Voto Electrónico Seguro con Criptografía Homomórfica

Pablo García [1]; Jeroen van de Graaf [2]; Germán Montejano [3];

[1] Departamento de Matemática
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-245220– Int. 7125
pablogarcia@exactas.unlpam.edu.ar – web: http://www.exactas.unlpam.edu.ar

[2] Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
Av. Antonio Carlos, 6627 – 31270-010 - Belo Horizonte – Minas Gerais - Brasil
Tel.:+55-3409-5836
jvdg@dcc.ufmg.br – web: http://www.dcc.ufmg.br/~jvdg

[3] Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-266-4520300– Int. 2128
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

Resumen

La viabilidad de la implementación del voto electrónico es un tema extremadamente discutido en la República Argentina. Por ejemplo, el Congreso de la Nación ha rechazado la propuesta del Poder Ejecutivo Nacional de implementar un sistema de boleta única electrónica, en concordancia con una publicación de un grupo de informáticos pertenecientes a universidades nacionales argentinas[1].

Se considera, sin embargo, que no existen argumentos contundentes para afirmar que es imposible conseguir que un sistema de votación electrónica garantice transparencia y privacidad para el votante. De hecho, existen sólidas propuestas de tipo híbrido que proporcionan evidencia física que permite asegurar que los procedimientos se llevaron a cabo de manera irreprochable[2]. Ese punto es crucial: el sistema debe demostrar de forma clara e indiscutible la transparencia del proceso de manera tal que cualquier ciudadano común pueda verificar los resultados y a la vez, convencerse de que el proceso se llevó a cabo de manera totalmente confiable.

En consecuencia, se propone analizar el problema en profundidad y generar un modelo que proporcione respuestas apropiadas. Además de la descripción detallada de la criptografía propuesta se llevará a cabo la implementación de un prototipo que implemente las funcionalidades básicas.

Palabras clave: ***Voto Electrónico, Transparencia, Anonimato, Evidencia***

[1] http://www.cronista.com/economiapolitica/Expertos-universitarios -lanzaron-una-campana-contra-el-voto-electronico-20161101-0113.html

[2] https://www.usenix.org/conference/evt wote13/workshop-program/presentation/bell

Física, Verificabilidad E2E, Criptografía Homomórfica, Paillier, ElGamal.

Contexto

Por Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa se acredita el Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en el ámbito de la FCEyN de la UNLPam. El mismo es dirigido por el Doctor Germán Antonio Montejano y codirigido por el Magister Pablo Marcelo García e incluye a los magisters Silvia Gabriela Bast y Daniel Vidoret como investigadores.

El Proyecto surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [1], y que a su vez se enmarca en el Proyecto "Ingeniería de Software: Aspectos de Alta Sensibilidad en el Ejercicio de la Profesión de Ingeniero de Software" de la Facultad de Ciencias Físico - Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL, http://www.sel.unsl.edu.ar/pro/proyec/2012/index.html) y que incluye acciones de cooperación con la Universidad Federal de Minas Geráis (UFMG, Brasil).

Entre tales acciones debe mencionarse que Jeroen van de Graaf, PhD., Docente de UFMG, y el Dr. Germán Montejano (UNSL) fueron orientadores del Mg. Pablo García en el desarrollo de su tesis de Maestría en Ingeniería de Software titulada "Optimización de un Protocolo Dining Cryptographers Asíncrono", defendida en 2013 en el ámbito de la UNSL. Durante el desarrollo de la misma se generaron una serie de publicaciones de avances parciales, como por ejemplo [2], [3], [4], [5] y [6].

Introducción

La implementación del voto electrónico es un tema muy discutido en la actualidad. Existen partidarios y detractores, en proporciones similares. Lo que debe quedar claro es que la implementación de un modelo innovador debe, necesariamente, resultar superador de las propuestas preexistentes. De no ser así no tiene sentido ninguna propuesta novedosa.

En consecuencia, la implementación de sistemas de voto electrónico presenta dos exigencias claras:

- El escrutinio asociado debe reflejar de manera indiscutible la voluntad de los ciudadanos
- Simultáneamente, los electores deben estar convencidos de que su privacidad es garantizada indefinidamente.

Se otorga máxima atención a las consecuencias que puede acarrear, para cualquier votante, el hecho de que su opción sea divulgada. Existen numerosas variantes de prácticas deshonestas que se derivan de conocimiento de esa información, con o sin el aval del elector. Es claro que si un ciudadano pudiera probar que votó a un determinado partido político, podría recibir una contraprestación. Análogamente, si un sector detecta que un votante votó a otra opción, podría llevar a cabo acciones que perjudiquen al votante.

Cualquier propuesta que se desee implementar en ese sentido, deberá cumplir con una serie de condiciones que se exigen actualmente a los sistemas de votación electrónica, [7]. Las principales son las siguientes:

- Debe existir evidencia física que garantice la transparencia del proceso [8]. Este punto debe ser implementado

de tal manera que sirva como prueba irrefutable, no sólo en la consideración de los expertos, sino también de los electores.

• Utilización de métodos criptográficos cuya seguridad pueda ser demostrada de manera matemática y que garanticen el anonimato del votante y la seguridad computacional necesaria en lo referido a la transparencia de los resultados de los comicios. En ese sentido, revisten máximo interés los esquemas homomórficos, es decir aquellos que permiten operaciones matemáticas sobre las versiones cifradas de la información. Ejemplos de modelos que presentan esa característica son Paillier [9], [10] y ElGamal exponencial [11], [12].

• Aplicación del concepto de independencia del software, es decir que si el software es corrupto, no hay ninguna posibilidad de que se generen resultados incorrectos y eso no sea detectado [13].

• Definir un modelo concreto para la aplicación de verificabilidad "End to End" (E2E) [14], [15]. Ello implica garantizar:

- Verificabilidad individual: es decir, que cualquier votante puede asegurarse de que su voto fue correctamente contabilizado.
- Verificabilidad universal, que implica que cualquier observador neutral pueda asegurarse de que todos los sufragios han sido correctamente contabilizados.
- Verificabilidad de padrón, de manera tal que sea posible probar que todos los votos incluidos en el recuento provienen de votantes habilitados.
- Imposibilidad de que algún votante pueda demostrar por quién votó, dado que eso daría lugar a maniobras de "compra de sufragios".

Líneas de Investigación, Desarrollo e Innovación

El grupo de trabajo investiga, básicamente sobre dos líneas paralelas, para generar modelos que pudieran aplicarse a los sistemas de voto electrónico:

- Basados en criptografía One Time Pad, desarrollada por la Magister Silvia Gabriela Bast.
- Basados en criptografía homomórfica, que es la línea relacionada con este documento y sus autores.

Resultados y Objetivos

En el ámbito del voto electrónico, este grupo de trabajo ha realizado durante el año 2017, las siguientes publicaciones:

- [16] expone una técnica de recuento y recuperación de sufragios para el modelo OTP – Vote cuyos conceptos pueden generalizarse a otros esquemas.
- [17] especifica una propuesta para el modelo de datos aplicable al sistema OTP – Vote.
- [18] propone un modelo para agregar verificabilidad OTP – Vote.
- [19] presenta una técnica para generar una optimización en el almacenamiento de sufragios en esquemas basados en el protocolo Non Interactive Dining Cryptographers (NIDC).
- [20] Se expone un sistema de generación de códigos para el sistema OTP – Vote, que optimiza el dicho proceso de manera significativa.

Llegado este punto, se decide investigar un camino alternativo, relacionado con la criptografía homomórfica. En

consecuencia, a futuro, se pretende llevar a cabo las siguientes acciones:

- Proponer un nuevo esquema de voto electrónico basado en las características expuestas en las secciones previas.
- Implementar una aplicación experimental que permita observar el comportamiento del modelo teórico que surja del avance de la investigación.
- Continuación del relevamiento de aplicaciones orientadas al voto electrónico, con el fin de detectar falencias y proponer mejoras.

Formación de Recursos Humanos

En el marco del presente proyecto se presentan los siguientes puntos relacionados con la formación de recursos humanos durante 2017:

- Pablo García realizó una estadía de un mes (3/9/2017) al 4/10/2017) en la Universidade Federal de Minas Geráis (UFMG), en el Departamento de Ciência da Computação (DCC) dependiente del Instituto de Ciências Exatas (ICEX) trabajando en el laboratorio 4303 del grupo "Criptografía Teórica y Aplicada", dirigido por Jeroen van de Graaf, PhD.
- Pablo García completó el cursado de la totalidad de los créditos exigidos en el Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL).
- Pablo García presentó su Plan de Tesis Doctoral, en el marco del Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL). El mismo se encuentra en proceso de evaluación. Dicha tesis será dirigida por Jeroen van de Graaf, PhD. y el Dr. Germán Montejano.

Referencias

[1] Uzal R., van de Graaf J., Montejano G., Riesco D., García P.: "Inicio de la Línea de Investigación "Ingeniería de Software y Defensa Cibernética". Memorias del XV Workshop de Investigadores en Ciencias de la Computación 2013 (WICC 2013). Ps.769 - 773. ISBN: 9789872817961. 2013.

[2] van de Graaf J., Montejano G., García P.: "Optimización de un Protocolo Non-Interactive Dining Cryptographers". Congreso Nacional de Ingeniería Informática / Sistemas de Información. CoNaIISI 2013. Córdoba, Argentina.

[3] van de Graaf J., Montejano G., García P., Bast S.: "Anonimato en Sistemas de Voto Electrónico". Memorias del XVI Workshop de Investigadores en Ciencias de la Computación 2014 (WICC 2014). Ps. 822 – 826. ISBN: 9789503410844. 8 y 9 de mayo de 2014.

[4] van de Graaf J., Montejano G., García P.: "Manejo de Colisiones en un Protocolo Non Interactive Dining Cryptographers". Anales de las 42° Jornadas Argentinas de Informática e Investigación Operativa (JAIIO, ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Ps. 29 a 43. Septiembre 2013.

[5] García P., van de Graaf J., Montejano G., Bast S., Testa O.: "Implementación de Canales Paralelos en un Protocolo Non Interactive Dining Cryptographers". 43° Jornadas Argentinas de Informática e Inves-

tigación Operativa (JAIIO 2014), Workshop de Seguridad Informática (WSegI 2014).

[6] García P., van de Graaf J., Hevia A., Viola A.: "Beating the Birthday Paradox in Dining Cryptographer Networks". The third International Conference on Cryptology and Information Security in Latin America, Latincrypt 2014. September 17-19, 2014. Florianopolis, Brasil. Lecture Notes in Computer Science, Springer (2014).

[7] Hao, F, Ryan P.: "Real -World Electronic Voting. Design, Analysis And Deployment". Cr Press. ISBN-13: 978-1498714693. ISBN-10: 1498714692. 2017.

[8] Prince, A.: "Consideraciones, Aportes y Experiencias para el Voto Electrónico en Argentina". Editorial Dunken. ISBN: 978-987-02-1732-9. 2006.

[9] Volkhausen T.: "Paillier Cryptosystem: A Mathematical Introduction". 2006.

[10] O'Keeffe M.: "The Paillier Cryptosystem: A Look Into The Cryptosystem And Its Potential Application". The College of New Jersey Mathematics Department. 2008

[11] El Gamal T. "A public key cryptosystem and a signature scheme based on discrete logarithms". In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc. 1985.

[12] Koscielny C.: "A New Approach to the Elgamal Encryption Scheme". Academy of Management of Legnica, Faculty of Computer Science. 2004.

[13] Rivest R.: "On the notion of 'software independence' in voting systems". Philosophical Transactions of The Royal Society A, 366(1881):3759–3767. 2008.

[14] Benaloh J. Bernhard M. Halderman J. Rivest R Ryan P. Stark P. Vora P. Teague V. Wallach D.:"Public Evidence from Secret Ballots". Documento presentado en E-Vote-ID 2017.

[15] Kelsey J., Regenscheid A., Moran T., Chaum D.: "Attacking Paper-Based E2E Voting Systems". In: Chaum D. et al. (eds) Towards Trustworthy Elections. Lecture Notes in Computer Science, vol 6000. Springer, Berlin, Heidelberg. ISBN: 978-3-642-12979-7. 2010.

[16] García P., Bast S., Montejano G.: "Recuento y Recuperación de Sufragios en OTP – Vote". Simposio de Informática en el Estado (SIE) del XLIII CLEI (Conferencia Latinoamericana de Informática) y 46° JAIIO (Jornadas Argentinas de Informática e Investigación Operativa. ISSN: 2451-7534. Ps. 38 a 51.

[17] Bast S., García P., Montejano G.: "Modelo de Datos del Sistema de Voto Electrónico Presencial OTP-Vote". Simposio de Informática en el Estado (SIE) del XLIII CLEI (Conferencia Latinoamericana de Informática) y 46° JAIIO (Jornadas Argentinas de Informática e Investigación Operativa). ISSN: 2451-7534. Ps. 23 a 37. 2017.

[18] García P., Bast S., Montejano G.: "Verificabilidad ´End to End´ para OTP – Vote". VI Workshop Seguridad Informática (WSI) del Congreso Argentino de Ciencias de la Computación (CACIC 2017).

[19] García P., Bast S., Montejano G.: "Efficient Votes Storage in a Non-Interactive Dining Cryptographers (NIDC) Protocol". VI Workshop Seguridad Informática (WSI) del Congreso Argentino de Ciencias de la Computación (CACIC 2017).

[20] Bast S., García P., Montejano G.: "Generación de Códigos para OTP – Vote". 5° Congreso Nacional de Ingeniería Informática / Sistemas de Información. CONAiisi 2017. http://tecnomate .xyz/Actas-CONAIISI-2017.pdf. Ps. 12 a 22.