A Simple Protocol for Yes-No Electronic Voting

A.B. Cabello Pardos†, A. Hernández Encinas†, S. Hoya White†, A. Martín del Rey†† and G. Rodríguez Sánchez†††

†E.T.S.I.I. de Béjar, Department of Applied Mathematics, Universidad de Salamanca, Avda. Fernández Ballesteros 2, 37700-Béjar, Salamanca, Spain
††E.P.S. de Ávila, Department of Applied Mathematics, Universidad de Salamanca, C/ Hornos Caleros 50, 05003-Ávila, Spain
†††E.P.S. de Zamora, Department of Applied Mathematics, Universidad de Salamanca, Avda. Requejo 33, 49022-Zamora, Spain

Summary
The present work exposes a new protocol of electronic voting based on the bit operation XOR and the use of blind signatures. Specifically it is an algorithm designed expressly for the case in which is necessary to choose between two candidates or two options. It is shown that the proposed algorithm satisfies the more important requirements of any e-voting scheme: anonymity, completeness, correctness and uniqueness.

Key words:
Electronic vote, cryptography, blind signatures.

1. Introduction

The great expansion of Internet use, as in its implantation as in the services offered through it, allows the user to carry out a lot of tasks of all kind: electronic trade, teleworking, databases enquiries, etc. Furthermore, the different governments and public administrations have been implied in this development and have put at citizens' disposal new services that have been called e-government (or electronic government). With this suggestive denomination is made a reference to more or less sophisticated services offered by the Public Administration designed to facilitate the business citizen-administration. So, between them, we can find from the simplest systems that provide access exclusively to the information (scholarships information, etc.) until the most sophisticated systems of on line attention that allow to replace the proceedings carried out in person for proceedings carried out in a telematic way: presentation of the rent declaration, payment of taxes, enrollments, etc. In this way, our society spreads to implant in the electronic environment all those performances that the citizens habitually develop and among them it can stand out the civic participation in the taking of decisions (e-democracy or digital democracy) through what has been called the electronic vote.
The minimum requirements that every outline of electronic voting should satisfy are the following ones:

- Anonimity: It should be impossible to link the ballot with the voter which casts it.
- Completeness: Only the elegible voters are allowed to vote.
- Uniqueness: Each legal voter can vote only once.
- Correctness: Each voter should can to check that the own vote has been considered appropriately.

So far several electronic voting protocols have been appeared in the literature (see, for example, [1, 2, 3, 6, 7, 8, 9, 11, 12, 13, 14]). Basically, the great majority is based on the use of three cryptographic primitives: mixnets, blind signatures and homomorphic encryption.

Mixnets are similar to the anonymous channels that are used to distribute among the voters, in an anonymous and sure way, the credentials (digital certificates, etc.). In a more rigorous way, we can say that it is third trusted party that distributes messages among the voters in such a way that possible attackers are not able to determine the sender or receiver of a certain message. The use of the mixnets was proposed by Chaum (See [4]).

Blind signatures were initially used to design the first e-cash protocols. Later, they were used by Fujioka et al. (See [10]) to validate ballots in an electronic electoral outline. Roughly speaking, blind signatures schemes allow an authority to sign digitally some data (for example the ballot of a voter) without knowing the content of this data. As in the previous case, blind signatures were introduced by Chaum (See [5]).

The homomorphic encryption was proposed by Cramer et al. (See [7]) and it takes advantage of the characteristic properties of the homomorphic encryption to provide verifiability to the electronic vote schemes without contributing any information on the individual votes. In the homomorphic encryption model there are two operations: A sum, $\oplus$, defined in the space of messages (votes), and a product, $\otimes$, defined in the space of the cryptograms (ciphering votes), in such a way that the product of two ciphering votes, $E(v_1)\otimes E(v_2)$, is the cryptogram of the sum of such votes: $E(v_1 \oplus v_2)$.

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

The present work exposes a new and simple protocol for electronic voting based on the use of blind signatures schemes. In this protocol the voters can choose between two candidates or options. It also satisfies the main necessary requirements of security: anonymity, completeness, correctness and uniqueness.

The rest of the work is organized in the following way: In section 2 and introduction to blind signatures schemes is made; the proposed protocol of electronic voting is shown in section 3. In section 4, the properties of the mentioned protocol are studied and, finally the conclusions and the future work are shown in the section 5.

2. Blind digital signature schemes

Blind signature schemes are bipartite cryptographic protocols between a user, *V*, and a signer, *U*, in such a way that *U* signs a message sent by *V* without knowing the content of such data.
The main purpose of this type of cryptographic protocols is prevent ths signer U from observing the message it signs and the signature. Every protocol of blind digital signature requires the presence of the following components:

1. A protocol of digital signature that is developed by the signer *U*, such that *S*(*m*) denotes the signature of the message *m*.
2. Two functions, *f* and *g*, known only by the sender *V*, in such a way that: $g\,(S\,(f\,(m))) = S(m)$

The function *f* is called the blinding function, while the function *g* is the unblinding function. In the present work we will use the blind signature protocol based on RSA cryptosystem and developed by D. Chaum (see [5]). This consists of the following: Let $n = p \cdot q$ be the product of two sufficiently large random primes. The digital signature protocol used by the signer *U* is the RSA digital signature scheme with public key (*n*, *e*) and private key *d*. Let *k* be a fixed integer random number such that $gcd(n, k) = 1$. The blindign function is:

$$f : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$m \mapsto f(m) = m \cdot k^e \pmod n$$

whereas the unblinding function is:

$$g : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$m \mapsto g(m) = k^{-1} \cdot m \pmod n$$

Note that it is:

$$g(S(f(m))) = g(S(mk^e \pmod n))$$
$$= g(m^d k \pmod n) = m^d \pmod n = S(m).$$

The protocol of blind signature is like this:

1. **Initialization phase**. Let $0 \le m \le n - 1$ be the message originated by *V* that should be signed by *U*, and set *k* an integer random number selected by *V* such that $0 \le k \le n - 1$ and $gcd\,(n, k) = 1$.

2. **Blinding phase**. *V* computes:
$$m^* = f(m) = mk^e \pmod n,$$
and sends this to *U*.

3. **Signing phase**. *U* computes
$$s^* = S(m^*) = (m^*)^d \pmod n,$$
and sends this to *V*.

4. **Unblinding phase**. *V* computes
$$s = S(m) = g(S(m^*)) = k^{-1}s^* \pmod n,$$
that is the digital signature of the message *m* by *U*.

3. Electroning voting protocol

In this section we will introduce the electronic voting protocol developed. For the construction of votes we will use the bit operation XOR, while its validation is obtained by means of a blind signature scheme. There are four parts implied in our scheme:

- **Voters**: V_1, V_2, …, V_N. They are the main actors of any electoral process. Every voter must emit one and only one anonymous vote that is assessed correctly by the pertinent authorities.
- **Authority of certification**: U_0. It is a third trusted party whose mission is to provide digital certificates to the legitimate voters registered and to carry out the blind digital signatures of the votes.
- **Authority of authentication**: U_1. It is a third trusted party whose mission is to authenticate the registered voters and to provide them of the necessary tools to emit their vote in a proper way.
- **Authority of collection**: U_2. It is a third trusted party responsible for collecting votes, to verify its validity, to store them and finally to carry out the recount of them. It is, therefore, the only entity that has permission for the deciphered of the votes.

The proposed protocol is as it follows:

1. The authority of certification U_0 emits a digital certificate to each one of the legal registered voters.
2. Each voter V_i is identified by the authority of authentication U_1, which validates its digital certificate and sends a random sequence of bits $B_i \in \mathbb{F}_2^N$ to the voter.
3. Each voter V_i constructs his/her vote, $v_i \in \mathbb{F}_2^N$, as follows:
   - If V_i votes for option 1, then:
     $$v_i = B_i \oplus \left(0,\ldots,0,\overset{i\text{-th bit}}{1},0,\ldots,0\right).$$
   - If V_i votes for option 2, then:
     $$v_i = B_i \oplus \left(0,\ldots,0,\overset{i\text{-th bit}}{0},0,\ldots,0\right).$$
4. Each voter V_i randomly chooses a bit sequence $C_i \in \mathbb{F}_2^N$ and computes: $P_i = v_i \oplus C_i$.
5. The authority U_0 makes the blind signature of P_i, P_i^*, and returns it to V_i, which obtains, when recovering it, $S(P_i)$.
6. Each voter V_i sends to the authority U_0 the bit sequence $C_i \in \mathbb{F}_2^N$.
7. Each voter V_i sends to the authority U_2 his/her vote signed by U_0: $S(P_i)$.
8. The authority U_0 computes:
   $$C = C_1 \oplus C_2 \oplus \ldots \oplus C_N \in \mathbb{F}_2^N$$
   and sends it to the authority U_2.
9. The authority computes:
   $$B = B_1 \oplus B_2 \oplus \ldots \oplus B_N \in \mathbb{F}_2^N$$
   and sends it to the authority U_2.
10. The authority U_2 verifies the validity of the different votes deciphering $S(P_1),\ldots,S(P_N)$, obtaining $P_1,\ldots,P_N$.
11. The authority U_2 computes:
    $$P = P_1 \oplus P_2 \oplus \ldots \oplus P_N,$$
    $$P \oplus C = v_1 \oplus v_2 \oplus \ldots \oplus v_N = v.$$
12. The authority U_2 calculates the number of votes obtained by option 1 simply computing the Hamming distance of bit sequences v and B. That is:
    Number of votes of option 1: $d_H(v,B)$,
    Number of votes of option 2: $N - d_H(v,B)$.
13. Finally, the authority U_2 publishes the bit sequences $P_1,\ldots,P_N$ together with C.

Note that to compute the blind digital signature of P_i, each voter has to choose a random integer number, k_i, such that $0 \le k_i \le n-1$ and $\gcd(k_i,n)=1$. Moreover V_i should transform the bit sequence P_i into an integer number m_i such that $0 \le m_i \le n-1$, which is obtained immediately considering its decimal expression. If N is greater than the bit length of the public key n, then it is necessary to break P_i into many pieces of lesser bit length.

4. Analysis of the properties of the proposed protocol

In this section we will verify that the protocol previously proposed satisfies the main indispensable requirements to any electronic vote scheme.

- **Anonymity**. None of the three authorities that participate in the electoral process can determine the vote of a voter V_i. The authority of certification U_0 knows the bit sequence C_i but it is impossible to determine v_i because he doesn't know B_i. The authority of authentication U_1 only knows the bit sequence B_i and consistently any forecast on the vote of V_i will not have a probability over 0.5. Finally, the authority of recollection U_2, knows P_i but he does not have any information about C_i since the only data he knows is the XOR sum
  $$C_1 \oplus C_2 \oplus \ldots \oplus C_N$$
- **Completeness**. This property remains guaranteed since the authority of certification U_0 takes charge of providing digital certificates to the registered voters and to make the blind signature of the different votes P_i.
- **Correctness**. Each voter V_i can verify that its vote has been considered since the bit sequence P_i is published by the U_2 authority. In addition it is possible to verify the final result of the recount since also sequence C is made public.
- **Uniqueness**. By the own construction of the algorithm, each one of the voters can cast only vote valid.

5. Conclusions and further work

In this work an electronic voting protocol in which the voter must choose between two options, has been developed. It is a very simple scheme that uses the bit operation XOR for the construction of the votes, and the blind digital signature to their validation. Besides the own voters, the presence of third trust part is necessary: An

authority of certification that provide the digital certificates to the voters and to have the capacity to make blind digital signature, an authority of authentication that identify the registered voters and provide them the tools necessary to construct their votes, and an authority of collection and recount that will be the responsible to collect and to count the votes. It is shown that the proposed protocol satisfies the main indispensable requirements: anonymity, completeness, uniqueness and correctness.

Acknowledgments

This work has been partially supported by "D. Samuel Solórzano Barruso" Memorial Foundation (University of Salamanca, Spain) under grant FS/7-2006, and by Junta de Castilla y León under grant SA110A06.

References

[1] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, A. Vaccarelli. « SEAS, a secure e-voting protocol: Design and implementation" Comput. Secur., vol. 24 (8), pp. 642-652, 2005.

[2] P. Bonetti, S. Ravaioli, S. Piergallini. "The italian academic community's electronic voting system" Comput. Netw. vol. 34, pp. 851-860, 2000.

[3] Ch.-Ch. Chang, J.-S. Lee. "An anonymous voting mechanism based on the key exchange protocol" Comput. Secur., vol. 25 (4), pp. 307-314, 2006.

[4] Y.-Y. Chen, J.-K. Jan, Ch.-L. Chen. "The design of a secure anonymous Internet voting system" Comput. Secur., vol. 23 (4), pp. 330-337, 2004.

[5] R. Cramer, R. Gennaro, B. Schoenmakers. "A secure and optimally efficient multi-authority election scheme" Advances in Cryptology-Eurocrypt 97, LNCS vol. 1233, 103-118, 1997.

[6] I. Damgard, M. Jurik. "A generalization, a simplification and some applications of Pailliers probabilistic public-key system" Proceedings of Public key cryptography, PKC 01, LNCS vol. 1992, pp. 119-136, 2002.

[7] G. Dini. "A secure and available electronic voting service for a large-scale distributed system" Future Gener. Comp. Sy. vol. 19, pp. 69-85, 2003.

[8] A. Hevia, M. Kiwi. "Electronic jury voting protocols". Theor. Comput. Sci., vol. 321 (1), pp. 73-94, 2004.

[9] W.-Ch. Ku, Sh.-D. Wang. "A secure and practical electronic voting scheme" Comput. Commun. vol. 22, pp. 279-286, 1999.

[10] H.-T. Liaw. "A secure electronic voting protocol for general elections" Comput. Secur., vol. 23, pp. 107-119, 2004.

[11] K. Sako, J. Killiam. "Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth" Advances in Cryptology-Eurocrypt 95, LNCS vol. 921, pp. 393-403, 1995.

[12] D. Chaum. "Untreaceable electronic mail, return addresses and digital pseudonyms" Comm. ACM vol. 24, pp. 84-88, 1981.

[13] A. Fujioka, T. Okamoto, K. Ohta. "A practial secret voting scheme for large scale elections" Advances in Cryptology-Asiacrypt 92, LNCS vol. 718, pp. 248-259, 1993.

[14] D. Chaum. "Blind signatures for untraceable payments" Advances in Cryptology-Proceedings of Crypto 82 pp. 199-203, 1983.

A.B. Cabello Pardos Ana Belén Cabello Pardos received her MSc. degree from Universidad de Salamanca in 1991. She is working as an assistant professor from 2004 in the Dept. of Applied Mathematics, Universidad de Salamanca. Her research interest includes cryptography, cellular automata and image processing.

Ascensión Hernández Encinas received her MSc. degree from Universidad de Salamanca in 1982. He received the PhD. degree from Universidad de Salamanca in 1990. After working as an assistant professor (from 1991) in the Dept. of Applied Mathematics, Universidad de Salamanca, he has been a full professor at Universidad de Salamanca, since 2002. His research interest includes cryptography, cellular automata, image processing and climatology.

S. Hoya White received her MSc degree from Universidad de Salamanca in 1999. Currently she is PhD. student in the department of Applied Mathematics of Universidad de Salamanca.

A. Martín del Rey received his MSc. degree from Universidad de Salamanca in 1996. He received the PhD. degree from UNED in 2000. After working as an assistant professor (from 1997) in the Dept. of Applied Mathematics, Universidad de Salamanca, he has been a full professor at Universidad de Salamanca, since 2003. His research interest includes cryptography, cellular automata, image processing and ordinary differential equations.

G. Rodríguez Sánchez Gerardo Rodríguez Sánchez obtained the Ph. D. in Mathematics from Universidad de Salamanca in 1996. He is full professor of Applied Mathematics Department in Universidad de Salamanca. His current research interests include image processing, cellular automata and cryptography.