A practical election scheme using the Guy Fawkes protocol and paired chaining publication

Jong-Hyeon Lee

Cambridge University Computer Laboratory
Pembroke Street, Cambridge CB2 3QG
jhl21@@cl.cam.ac.uk

Abstract. In view of their construction, digital election schemes are classified in two types. The one is based on anonymous channels and the other is based on number theoretic encryption techniques. In this paper, we present a hybrid scheme with has functions and paired chaining publication, which is a variation of anonymous channels. The Guy Fawkes Protocol supports an alternative of digital signature scheme using only hash function. With the Guy Fawkes protocol and a publication method, our election scheme achieves low complexity and resource consumption; this scheme aims at low computational load, high voter's privacy, untraceability of voters and universal verifiability of ballots.
Keywords: digital election, the Guy Fawkes Protocol, paired chaining publication, hash, anonymous channel.

1 Introduction

Most of digital election schemes which have been studied are based on public key cryptosystem and each voter should have his/her own private/public key pair. At the time of verifying a digital signature, the verifier must be sure that the public key which s/he uses for the verification of the signature is the public key of the supposed signer. To reduce the difficulty of this problem, the third party, so-called certification authority, is adopted. The procedure and structure of election scheme using public key cryptosystem become more complex. The computational burden is also huge.

Sako and Kilian classified election scheme by use of anonymous channels [13]. The one is a scheme based on anonymous channels, and the other is a scheme based on number theoretic technique for encrypted communication without anonymous channels and mixers. The former is efficient and flexible to adopt and has been originally proposed by Chaum [3]. The latter has desirable security properties but its communication complexity is high. This type of the scheme has been proposed and developed by Cohen and Fisher [5], and Benaloh and Yung [2]. Fujioka *et al.* pointed out that this type is not practical for a large-scale elections because of a lot of communication load [7].

In this paper, we present a hybrid scheme with hashed communication flow and the anonymous channel-like feature. To simplify the structure and reduce

communication burden, especially voters' burden, we used a anonymous channel-like feature with hash function. To reduce computational load, we adopt a scheme based on hashed communication. We only require two private/public key pair around whole structure. Our scheme aims low complexity of structure, less computational load for voters, privacy of voter and untraceability for votes, protection for double voting, and universal verifiability.

Efficiency and complexity of structure The structure of election scheme should not be complex for practical implementation, that is, the round complexity should be simple and communication cost should be low. The phases in the scheme also should be simple and clear. For large scale ballot, whole structure should be designed efficiently.

Computation load Computational load for confidential communication should be low. Especially, voter's load should be low. Voters can cast their vote and compute messages easily under simple computing environment such as PCs or NCs.

Privacy and untraceability All votes must be secret and others cannot guess someone's vote. It is a requirement of secret ballot. Even though principals can co-operate and can exchange information each other, the relation between a voter and his/her vote is kept hidden. This scheme does not allow principals to trace votes and voters by use of blind signature and paired chaining publication.

Protection for double voting Any voter cannot vote twice. It is the first requirement for digital election scheme. In our scheme, it is checked in each phase.

Eligibility No one who is not allowed to vote can take part in a ballot. If there is any authority in the scheme, each authority has to be able to protect non-eligible voting.

Universal verifiability Every action by a voter, whether initialising a vote, actual voting, or publishing a vote, is verified by proof that the ballot is correctly constructed. Also, anyone can convince that the published final tally is computed fairly from the ballots that were correctly cast.

2 Cryptographic primitives

Cryptographic protocols or techniques used in our scheme are the Guy Fawkes protocol, blind signature, and paired chaining publication.

2.1 The Guy Fawkes protocol

RJ Anderson *et al.* proposed efficient signature scheme named the Guy Fawkes protocol [1]. It is an alternative signature scheme using only hash function and publication procedure.

Basic procedure of the Guy Fawkes protocol is as follows:

1. Select a random codeword X.

2. Form its hash $Y = h(X)$, where h is a hash function.
3. Construct a message M = *"We are the free Jacobin army and we are going to blow up the Houses of Parliament on the 5th November. The codeword by which we will authenticate ourselves afterwards will be the preimage of Y"*
4. Compute $Z = h(M)$ and post it to bulletin boards.
5. Blow up the Houses of Parliament.
6. Reveal M

2.2 The blind signature

In our scheme, we use Chaum's classical blind signature scheme [4]. The major property of blind signature is untraceability, that is, the requester can protect the signer from tracing the relation between the signing process and the signature which will be publicised.

RSA blind signature that we used is as follows: Let M be a message to be signed and S is signature of M.

1. The requester sends $M^{'} = MR^{e} \pmod N$, where (e, N) is the public key of the signer and R is a random number chosen by the requester with $(R, N) = 1$,
2. Receiving the message $M^{'}$, the signer generates $S^{'} = (M^{'})^{d} \pmod N$ with signer's private key d. Then the signer sends the message $S^{'}$ back to the requester.
3. The requester can obtain desired signature S from $S^{'}$ by computing

$$S = S^{'}R^{-1} \pmod N = M^{d} \pmod N$$

The signer cannot derive M from $M^{'}$ since $M^{'}$ is chosen by the requester at random.

2.3 The paired chaining publication

This technique is used for publication of votes protecting other principals from tracing relation between publicised vote and voter.

This procedure is used between publication boards PB_i and ballot boxes BB_i. Anyone can read list of published entries in PB_i, but the entries in BB_i are kept with secret until the end of the ballot.

Voter casts a vote v_k and generates nonce N_0 for vote verification in BB_i. For chaining between PB_i and BB_i, the initial identifier for the hash is needed. Let's say P. The procedure of the paired chaining publication is as follows.

1. Voter publishes hash $h(v_k|N_0)|P$ with P to PB_1 and submits vote verifier $N_0|P$ with P.
2. Receiving the hash with initial identifier P, PB_1 generates nonce N_1 and calculates $h(h(v_k|N_0)|N_1)$ and $P \oplus N_1$. Then PB_1 concatenate them and publishes $h(h(v_k|N_0)|N_1)|P \oplus N_1$ in a lexicographical order. PB_1 also sends $N_1|P$ to BB_1.

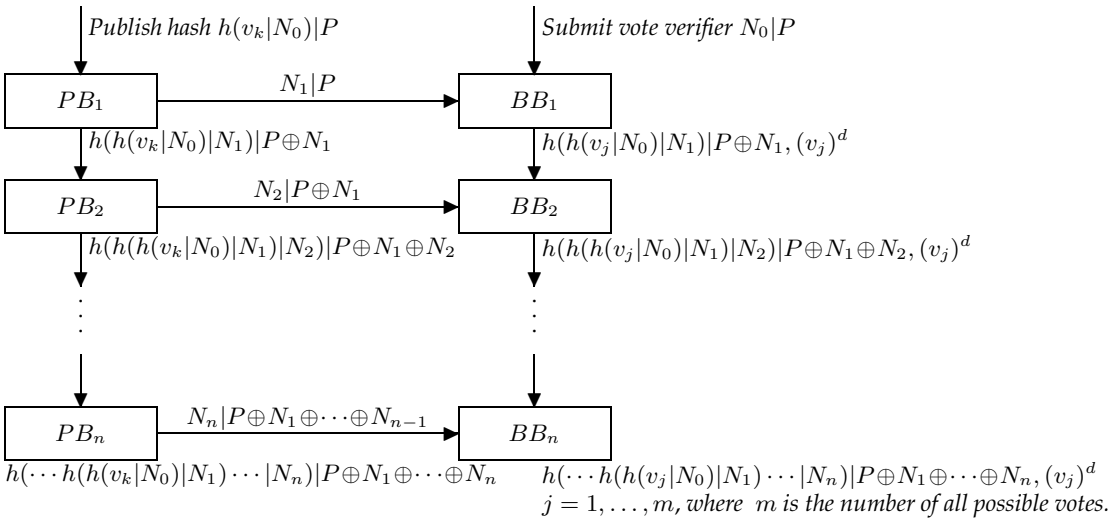

Fig. 1. Paired Chaining Publication

3. Receiving $N_1|P$ from PB_1, BB_1 searches $N_0|P$ using P as a searching key, and calculates $h(h(v_j|N_0)|N_1)$ where $j = 1,\ldots,m$ and m is the number of all possible votes. If this ballot is a yes/no ballot, m will be 2. BB_1 then sends $h(h(v_j|N_0)|N_1)|P \oplus N_1,(v_j)^d$ to BB_2, where $(v_j)^d$ is a signed vote value.
4. After publication of the list in PB_1, PB_2 fetches entries in the list and repeat procedure 2.
5. Receiving $h(h(v_j|N_0)|N_1)|P\oplus N_1$ from BB_1, BB_2 repeats procedure 3.
6. Repeat procedure 4 and 5 through PB_n and BB_n.
7. At the end of the ballot, BB_n matches entries in its list by referencing the list of PB_n, and counts votes.

This paired chaining publication can provide similar effect of anonymous channels. If at least one PB_i is honest, the correspondence between voter and his vote is kept secret.

3 Proposed election scheme

We now describe our election scheme. We use three primitives: registration office RO, publication board PB_i, ballot box BB_i. To construct paired chaining publication mechanism, multiple publication boards and ballot box are used. In order to guarantee uniqueness of identifiers, we assume that hash function used in this scheme is collision-free, and every nonce is chosen as an large enough random number.

In our election scheme, there are four phases: initialisation phase, registration phase, voting and publication phase, and counting phase.

Let $\{ (e_R, N_R), d_R \}$ and $\{ (e_B, N_B), d_B \}$ be the public/private key pairs of registration office and the first ballot box, respectively.

Initialisation phase

1. Voter generates random numbers r as a blind factor and P as a pseudonym. Since the pseudonym will be an identifier, it must be chosen large enough at random.

Registration phase

1. Voter sends $\{ P \cdot r^{e_R}$, name $\}^{e_R}$ to registration office.
2. Registration office stores name and $P \cdot r^{e_R}$, and checks duplication of registration. If it is not duplicated, registration office signs on $P \cdot r^{e_R}$ and send it back to voter. Otherwise, registration office informs voter of duplicated registration.
3. Voter remove blind factor from $(P \cdot r^{e_R})^{d_R}$, and obtains P^{d_R}.

Voting & publication phase

1. Voter casts a vote v_k where $1 \leq k \leq m$ and m is the number of all possible votes.
2. Voter generates a random number N_0 for vote verification.
3. Voter publishes $h(v_k|N_0)|P^{d_R}$ to PB_1.
4. Voter also submits vote verifier and signed pseudonym $N_0|P^{d_R}$ to BB_1 which is encrypted by the public key of BB_1.
5. Each of PB_1 and BB_1 checks the signature of registration office and duplication of publication or submission of a vote. If the signature is compromised, each principal rejects publication or submission.
6. Between PB_1 and BB_1, paired chaining publication is processed.

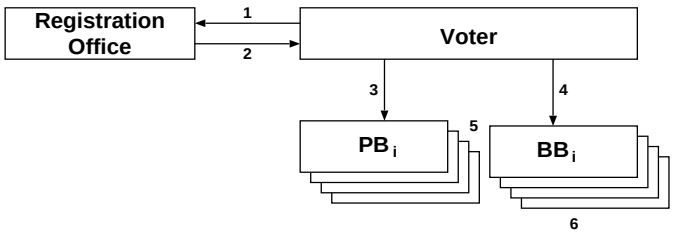

Fig. 2. Brief flow of our election scheme

Counting phase

1. At the end of the ballot, BB_n counts votes by referencing the list of published entries in PB_n.

Fig. 2 shows brief flow of our election scheme. Initialisation phase is performed by voter, registration phase is done between voter and registration office (procedure 1 and 2), and voting & publication phase is done between voter and the first publication board & the first ballot box (procedure 3, 4, and 5). Finally, counting phase is done by the last ballot box (procedure 6).

4 A model for distributed election

In real world, general elections such as the Presidential election or ballot for the promised referendum on the European single currency, are held in whole around the country. For these election or online democracy, a distributed digital election scheme is necessary. In this section, we will adopt our scheme for these distributed wide-area environment and will also consider efficiency of the scheme such as communication frequency, voter's computation load, each authority's database access load, and so forth.

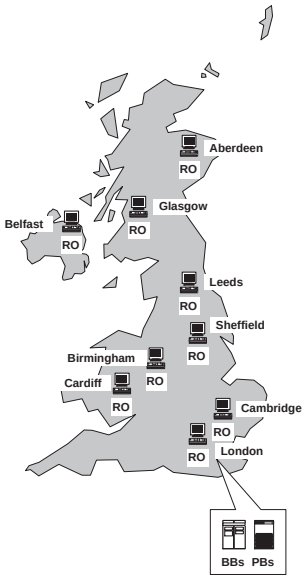

Fig. 3. Configuration of the Voting Network in the U.K.

Fig 3 respresents a configuration of the digital election system over the U.K. We recommend that SuperJANET network [16] as a networking environment

for this configuration. Since SuperJANET has wide-range of coverage and supports high speed networking, it can be a proper candidate for infrastructure of the digital election system. SuperJANET connects registration offices and publication box-ballot box pairs.

The connection between registration offices and voters is an ordinary telephone line. Each voter uses its PC with modem or NC for the connection. You may use specially designed set-top box for the election.

In this configuration, registration offices are scattered over whole country and the position of the office is considered by the number of population, size of area to be covered by an office, and the position of SuperJANET centers.

In the Greater London, East Anglia, and Middle England, since the population of these area is dense, several registration offices are allocated. In Wales and Northern Ireland, the population is sparser than above area but these area is geographically not so close to other registration office. Then there is one registration office in each area. In Scotland, most population reside in Glasgow and Edinburgh, then one registration office is allocated for these area. Since the area of the northern territory of Scotland and islands is wide, one registration office is allocated in Aberdeen, although the population of this area is much sparser than other area.

For integrity of database in publication boxes and ballot boxes, there is unique publication box-ballot box chain in London. To reduce congestion of publication or verifying process, you may consider that each registration office can route each voter's publication or verifying message to the chain of publication box-ballot box.

5 Evaluations

Based on our aims described in the introduction, we evaluate and criticise our scheme.

5.1 Efficiency and complexity of structure

Our scheme requires three types of principals: registration office, publication board, ballot box. Voters communicate with these principals just one transaction per principal.

There are four phases: initialisation phase, registration phase, voting and publication phase, and counting phase. Since the structure and procedure in each phase are simple, this scheme is easy to implement and is suited for environment with massive voters.

5.2 Computation load

Most of computation used in this scheme are based on hash calculation and nonce generation. One blind signature using public key cryptosystem is needed in registration phase. Full computational load of this scheme is less than schemes

based on public key cryptosystem. Especially, each voter's burden is extremely less than other kinds of schemes.

5.3 Privacy and untraceability

Using blind signature and paired chaining publication, the relation between voter and its vote can be kept secret and no vote can be traced back even though authorities such as registration office, publication boards, and ballot boxes are collaborating. During the chaining process, submitted published hash values and vote verifiers are completely shuffled.

5.4 Protection for double voting

At first, the registration office checks duplication of registration request whenever it receives the request from a voter. The first publication board and the first ballot box check the duplication of published values and vote verifiers. When a duplication is revealed, the authority informs the voter of the duplication, and requests a retrial or administrative procedures. After detecting a duplication, handling of the case depends on the policy.

5.5 Eligibility

When voters register to registration office, the office checks validity of voters. If they are valid, they can get a signed pseudonym by registration office, otherwise they are rejected. In our scheme, the voter is just verified by voter's name and it can be not practical in real model. In real model, face-to-face verification can be used as usual.

5.6 Universal verifiability

By sending the same publication message to the publication board, a voter can verify that its vote has been included in the tally. In our scheme, since the verification procedure of vote is based on the secret of each voter, a voter cannot verify that others' votes have been in the tally, but s/he can check the total number of participants.

6 Conclusion

This paper proposed a digital election scheme based on hash functions and the paired chaining publication. It uses the Guy Fawkes Protocol for secret communication and the publication of votes. This scheme achieves low complexity of structure, low computational load, privacy of voters, untraceability and universal verifiability of ballots.

References

1. RJ Anderson, B Crispo, J-H Lee, C Manifavas, and RM Needham, "The Guy Fawkes Protocol", Submitted to Crypto 97.
2. JC Benaloh and M Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters", *Proceedings of the 5th Annual ACM Symposium on Principles of Distributed Computing*, 1986, pp 52-62.
3. D Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of ACM* **24**(2), 1981, pp 84-88.
4. D Chaum, "Blind Signatures for Untraceable Payments", *Advances in Cryptology - Crypto '82*, Plenum, 1982, pp 199-203.
5. J Cohen and M Fisher, "A Robust Verifiable Cryptographically Secure Election Scheme", *26th Annual Symposium on Foundations of Computer Science*, IEEE, 1985, pp 372-382.
6. R Cramer, M Franklin, B Schoenmakers, and M Yung, "Multi-Authority Secret-Ballot Elections with Linear Work", *Advances in Cryptology - Eurocrypt '96*, Springer-Verlag, 1996, pp 72-83.
7. A Fujioka, T Okamoto, and K Ohta, "Practical Secret Voting Scheme for Large Scale Elections", *Advances in Cryptology - Auscrypt '92*, Springer-Verlag, 1992, pp 244-251.
8. ID Hill, "Some Aspects of Elections – to Fill One Seat or Many" *Journal of Royal Statistical Society*, Royal Statistical Society, 1988, pp 243-275.
9. W-S Juang and C-L Lei, "A Collision-free Secret Ballot Protocol for Computerized General Election", *Computer & Security*, **15**(4), 1996, pp 339-348.
10. V Niemi and A Renvall, "Cryptographic Protocols and Voting", *Results and Trends in Theoretical Computer Science*, LNCS 812, 1994, pp 307-316.
11. C Park, K Itoh, and K Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", *Advances in Cryptology - Eurocrypt '93*, Springer-Verlag, 1993, pp 248-259.
12. B Pfitzmann, "Breaking an Efficient Anonymous Channel", *Advances in Cryptology - Eurocrypt '94*, Springer-Verlag, 1994, pp 332-340.
13. K Sako and J Kilian, "Secure Voting Using Partially Compatible Homomorphism", *Advances in Cryptology - Crypto '94*, Springer-Verlag, 1994, pp 411-424.
14. K Sako and J Kilian, "Receipt-Free Mix-Type Voting Scheme", *Advances in Cryptology - Eurocrypt '95*, Springer-Verlag, 1995, pp 393-403.
15. GJ Simmons and D Holdridge, "Forward Search As a Cryptanalytic Tool Against a Public Key Privacy Channel", *1982 IEEE Symposium on Security and Privacy*, IEEE, 1982, pp 117-128.
16. `http://www.ja.net`, SuperJANET WWW site.