XX Congreso de Ecuaciones Diferenciales y Aplicaciones
X Congreso de Matemática Aplicada
Sevilla, 24-28 septiembre 2007
(pp. 1–7)

Un protocolo de votación electrónica basado en firmas digitales ciegas

A.B. Cabello Pardos[1], A. Hernández Encinas[1]
S. Hoya White [1], A. Martín del Rey[2],
G. Rodríguez Sánchez[3]

[1] *E.T.S.I.I. de Béjar, Dpto. Matemática Aplicada, Universidad de Salamanca*
Avda. Fernández Ballesteros 2, 37700-Béjar, Salamanca.
E-mails: anabelencp@usal.es, ascen@usal.es, sarahw@usal.es.
[2] *E.P.S. de Ávila, Dpto. de Matemática Aplicada, Universidad de Salamanca*
C/Hornos Caleros 50, 05003-Ávila. E-mail: delrey@usal.es.
[3] *E.P.S. de Zamora, Dpto. de Matemática Aplicada, Universidad de Salamanca*
Avda. Requejo 33, 49022-Zamora. E-mail: gerardo@usal.es.

Palabras clave: Voto electrónico, Criptografía, Firmas ciegas.

Resumen

En el presente trabajo se expone un nuevo protocolo de votación electrónica basado en la operación bit a bit XOR y el uso de firmas ciegas. Concretamente se trata de un algorimo diseñado expresamente para el caso en que en la votación haya que elegir entre dos candidatos o dos opciones.

1 Introducción

La gran expansión del uso de Internet, tanto en su implantación como en los servicios ofrecidos a través de la misma, permite al usuario realizar multitud de tareas de todo tipo: comercio electrónico, teletrabajo, consulta de bases de datos, etc. Es más, los diferentes gobiernos y administraciones públicas se han implicado en este desarrollo y han puesto a disposición de los ciudadanos nuevos servicios que se han dado en llamar *e-government* (o gobierno electrónico). Con esta sugerente denominación se hace referencia a servicios más o menos sofisticados ofrecidos por la Administración Pública tendentes a facilitar las gestiones ciudadano-Administración. Así, entre los mismos, podemos encontrar desde los sistemas más sencillos que proporcionan exclusivamente acceso a la información (información sobre becas, oposiciones, etc.), hasta los sistemas más sofisticados de ventanilla

electrónica que permiten sustituir los trámites presenciales por trámites realizados por vía telemática: presentación de la declaración de la renta, pago de tasas, matriculaciones, etc. De esta forma, nuestra sociedad tiende a implantar en el ámbito electrónico todas aquellas actuaciones que los ciudadanos desarrollan habitualmente y entre ellas cabe destacar la participación ciudadana en la toma de decisiones (e-democracia o democracia digital) a través de lo que se ha dado en llamar el voto electrónico.

Los requerimientos mínimos que debe satisfacer todo esquema de votación electrónica son los siguientes:

- *Anonimato.* Debe ser imposible relacionar el voto con el votante que lo ha emitido.
- *Autenticidad.* Sólo los votantes legítimamente censados pueden votar.
- *Unicidad.* Cada votante puede emitir un único voto.
- *Verificabilidad.* Cada votante debe poder comprobar que su voto ha sido considerado adecuadamente.

Hasta la fecha se han propuesto multitud de protocolos criptográficos que permiten el desarrollo de votaciones electrónicas(véanse, por ejemplo, [1, 2, 3, 6, 7, 8, 9, 11, 12, 13, 14]). La gran mayoría están basados en el uso de, fundamentalmente, tres primitivas criptográficas: *mixnets* (redes de cifrado, redes de descifrado, redes DC), firmas digitales ciegas, cifrado homomórfico.

Las **mixnets** son similares a los canales anónimos que son usados para distribuir de forma anónima y segura entre los votantes las credenciales (certificados digitales, etc.) necesarias para llevar a cabo la votación electrónica. De forma un poco más rigurosa, podemos decir que se trata de terceras partes de confianza que distribuyen mensajes entre los votantes de tal forma que un posible atacante no es capaz de determinar el emisor o receptor de un determinado mensaje. El uso de las mixnets fue propuesto por Chaum (véase [4]).

Las **firmas digitales ciegas** se utilizaron inicialmente para diseñar los primeros protocolos de dinero electrónico. Posteriormente fueron utilizadas por Fujioka *et al.* (véase [10]) para validar votos en un esquema electoral electrónico. Grosso modo, mediante el uso de firmas digitales ciegas es posible que una autoridad firme digitalmente una serie de datos (por ejemplo el voto de un votante) sin conocer el contenido de dichos datos. Al igual que en el caso anterior, la firmas digitales ciegas fueron introducidas por Chaum (véase [5]).

El **cifrado homomórfico** fue propuesto por Cramer *et al.* (véase [7]) y aprovecha las propiedades características de los cifrados homomórficos para dotar de verificabilidad a los esquemas de voto electrónico sin aportar ninguna información sobre los votos individuales. En los cifrados homomórficos existen dos operaciones: una, $\oplus$, definida en el espacio de mensajes (votos), y otra, $\otimes$, definida en el espacio de los criptogramas (votos cifrados), de tal forma que el "producto" de dos votos cifrados: $E(v_1) \otimes E(v_2)$ es el criptograma de la "suma" de dos votos: $E(v_1 \oplus v_2)$.

En el presente trabajo se propone un nuevo protocolo de votación electrónica basado en la utilización de los esquemas de firmas digitales ciegas. En este protocolo los votantes pueden elegir entre dos candidatos o dos opciones. Además satisface los principales requisitos de seguridad exigibles a protocolos de este tipo: unicidad, autenticidad, anonimato y verificabilidad.

El resto del trabajo está organizado de la siguiente manera: en la sección 2 se hace una pequeña introducción a los esquemas de firmas digitales ciegas; el protocolo de votación electrónica propuesto es mostrado en la sección 3. En la sección 4 se estudian las propiedades del citado protocolo y, finalmente las conclusiones y el trabajo futuro se muestran en la sección 4.

2 Esquemas de firmas digitales ciegas

Los esquemas de firmas ciegas son protocolos criptográficos bipartitos entre un usuario V y un firmante U de tal forma que U firma digitalmente una serie de datos enviados por V sin conocer el contenido de los mismos. El principal propósito de este tipo de protocolos es la obtención de una serie de datos firmados cuyo contenido sólo sea conocido por el usuario. Todo protocolo de firma ciega requiere de la presencia de los siguientes componentes:

1. Un protocolo de firma digital que sea desarrollado por el prestador del servicio o firmante U, de tal forma que $S(m)$ denote la firma digital del mensaje m.
2. Dos funciones, f y g, conocidas sólo por el usuario V, de tal forma que
$$g(S(f(m))) = S(m). \tag{1}$$

A la función f la denominaremos función de ocultación o de opacidad, mientras que la función g es la función de recuperación. En el presente trabajo utilizaremos el protocolo de firma ciega basado en el criptosistema RSA y desarrollado por D. Chaum (véase [5]). Éste consiste en lo siguiente: sea $n = p \cdot q$ el producto de dos primos aleatorios suficientemente grandes. El protocolo de firma digital utilizado por el firmante U será el esquema de firma digital RSA con clave pública (n, e) y clave privada d. Sea k un entero aleatorio tal que $mcd(n, k) = 1$. Las funciones utilizadas por el usuario V son:

$$\begin{aligned} f\colon \mathbb{Z}_n &\to \mathbb{Z}_n \\ m &\mapsto f(m) = m \cdot k^e \bmod n \end{aligned} \tag{2}$$

$$\begin{aligned} g\colon \mathbb{Z}_n &\to \mathbb{Z}_n \\ m &\mapsto g(m) = k^{-1} \cdot m \bmod n \end{aligned} \tag{3}$$

Obsérvese que de esta forma se tiene:

$$\begin{aligned} g(S(f(m))) &= g(S(m \cdot k^e \bmod n)) \\ &= g\left(m^d \cdot k \bmod n\right) = m^d \bmod n = S(m). \end{aligned} \tag{4}$$

Así pues el protocolo de firma ciega es como sigue:

1. **Fase de inicialización**. Sea $0 \leq m \leq n-1$ el mensaje originado por V y que debe ser firmado por U, y sea k un entero aleatorio elegido por V tal que $0 \leq k \leq n-1$ y $mcd(k, n) = 1$.
2. **Fase de ocultación**. V calcula $m^* = f(m) = m \cdot k^e \bmod n$ y se lo envía a U.
3. **Fase de firma**. U calcula $s^* = S(m^*) = (m^*)^d \bmod n$ y se lo envía a V.
4. **Fase de recuperación**. V calcula $s = S(m) = g(S(m^*)) = k^{-1} \cdot s^* \bmod n$ que es la firma digital del mensaje m por U.

3 El protocolo de votación electrónica

En esta sección introduciremos el protocolo de votación electrónica desarrollado. Para la construcción de los votos, se hace uso de la operación bit a bit XOR, mientras que la validación de los mismos se consigue mediante un esquema de firma digital ciega. Son cuatro las partes implicadas en el esquema de votación electrónica propuesto en este trabajo:

- **Votantes**: $V_1, V_2, \ldots, V_N$. Son los principales actores de todo proceso electoral. Deben emitir un único voto anónimo que sea contabilizado correctamente por las autoridades pertinentes.
- **Autoridad de certificación**: U_0. Es una tercera parte de confianza cuya misión es proporcionar certificados digitales a los legítimos votantes censados y realizar las firmas digitales ciegas de los votos emitidos.
- **Autoridad de autenticación**: U_1. Es una tercera parte de confianza cuya misión es autenticar a los votantes censados y proveerles de las herramientas necesarias para emitir su voto correctamente.
- **Autoridad de recolección y recuento**: U_2. Es una tercera parte de confianza encargada de recolectar los votos, comprobar su validez, almacenarlos y finalmente llevar a cabo el recuento de los mismos. Es por tanto, la única entidad que tiene permitido el descifrado de los votos.

El protocolo propuesto es como sigue:

1. La autoridad de certificación U_0 emite un certificado digital a cada uno de los votantes legítimanente censados.
2. Cada votante V_i se identifica ante la autoridad de autenticación U_1, la cual valida su certificado digital y le envía una secuencia aleatoria de bits $B_i \in \mathbb{F}_2^N$.
3. Cada votante V_i crea su voto, $v_i \in \mathbb{F}_2^N$, haciendo la suma XOR bit a bit del i-ésimo bit de la sucesión B_i con un 1 si opta por la Opción 1, o con un 0 si opta por la Opción 2. Esto es:

$$\text{Si opta por la Opción 1: } v_i = B_i \oplus (0, \ldots, 0, \overbrace{1}^{i-\text{ésimo}}, 0, \ldots, 0) \tag{5}$$

$$\text{Si opta por la Opción 2: } v_i = B_i \oplus (0, \ldots, 0, \overbrace{0}^{i-\text{ésimo}}, 0, \ldots, 0) \tag{6}$$

4. Cada votante V_i elige de forma aleatoria una secuencia de bits $C_i \in \mathbb{F}_2^N$ y calcula $P_i = v_i \oplus C_i$.
5. Cada votante V_i solicita a la autoridad de certificación U_0 que le haga la firma ciega, P_i^*, de P_i y obtiene, al recuperarla, $S(P_i)$.
6. Cada votante V_i manda a la autoridad de certificación U_0 el vector aleatorio $C_i \in \mathbb{F}_2^N$.
7. Cada votante V_i manda a la autoridad de recolección U_2 su voto firmado por U_0: $S(P_i)$.

8. La autoridad de certificación U_0 calcula

$$C = C_1 \oplus C_2 \oplus \ldots \oplus C_N \in \mathbb{F}_2^N, \tag{7}$$

y se lo envía a la autoridad de recuento U_2.

9. La autoridad de autenticación U_1 calcula:

$$B = B_1 \oplus B_2 \oplus \ldots \oplus B_N \in \mathbb{F}_2^N, \tag{8}$$

y se lo envía a la autoridad de recuento U_2.

10. La autoridad U_2 comprueba la validez de los diferentes votos descifrando $S(P_1), \ldots, S(P_N)$, con lo que obtiene de esta manera: $P_1, \ldots, P_N$.

11. La autoridad U_2 calcula:

$$P = P_1 \oplus P_2 \oplus \ldots \oplus P_N. \tag{9}$$

12. La autoridad U_2 calcula:

$$P \oplus C = v_1 \oplus v_2 \oplus \ldots \oplus v_N = v. \tag{10}$$

13. La autoridad U_2 calcula el número de votos obtenido por la Opción 1 sin más que hallar la distancia de Hamming entre los vectores v y B. Esto es:

$$\text{Nº de votos de la Opción 1} \quad : \quad d_H(v, B), \tag{11}$$
$$\text{Nº de votos de la Opción 2} \quad : \quad n - d_H(v, B). \tag{12}$$

14. Finalmente, la autoridad U_2 hace públicas las secuencias de bits $P_1, \ldots, P_N$ junto con C.

Obsérvese que a la hora de calcular la firma digital ciega de P_i, cada votante ha de elegir un número entero aleatorio, k_i, tal que $0 \leq k_i \leq n-1$ y $mcd(k_i, n) = 1$. Además debe transformar la secuencia de bits P_i en un número entero m_i tal que $0 \leq m_i \leq n-1$, lo cual se consigue sin más que tener en cuenta su expresión decimal. Podemos suponer que la longitud en bits de la clave pública n es de 4096, con lo que no existiría problema a la ahora de realizar este proceso siempre que $N < 4096$. Si no fuera así, entonces habría que romper P_i en tantos trozos de longitud menor que 4096 como fueran necesarios y firmar cada uno de ellos por separado.

4 Análisis de las propiedades del protocolo propuesto

En esta sección comprobaremos que el protocolo anteriormente propuesto satisface los principales requisitos exigibles a cualquier esquema de voto electrónico.

- **Anonimato**. Ninguna de las tres autoridades que participan en el proceso electoral pueden determinar el voto de un determinado votante V_i. Así, la autoridad de certificación U_0 conoce el valor del vector binario C_i pero le es imposible determinar v_i ya que no conoce B_i. La autoridad de autenticación U_1 sólo conoce la secuencia de bits B_i y consecuentemente cualquier pronóstico sobre el voto de V_i no tendrá una probabilidad superior a 0.5. Finalmente, la autoridad de recolección y recuento, U_2, conoce P_i pero no tiene ninguna información sobre C_i ya que el único dato que posee es la suma XOR $C_1 \oplus \ldots \oplus C_N$.

- **Autenticidad**. Esta propiedad queda garantizada puesto que que la autoridad de certificación U_0 se encarga de proporcionar certificados digitales a los votantes censados y de realizar las firmas ciegas de los diferentes votos P_i.

- **Verificabilidad**. Cada votante V_i puede comprobar que su voto ha sido tenido en cuenta pues la secuencia de bits P_i es publicada por la autoridad U_2. Además es posible comprobar el resultado final del recuento ya que también se hace pública la secuencia C.

- **Unicidad**. Por la propia construcción del algoritmo, cada uno de los votantes puede emitir un único voto válido en su nombre. Obsérvese que podría darse el caso que un mismo votante, por ejemplo V_i, votara por sí mismo y por otro votante V_j, $j \neq i$ sin mas que modificar el bit i-ésimo y el bit j-ésimo. En este caso se estaría violando una de las premisas fundamentales.

5 Conclusiones y trabajo futuro

En este trabajo se ha desarrollado un protocolo de votación electrónica en el que el votante debe elegir entre dos opciones. Se trata de un esquema muy sencillo que hace uso exclusivamente de la operación bit a bit XOR para la construcción de los votos, y de la firma digital ciega para la validación de los mismos. Aparte de los propios votantes, se hace necesaria la presencia de tres terceras partes de confianza: una autoridad de certificación que provea a los votantes de certificados digitales y que tenga la capacidad de realizar firmas digitales ciega, una autoridad de autenticación que identifique a los votantes legítimamente censados y les proporcione las herramientas necesarias para construir su voto, y una autoridad de recolección y recuento que será la encargada de recoger los votos y contarlos. Se demuestra que el protocolo propuesto satisface los principales requisitos exigibles: anonimato, autenticidad, unicidad y verificabilidad. Además aunque, debido a la construcción del algoritmo, cada votante sólo puede emitir un voto en su nombre, podría darse el caso que votara por otra persona. Este es el problema que presenta este protocolo y que, como trabajo futuro, se propone subsanar.

Agradecimientos

Ese trabajo ha sido parcialmente subvencionado por la Fundación "Memoria D. Samuel Solórzano Barruso" de la Universidad de Salamanca con el proyecto FS/7-2006 y por la Consejería de Educación de la Junta de Castilla y León con el proyecto SA110A06.

Referencias

[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), (2005), 642-652.

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

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

[4] D. Chaum. *Untreaceable electronic mail, return addresses and digital pseudonyms.* Comm. ACM vol. 24, (1981), 84-88.

[5] D. Chaum. *Blind signatures for untraceable payments.* Advances in Cryptology-Proceedings of Crypto 82 (1983), 199-203.

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

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

[8] 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, (2002), 119-136.

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

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

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

[12] W.-Ch. Ku, Sh.-D. Wang. *A secure and practical electronic voting scheme.* Comput. Commun. vol. 22, (1999), 279-286.

[13] H.-T. Liaw. *A secure electronic voting protocol for general elections.* Comput. Secur., vol. 23, (2004), 107-119.

[14] 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, (1995), 393-403.