed for the receipt, voter can take this receipt to verify their vote after the close of polls. This article combines VVPAT with a new scheme based on confirmation code to achieve the goal of dual-authentication in e-voting system. We will introduce our system design architecture in the following section.

2. Preliminary

Quick Response Code [5] originated from Japan by Denso Corporation in 1994. QR Code is common in Japan and it is used in a very wide variety of applications such as the bus stop bulletin board, sales applications. QR code is one kind of matrix code (or two-dimensional bar code) that can contain much more data than the one-dimensional bar code, and it also provides the error correction capability to increase the data recovery. There are 40 versions in QR Code, four levels for the error correction capability, and the maximum symbol size can contain 2953 bytes data capacity. Table 1 shows the related data.

Table 1. QR Code Storage

Data capacity (maximum)		Error Correction Recovery Capacity	
Numeric	7089 characters	Level L	7 %
Alphanumeric	4296 characters	Level M	15 %
Byte	2953 characters	Level Q	25 %
Kanji	1817 characters	Level H	30 %

The symbol size of QR code is direct proportion. It increases in steps of 4 modules per side from version 1 (21*21) to version 40 (177*177). In accordance with the required ballot information, we will choose a specified symbol size and error correction level to use.

3. System Architecture Design

We now describe the detail of the dual-authentication scheme. The contributions and advantages can be summarized as follows:

1. Reduce paper cost: In traditional election, the cost of paper ballot is an issue that ignored easily by people. And it is also a problem to preserve a great quantity of paper ballots. For this reason, we choose QR code to be the paper ballot to solve above problems.
2. Security: To make sure the paper ballot is secure and avoid machine cheating, we embed the digital signature into QR code. It can authenticate that the paper ballot is valid or invalid.
3. Immunity to coercion and vote-buying: Voters can check the vote records by the receipt, but can not prove to anyone the real vote.

3.1 Embedded with the digital signature algorithm (DSA)

In our design requirements, we have to consider the symbol size in order to minimum the printing area. And for the consideration of vote record security, we embed the digital signature into the symbol to identify and authenticate the vote records. Before the election, the election official generates a pair key of DSA. The private key is used to generate the signature from data, and the public key is used to verify the validity of signature. The digital signature is generated from the ballot information, and then embeds both into QR code to create the paper ballot. When the voter completes the voting procedure on DRE system, our system generates the QR code embedded with the digital signature. After voter check the content of QR code that is correct, our system will do the printing action automatically. The

procedure shows in Figure 1.

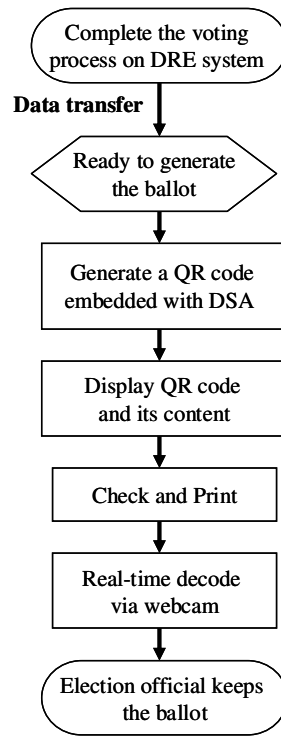


Figure 1. The procedure of QR code generate

3.2 Proposed Scheme

Scantegrity II proposed the confirmation code that enables each voter to verify their vote is recorded correctly. Based on the confirmation code, we proposed a new scheme to provide a verifiability mechanism in our system.

It's very common to use the asterisk (*) to protect the personal privacy such as the personal account, mobile phone bill etc. For example, there is a mobile phone number "0912345678", but it will only show partial numbers such like 09**34**78. This way could keep the personal privacy. Due to the QR code needs some essential plaintexts to display, we apply this conception into integrate QR code and develop a new verifiable scheme as Figure 2. In addition, we add the candidate's number from the ballot information so that voter can directly verify the vote by human eyes.



Figure 2. QR code integrated with the proposed scheme.

3.2.1 Preparation

In our new scheme, each code consists of two parts: the first part A is unique within each candidate on each ballot, and this part is pseudo-randomly generated from a set of possible codes. The second part B is repeatable on each ballot, but it has to be satisfied the uniqueness for each candidate on the same ballot index.

1. Secret table: Before the election, the content of the part A in secret table were generated from PRNG [6]. And the part B was designed for the requirements in check table. Let n be the number of candidates, each row contains n different codes that correspond to each candidate. The same codes can not repeat on the same row, but can duplicate on the same column. Secret table has to keep the secrecy and never published.
2. Random table: Each code on the same ballot index has been pseudo-randomly permuted from the secret table, and each code only displays the first part on the random table. The second part on each code keeps unknown on the random table. Each row contains a flag, which will be raised if the code was selected. The raised flag can be used to check the tally.
3. Check table: After the close of polls, voter can verify their vote by using ballot the part A of new scheme via public bulletin board. Voter will see n different contents of the part B , but voter can not prove to anyone the real vote record.
4. Public table: Each row only reveals the fixed candidate that corresponds to the content of the check table. Therefore, the tally result can be examined by comparing the random table and the public table.

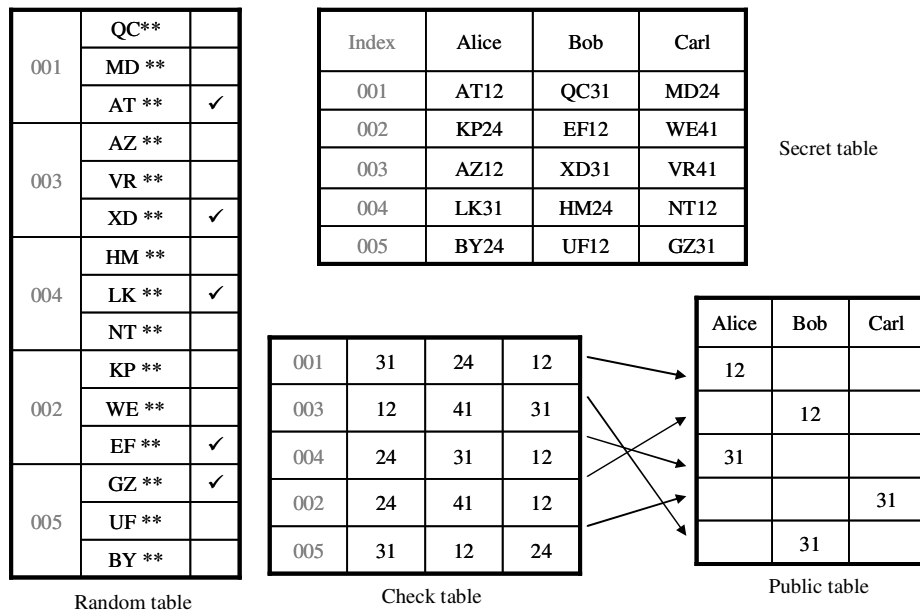


Figure 3. The example of proposed scheme

In Figure 3, we offer an example to explain the procedure of proposed scheme. A voter whose vote is for Alice on ballot 001, the public result would reveal the AT** which is raised on the random table. No one would know the real vote record which hide from the asterisk except the voter himself. Then voter can input the AT** to remind and check the hidden data on public bulletin board (PBB), it will represent as table 2. In the end, voter can check whether the real vote record is recorded correctly on the public table. Furthermore, anyone can compare the random table and public table to examine the tally result.

Table 2. The check table on PBB.

001	31	24	12
-----	----	----	----

4. Discussions

In our proposed scheme, there are some issues we have to discuss.

1. The voting system has to display the exact ballot information, let voter easy to realize the hidden data and keep the secrecy.
2. The voter can choose to participate in the verification process by making a vote receipt. Before enter the voting booth, voter can demand an empty note to transcribe the content of proposed scheme. Afterwards, voter can take this receipt to do the verification process.
3. The result of public table will be affected by the check table. We assume that there are N candidates in this election, and the permutation in check table is selected from a finite set. It is satisfied by the formula: $P(N+1, N)$.
4. For each table, there exists a one to one mapping function. The mapping function should keep its secrecy and can not release the link to anyone.
5. The proposed scheme reduces the negative effect on receipts. Even though attacker (coercer or vote-buyer) gets the receipt, he can't recognize which one is the real vote. If a voter wants to prove his vote record to the attacker, the result of public table will make a confusion that shows in Figure 3.

5. Conclusion

There are many issues that discuss whether it should use the receipts in e-voting system. The receipts not only provide voter a way to check the vote records, but also enhance the voter confidence of e-voting system. However, the receipts could cause an attack by the coercer or vote-buyer. Therefore we propose the dual-authentication scheme to resolve these fraudulent behaviors. Our scheme satisfies the voter verifiability and the universal verifiability in e-voting system. The voter can check whether the vote is recorded as intended, and anyone can check the vote records are counted correctly.

Acknowledgement

This work was supported by a research grant NSC 96-2221-E-214-071-MY3 from the National Science Council of Taiwan.

References

1. N.Ansari, P.Sakarindr, E.Haghani, Chao Zhang, A.K.Jain and Y.Q.Shi. *Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records*. Security & Privacy, IEEE Volume 6, Issue 3, May-June 2008 Page(s):30 – 39.
2. Voting technology state by state. Website: <http://www.computerworld.com/action.do?command=viewArticleBasic&articleId=9115258>
3. D.Chaum, A.Essex, R.Carback, J.Clark, S.Popoveniuc, A.Sherman and P.Vora. *Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting*. Security & Privacy, IEEE Volume 6, Issue 3, May-June 2008 Page(s):40 - 46
4. D.Chaum, R.Carback, J.Clark, A.Essex, S.Popoveniuc, R.L.Rivest, P.Y.A.Ryan, E.Shen and A.T.Sherman. *Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes*. In EVT'08: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2008 on Electronic Voting Technology Workshop.
5. International Standard ISO/IEC 18004. Information technology – *Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification*, 2006.
6. A.Shamir. *How to share a secret*. Communications of the ACM, 22(11):612–613, 1979.