Single Transferable Electronic Voting Protocol for Elections with Barriers

Okan YÜCEL, Nazife BAYKAL

***Abstract*—A secure electronic vote protocol is proposed for the elections having the constraint of discarding the candidates that cannot exceed the barrier. The protocol prevents the loss of votes that remain under a certain threshold by making use of the concept of single transferable voting (STV) as a solution to the problem of exhausted votes. New protocol is very suitably applied to the 'Prêt a Voter: All-In-One' scheme proposed in 2007, with our modification in the tallying phase. We also give details of the cryptographic part and propose two modifications in the ballot construction phase of the 'Prêt a Voter: All-In-One' scheme, which enhances its security. 'Prêt a Voter' scheme, which provides voting receipts without any thread of coercion and ballot-selling is chosen in this work mainly because of its voter verifiability property.**

***Keywords* —Electronic voting, public key encryption, single transferable voting, voter verifiability.**

I. Introduction

LARGE scale elections are starting to be held increasingly by electronic means in various countries. Electronic voting over the Internet or closed networks accessible from voting booths has several advantages over paper based voting, especially in terms of voter verifiability. Arising new protocols for electronic voting are competing with each other and solving the earlier encountered problems such as the confliction between anonymity and voter verifiability.

Voter verifiability is a concept which does not exist in traditional paper-based elections but becomes an important issue of democracy in the electronic world. The idea is to endow each voter with the facility of *verifying that his vote is counted*. The first level of such a verification could be to verify that *his vote is cast correctly* and the second level is whether *his vote is counted (or tallied) correctly*. The check mechanism for the *correct count of the vote* can be provided by means of a voting receipt. On the other hand, whenever one has a receipt that serves to check the correct tallying of the vote, it can also be used as the proof for the content of the vote used in the election. This may in turn lead to voter coercion and ballot-selling. Hence, previous versions of the electronic voting protocols have avoided giving receipts to the voters, and introduced the concept of *receipt-freeness* as an integral part of the voting system. On the other hand, the psychology of voters, who are traditionally used to paper based voting is much more on the side of having something touchable, like a paper in hand, rather than completely relying on the electronic media.

'Prêt a Voter' scheme is an electronic voting scheme, which responds to this psychological need of having the receipt. More importantly, the way that the receipt is constructed provides voter verifiability up to the second level, i.e., each voter can verify that his vote is cast correctly, by means of the receipt that does not tell anything about the content of the vote to anybody except for the voter himself. The second level of verifiability, i.e., the check of *correct tallying of each received vote* is managed by the *universal verifiability* of the overall system. In other words, the robustness, correctness and dependability of the overall system is provable. Prêt a Voter schemes have their origins in the scheme proposed by Chaum [1] in 2004 and developed by Ryan [2] in the same year.

Among different types of voting systems depending on the needs of the particular election, FPTP (First Past The Post), STV (Single Transferable Voting), Condorcet and Borda Count elections are the main ones to be mentioned. The 'Prêt a Voter' scheme proposed by Chaum, Ryan and Schneider [3] in 2005, PAV 2005, and its enhanced form PAV 2006 [4] are easily implemented for FPTP elections; however, they may be complicated for application to STV elections. On the other hand, 'Prêt a Voter: All-In-One' scheme [5] that we call PAV 2007, solves the problem of handling the STV elections efficiently.

In this work, we focus on STV elections and propose a protocol to be applied to large scale elections, in which political parties, whose votes remain below a certain barrier are eliminated. Our proposal prevents the loss of votes used for the eliminated parties and distributes them securely to the second choices of their voters. This protocol is then applied to PAV 2007 scheme, which we suitably modify to enhance the security of the ballot-construction and tallying phases.

In the original STV elections, voters give a preference ranking of the candidates (or political parties) rather than indicating a single choice on the ballot as in FPTP elections. In the first stage of tallying, only the first preference of each

Manuscript received November 10, 2008. This work is a part of the Ph. D. thesis presently being held at the Informatics Institute of Middle East Technical University.

O. Yücel is the co-founder of an information security company, Barikat Bilişim in Ankara (phone: 312-472-2055; fax: 312-472-2056; e-mail: okan.yucel@ bigb.com.tr).

N. Baykal is a professor at the Informatics Institute of Middle East Technical University (e-mail: baykal@metu.edu.tr).

STV ballot is taken into account. If a candidate wins enough percentage of votes to achieve the winning quota, procedure terminates. If not, the votes of the candidate, who takes the least number of votes, are transferred to the other candidates. For that purpose, all ballots, on which the candidate having the least amount of votes are the first choices, are tallied again and the second choices on these ballots are distributed to the corresponding candidates. This procedure is repeated until one of the candidates achieves a vote percentage above the winning quota.

Some large scale elections have barriers (an example is the 10% barrier in Turkish Parliamentary elections), which eliminate the political parties that obtain a vote-percentage below a certain threshold. For preventing the problem of exhausted votes in such cases, we propose the following protocol in the tallying phase of STV elections: As in the original form, each voter indicates a preference ranking of the political parties on the ballot. The first step of tallying is the same, so in the first evaluation of ballots, only the first preference of each voter is taken into account. If all parties get enough votes to exceed the barrier, the tallying phase terminates. If not, in the second step, ballot tallying is repeated for all the voters whose first choice is a loser party that remains under the threshold. The second choice on these ballots is taken into account provided that it is a winning party above threshold. If the second choice is also a loser party, the successive choice on that ballot is used until one of the winner parties is encountered. Unlike the original STV elections, there is no need for repetition of tallying after this step. So, the election rule of eliminating the parties below the barrier is preserved, whereas no vote is exhausted. For the most suitable application, we suggest the use of PAV 2007, with our modification to enhance the security of the ballot-construction and tallying phases; and perhaps by adding blind signatures of all the observers of the parties entering the elections.

In Section II, we present a brief and comparative review of PAV 2005, PAV 2006 and PAV 2007 schemes. Section III discusses our modification in the STV protocol for elections with barriers and applies it to the tallying phase of PAV 2007. The security enhancement that we propose for the ballot construction phase of the PAV 2007 scheme is also given. In Section IV, we summarize our conclusions.

II. Prêt a Voter schemes

We firstly describe the common properties of the Prêt a Voter schemes [3], [4] and [5] in part A; then give a comparative discussion in part B. Part C is devoted to the explanation of the cryptographic core used in 'Prêt a Voter: All-In-One' scheme [5], with vital details which cannot be found in the original reference.

A. *Common Properties of 'Prêt a Voter' Schemes*

Prêt a Voter schemes, PAV 2005 [3], PAV 2006 [4] and PAV 2007 [5] are all voter-verifiable electronic voting schemes, which provide voting receipts without any thread of coercion and ballot-selling. Ballots contain two columns as shown in Fig. 1, say the left column including the candidate names in random order (or alphabetical order simply rotated by a random cyclic shift, say 2 downward shifts as in Fig. 1) and the right column having an encrypted number called 'onion' that is prepared as a function of the random order of candidates on this ballot. In the voting booth, voter marks his vote on the right column and the left column of the ballot on which the candidates are tabulated is removed after voting, as a part of the voting phase. The provided receipt includes only the right column that shows the marked vote and the onion; hence it is meaningless to anybody except the voter himself, who has seen the order of the candidates before the removal of the left column of the ballot.

Demet Diker	X
Efe Ersoy	
Ayşegül Ayaz	
Binnur Bulut	
Cihan Celasun	
	8HbWs6

Fig. 1. Ballot form used by original Prêt a Voter schemes (after voting but before removal of the left column).

There are k tellers (or clerks) of the mix network, each one having two sets of a public/private key pair. Ballots are prepared before the elections and the secret number, which indicates the candidate order on the left column of the ballot is encrypted one-after-another with $2k$ public keys of k tellers to form the onion. To decrypt this onion in the tallying phase, contribution of each teller is indispensable, because each layer of the encrypted onion can only be decrypted by one of the private keys of the corresponding teller. In order to preserve anonymity and break any linkage between the voter and decrypted vote, each teller randomly permutes the output list of ballots before submitting it to the next teller.

Voter verifiability is achieved by means of bulletin boards, which have universally accessible memory, and provide public communication, such that an election authority can write secured, unalterable and undeletable information on it and any other party can read. The receipt containing the right column with voter's mark and the onion will be scanned after voting phase, and published onto the bulletin board by election authorities. Any voter can check for the existence and integrity of his receipt on the bulletin board and make an objection whenever any problem occurs. Perhaps the most attractive part of the Prêt a Voter schemes is that, although the receipts are publicized, nobody except the voter himself is able to understand the content of the vote, unless the onion is decrypted properly. However, decryption of the onion is distributed cleverly to k tellers, who also have to randomly shuffle the ballot lists that they receive, before submitting to the next teller; so that the link between the initial voter and the final tallied vote cannot be tracked unless all tellers are corrupted.

B. *Differences Among ‘Prêt a Voter’ Schemes*

Improvements brought by PAV 2006 over PAV 2005 are,

i) preparation of ballot forms with two onions, the new-left onion on the left column being encrypted by the public key of the voting machine and decrypted by its private key whenever the voter casts his vote,

ii) distributed generation of ballot forms, to enhance the security of ballot generation phase,

iii) on demand-printing of ballots to resist the chain voting attack reported in [6],

iv) size-independence of onion from the number of tellers,

v) separation of shuffle and decryption phases to increase robustness, by first shuffling the received votes by a re-encryption mix network as suggested in [7].

The main improvement brought by PAV 2007 over PAV 2006 is its adjustment according to the needs of preferential elections, such as STV or Condorcet elections. Since each voter makes a ranking of the candidates in preferential elections, the order of the ballot candidate list needs to be totally randomized as in Fig. 2, instead of simply cyclically shifting the same alphabetically ordered list on each ballot. The implementation of previous PAV 2005 and PAV 2006 schemes may be complicated with this constraint, as compared to the implementation of the approval elections like FPTP or Borda Count. PAV 2007 takes care of this problem by treating the ballot as a whole in the ballot tallying phase. It makes use of the Paillier encryption [8] and exploits its homomorphic property in absorbing all ranked choices of the ballot within a single encrypted onion. Ballots are then shuffled by a re-encryption mix network composed of many tellers (or clerks).

Ayşegül Ayaz	5	dBOpTf
Efe Ersoy	3	66rdMv
Demet Diker	1	Abc123
Binnur Bulut	2	7YJLfN
Cihan Celasun	4	Vs68Hb

Fig. 2. Ballot form used by “Prêt a Voter: All-In-One” (PAV 2007) scheme (after voting but before removal of the left column).

C. *Encryption and Decryption by Paillier Cryptosystem*

Brief description of Paillier cryptosystem [8], [9] is needed at this point for making our contribution to “Prêt a Voter: All-In-One” (PAV 2007) scheme understandable. The Paillier algorithm has the additive homomorphic property; that is, an encryption of m_1+m_2 can be obtained from any encryption of m_1 and m_2, as

$$E(m_1, r_1)E(m_2, r_2) \equiv E(m_1+m_2, r_1r_2). \qquad (1)$$

In (1), the ciphertext $c= E(m, r)$ stands for the encrypted form of the plaintext m,

$$c = E(m, r) = g^m r^n \pmod{n^2}, \qquad (2)$$

r is chosen at random, n and g are fixed public elements defined by

- $n = pq$, the modulus where p and q are large primes
- $g \in Z^*_{n^2}$, and a multiple of n

So, the pair (n, g) is the public key, and the pair (p, q) or equivalently λ = LCM (p-1, q-1) is the private key of the Paillier’s algorithm. As a consequence of (1), it is clear that

$$E(m, r)^k \equiv E(km, r^k). \qquad (3)$$

Ballot Construction:

In Fig.2, the numbers on the rightmost are obtained as a result of successive encryptions performed by the clerks of the mix network. The order {1, 5, 4, 2, 3} on the ballot shown in Fig. 2 of the candidates {1: Ayşegül, 2: Binnur, 3: Cihan, 4: Demet, 5: Efe} is chosen randomly by the first clerk. First clerk also picks up the random numbers r_1, r_2,…, r_5 and prepares the encrypted numbers c_1, c_2,…, c_5 showing the candidate placed at each row, using (2) and the public key (n, g). More specifically, the encrypted number that the first clerk prepares for the j’th row is

$$c_j = E(M^i, r_j) = g^{M^i} r_j^n \pmod{n^2}, \qquad (4)$$

where M is any integer greater than the number, v, of candidates, and i=1,2,…,v shows the alphabetical order of the candidate corresponding to that row. Hence, for the example of Fig. 2, the candidate order {1, 5, 4, 2, 3} is reflected directly to the exponents of M as follows

$$c_1 = E(M^1, r_1), \quad c_2 = E(M^5, r_2), \quad c_3 = E(M^4, r_3),$$
$$c_4 = E(M^2, r_4), \quad c_5 = E(M^3, r_5).$$

Each successive clerk of the mix network re-encrypts the numbers c_1, c_2,…, c_5 by multiplying them with the n’th power of a random number t, so that the new value of the ciphertext becomes

$$\tilde{c}_j = c_j t^n = g^{M^i} r_j^n t^n = E(M^i, r_j t). \qquad (5)$$

Equation (5) shows that, the plaintext M^i remains untouched while the random numbers picked by the first clerk are each time multiplied by a different random number t; so that the first clerk, the only person who knows the candidate order, cannot trace the ballot. Since $\tilde{c}_j$ value of the j’th row keeps the message M^i in encrypted form, the number i showing the alphabetical order of the candidate sitting at the j’th row is always preserved and not affected by increasing number of re-encryptions. The numbers on the rightmost of the ballot in Fig. 2 are those $\tilde{c}_j$ values obtained by the last clerk at the end of the ballot construction chain.

Ballot Casting:

The voter casts his vote by ranking, i.e., filling up the numbers 1 to v in the right hand column; tears the ballot apart, destroys the left part and keeps the right part as the receipt after being scanned by the election authority at the voting booth. The scanned receipt is also announced at the web bulletin board for further checks demanded by the voter or any other party.

Ballot Tallying:

After the ballot is ranked by the voter, a single onion for each ballot having v candidates is calculated as follows:

$$E(m,r)=\prod_{i=1}^{v}E(M^{i},r_{i})^{k_i}=\prod_{i=1}^{v}\tilde{c}_{i}^{\,k_i}\ , \tag{6}$$

where k_i's indicate the voter's ranking corresponding to the candidate, who is the i'th one in alphabetical order. In the decryption of this onion, homomorphism of the Paillier algorithm leads to a very useful result:

$$\prod_{i=1}^{v}E(M^{i},r_{i})^{k_i}=E(\sum_{i=1}^{v}k_{i}M^{i},\prod_{i=1}^{v}r_{i}^{k_i})\ . \tag{7}$$

The authority who has the private key (p, q) or equivalently λ = LCM (p-1, q-1) corresponding to the public key pair (n, g), extracts the useful message m in $E(m, r)$ given by (6). Because of the homomorphic property in (7),

$$m=\sum_{i=1}^{v}k_{i}M^{i}\ ,\quad \text{and since } M>v, \tag{8}$$

retrieval of all choices of the ballot becomes possible. Because from (8) it is clear that (m / M^{v}) equals k_v, the {remainder of m/ M^{v}} divided by $M^{v\text{-}1}$ equals $k_{v\text{-}1}$; and the remainder after dividing by $M^{v\text{-}1}$, again divided by $M^{v\text{-}2}$ gives $k_{v\text{-}2}$ and so on.

Example: In Fig. 2, the candidate order {1, 5, 4, 2, 3} during the ballot construction is reflected to the subscript i of k_i's, as {k_1, k_5, k_4, k_2, k_3} and the voter's choice on the ballot shows that k_1=5, k_5=3, k_4=1, k_2=2, k_3=4.

If M (>v=5) is chosen as 7, the following useful message m is obtained from (8).

$$m=\sum_{i=1}^{v}k_{i}M^{i}=5\times 7^{1}+3\times 7^{5}+1\times 7^{4}+2\times 7^{2}+4\times 7^{3}$$

So, m divided by 7^5 gives k_5=3, hence we understand that the alphabetically 5'th candidate Efe is the third in the list of the voter,

Rem{m/7^5}/7^4 gives k_4=1,

which shows that the alphabetically 4'th candidate Demet is the first choice of the voter,

Rem{Rem{m/7^5}/7^4}/7^3= k_3 = 4 , so Cihan is his 4'th choice,

Rem{Rem{Rem{m/7^5}/7^4}/7^3}/7^2 = k_2 = 2, so Binnur is the 2'nd, and finally, Ayşegül is the last choice of the voter since Rem{Rem{Rem{Rem{m/7^5}/7^4}/7^3}/7^2}/7 = k_1 = 5.

III. A NEW PROPOSAL

Large scale elections having vote-barriers such as the 10% barrier of Turkish Parliamentary elections eliminate the political parties, which obtain a vote-percentage below that threshold. People who vote for these parties feel a kind of injustice because of the invalidity and final loss of their votes.

On the other hand, STV elections in which each voter gives a ranked list of preferred political parties may be an excellent and democratic solution to the problem of exhausted votes. In the following, we propose an e-voting application for the elections having such barriers; first by modifying the STV protocol and then applying it to the "Prêt a Voter: All-In-One" (PAV 2007) scheme accordingly. Finally we propose two modifications in the ballot construction phase of PAV 2007, to enhance its security.

Modification of the STV Protocol:

Each voter gives a preference order (of say political parties entering the elections) on the ballot and the tallying phase of the applied voting scheme is modified as follows:

1) In the first evaluation of ballots, only the *first preference* of each voter is counted. If all parties get enough votes to exceed the barrier, the tallying phase terminates.

2) If not all the parties pass the barrier, calling the parties above the threshold *winners* and those below the threshold *losers*, ballot tallying is repeated for all the loser ballots having a loser party as the first choice. The choice on the ballot that is counted this time is the winner party, which is on top of all other winners in the voter's preference list. The new ballot-counts are added on the votes gained by *winners* in part (1) and the tallying phase terminates.

The above protocol preserves the election rule of eliminating the parties below the barrier, whereas no vote is exhausted and citizens are satisfied. The protocol should be accompanied by a secure control mechanism to publicly assure the robustness of the used scheme. To achieve this goal, observer teams assigned by each political party may play critical roles for increasing the robustness and accuracy of the voting scheme.

Application to "Prêt a Voter: All-In-One" (PAV 2007) Scheme and Enhancement of Its Security

The tallying phase of the PAV 2007 scheme [5], which is inherently very suitable for preferential elections can be easily modified according to the STV protocol suggested above. We strongly predict that such an e-voting scheme may become an indispensable alternative for paper-based elections, if the security of the overall system is enhanced. The weakest point in ballot-construction phase of the PAV 2007 scheme seems to be the over-dependence on the first clerk, who decides on the random candidate order of the ballots. He chooses this random order, and encrypts it by using random seeds for each row of the ballot and the public keys of the election authority, who is responsible for tallying the votes. The re-encryptions performed by the following clerks in the network has the purpose of obscuring the path that the ballot follows. We propose at this point to enhance the security of the system by holding the first clerk in the chain more responsible of the encryption he performs, say by including his digital signature (or blind signature) as a part of the encrypted information, which may be checked whenever a need occurs. Such a modification increases the robustness of the scheme since any corrupted behavior is known to be traceable even in the future.

The second modification that we propose to enhance the security is in the re-encryption equation (5) that is used by the other clerks of mix network,

$$\tilde{c}_j = c_j t_j^n = g^{M^i} r_j^n t_j^n = E(M^i, r_j t_j) \qquad (9)$$

in which we change the random number t by a row dependent random number t_j, so that each clerk in the network generates v (number of candidates and ballot rows) random numbers for each ballot, rather than a single one. The use of v random numbers by each clerk (or teller), will make the path more invisible and difficult to catch by the first clerk, who generates the crucial random ordering of the candidates on the ballot.

IV. Conclusion

The voter-verifiable e-voting scheme, 'Prêt a Voter: All-In-One' proposed in 2007 (so called PAV 2007 in this paper) [5], which supports single transferable voting (STV) seems to be a very suitable option for the elections having vote-barriers as in the Turkish Parliament elections. We modify STV elections protocol and the tallying phase of PAV 2007 accordingly. We then propose two modifications in the ballot construction phase of PAV 2007, to increase the security and the robustness of the overall system. The analysis we present for the cryptographic part of PAV 2007 is more detailed and inclusive than given in the original paper [5].

References

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

[2] P. Y. A. Ryan, "A Variant of the Chaum Voter-Verifiable Scheme," *Technical Report of University of Newcastle*, CS-TR:864, 2004. Also in *Workshop on Issues in the Theory of Security*, WITS 2005.

[3] D. Chaum, P. Y. A. Ryan, and S. Schneider, "A practical, voter-verifiable election scheme," *Technical Report of University of Newcastle*, CS-TR: 880, 2005.

[4] P. Ryan, and S. Schneider, "Prêt a Voter with re-encryption mixes," *Technical Report of University of Newcastle*, CS-TR:956, 2006.

[5] Z. Xia, S. Schneider, J. Heather, P. Ryan, D. Lundin, R. Peel and P. Howard, "Prêt a Voter: All-In-One," *IAVoSS Workshop On Trustworthy Elections (WOTE 2007) ,University of Ottawa, Ottawa, CANADA,* June 20 - June 21, 2007.

[6] P. Ryan and T. Peacock, "Prêt a Voter: a system perspective," *Technical Report of University of Newcastle, CS-TR:929*, 2005.

[7] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," *in Proc. 8'th ACM Conference on Computers and Communications Security*, CSS'01, pp. 116–125, 2001.

[8] P. Paillier, "Public-key cryptosystems based on discrete logarithm residues," *Advances of Eurocrypt'99,* LNCS 1592, pp. 223–238, 1999.

[9] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," *Proc. Eurocrypt'99*, LNCS 1592, pp. 223–238, 1999.