Un protocolo de votación electrónica basado en firmas digitales ciegas

A. Martín del Rey

Dpto. de Matemática Aplicada, E.P.S. de Ávila, Universidad de Salamanca

delrey@usal.es

A.B. Cabello Pardos, A. H. Encinas, S. Hoya White

Dpto. de Matemática Aplicada, E.T.S.I.I. de Béjar, Universidad de Salamanca

{anabelencp, ascen, sarahw}@usal.es

G. Rodríguez Sánchez

Dpto. de Matemática Aplicada, E.P.S. de Zamora, Universidad de Salamanca

gerardo@usal.es

Resumen

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.

Hasta la fecha se han propuesto multitud de protocolos criptográficos que permiten el desarrollo de votaciones electrónicas (véanse, por ejemplo, [1, 3, 4]). La gran mayoría están basados en el uso de técnicas criptográficas de clave pública: criptosistema RSA o ElGamal, Firma digital, Firma Digital Ciega, etc.

En el presente trabajo se propone un nuevo protocolo de votación electrónica basado en los protocolos desarrollados recientemente por Liaw (véase [5]) y Chang y Lee ([2]) que hacen uso de la firma digital ciega. El protocolo propuesto está especialmente diseñado para entornos reducidos (votaciones sobre una red local de acceso restringido, por ejemplo). Además satisface los principales requisitos de seguridad exigibles a protocolos de este tipo: unicidad, robustez, anonimato, eficiencia, verificabilidad, completitud, imposibilidad de coerción, etc.

Sección en el CEDYA 2007: OTROS TEMAS

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

[3] 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.

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

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