Un Sistema de Voto Electrónico para la FCEyN (UNLPam.)

Pablo García[1] Germán Montejano[2] Andrés Farías[3]
Claudio Ponzio[1] Martín Lobos[1] Adrian García[1]

[1]Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-425166– Int. 28
pablogarcia@exactas.unlpam.edu.ar

[2]Departamento de Informática
Facultad de Ciencias Físico Matemáticas y Naturales
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-2652-424027 – Int. 251
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

[3]Facultad de Ciencias Físicas Exactas y Naturales
Universidad Nacional de La Rioja
Av. De La Fuente S/N - La Rioja
afarias@yahoo.com.ar

RESUMEN

La utilización del voto electrónico sigue siendo un tema que genera fuertes controversias. En los ámbitos políticos, se utiliza la dicotomía planteada contra el voto manual como un elemento de permanentes disputas.

Desde hace varios años este equipo de trabajo propone un análisis imparcial de los costos y beneficios de implementar este tipo de sistemas, proponiendo métodos y técnicas que permitan que un sistema de voto electrónico responda a exigencias del más alto nivel y publicando periódicamente sus avances (por ejemplo, [1], [2], [3] y [4]).

Se afirma que un sistema de E-Voting no solamente debe ser absolutamente seguro, sino que además, tal característica debe ser plenamente comprobable. Pero no sólo para los expertos en la materia; también para todos los votantes que participen de un proceso electoral.

La confiabilidad del sistema no solamente debe apuntar a la integridad de los resultados obtenidos, sino que aparecen otros aspectos que deben observarse, como por ejemplo la confidencialidad del elector (que debe protegerse indefinidamente) y la velocidad con la que se obtienen los resultados finales.

En consecuencia, se propone implementar un sistema de voto electrónico que pudiera aplicarse en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa, a través de un nuevo proyecto de investigación que será presentado durante 2021 y que tendrá una duración de cinco años. Se busca implementar todos los avances realizados en publicaciones previas y agregar

elementos novedosos en algunos puntos, tal como lo describe el presente documento

Palabras clave: Sistemas de Voto Electrónico, Anonimato, Transparencia, Criptografía Homomórfica, Verificabilidad E2E, Prueba Física.

CONTEXTO

El presente trabajo tiene por objeto presentar un Proyecto de Investigación que será presentado durante 2021 en el ámbito de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa. El mismo se titulará: "Un Sistema de Voto Electrónico Basado en Criptografía Homomórfica para la FCEyN (UNLPam.)". El mismo es una derivación de un proyecto anterior ("Aspectos de Seguridad en Proyectos de Software", Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales) y que fue dirigido por el Doctor Germán Antonio Montejano (Universidad Nacional de San Luis) y codirigido por el Magister Pablo Marcelo García (FCEyN - UNLPam) e incluyó a la Magister Silvia Gabriela Bast, al Magister Daniel Vidoret, a la Profesora Estela Marisa Fritz, al Analista Programador Adrián García y al Programador Superior Claudio Ponzio como investigadores y a la estudiante Silvia Nicosia como asistente de investigación.

El nuevo proyecto incluirá inicialmente, a los autores del presente trabajo, aunque se buscará elevar el número de investigadores a los efectos de enfrentar los fuertes desafíos que se presentan desde el punto de vista teórico pero también para lograr una implementación eficaz de la aplicación final.

Queda claro que se trata de la continuidad de proyectos anteriores. El origen de esta línea de investigación se ubica en [5], 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), y que se desarrolla en cooperación con la Universidad Federal de Minas Geráis (UFMG, Brasil).

1. INTRODUCCIÓN

Una de las ventajas principales de un sistema de voto electrónico tiene que ver con la obtención de resultados en tiempos significativamente inferiores a los que existen si el proceso es manual. Si bien esa velocidad no es la cuestión más importante dentro del proceso, tampoco es un detalle que deba ignorarse. Cabe recordar que en las elecciones legislativas PASO de 2017, la provincia de Buenos Aires mostraba, ya muy tarde en la noche, resultados opuestos a los que finalmente se obtuvieron al final del recuento, 16 días después (https://www.perfil.com/noticias/elecciones2017/paso-cristina-le-gano-a-bullrich-por-021-de-los-votos.phtml). También se puede mencionar que Al Gore en 2000 tardó un mes en reconocer su ajustada derrota frente al candidato George W. Bush (https://aristeguinoticias.com/0811/mundo/bush-vs-gore-la-eleccion-presidencial-que-casi-colapsa-a-eu/).

Los efectos producidos por esa demora en la difusión de los resultados de los comicios resultan perjudiciales. Se produce una incertidumbre que sólo se despeja cuando la incógnita es develada. Tal situación es indeseable para cualquier sociedad.

Es precisamente en ese aspecto, que la criptografía homomórfica presenta una característica muy conveniente a los efectos de implementar sistemas de voto electrónico, dado que permite realizar operaciones directamente sobre los datos cifrados. Ese atributo le otorga un gran atractivo a su aplicación práctica, aunque, por supuesto, es necesario arbitrar los medios para garantizar la veracidad de los resultados obtenidos y, simultáneamente, proteger la privacidad del votante. Adicionalmente, todo deberá ser absolutamente demostrable.

La criptografía homomórfica aparece en 1978 [6]. Las primeras técnicas presentaban homomorfismo parcial, dado que sólo era posible aplicar un tipo de operación sobre los

datos cifrados (suma o producto). Son ejemplos de este tipo El Gamal [7], Benaloh [8] y Paillier [9].

El primer esquema totalmente homomórfico es de 2009 y se presenta en [10]. Esto resulta un avance de gran importancia, porque permite operaciones de adición y producto sobre datos cifrados.

El modelo que se va a implementar, utilizará alguna técnica de criptografía homomórfica, que será definida como parte del proceso de investigación. Se piensa en variantes de métodos existentes o combinación de más de uno, considerando que es posible que aparezca un esquema novedoso que aporte ventajas concretas.

Por otra parte, el sistema a implementar deberá cumplir con una serie de requisitos que se exigen actualmente a los sistemas de votación electrónica:

- Evidencia física que garantice la transparencia del proceso [11].
- Aplicación del concepto de independencia del software [12].
- Definición de un modelo concreto para la aplicación de verificabilidad "End to End" (E2E) [13]. Esto incluye la aplicación de estrategias que eviten la aparición de maniobras fraudulentas
- Selección de una interface apropiada, con un fuerte análisis de alternativas y una fundamentación sobre la elección.
- Implementación de esquemas de seguridad que permitan asegurar la total integridad en la base de datos asociada.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El grupo de investigación trabajará en forma paralela sobre cada uno de los aspectos que se mencionaron en el punto anterior:

- **Evidencia física:** se trabajará en la búsqueda de alternativas respecto de la impresión concreta del sufragio en papel como elemento de respaldo. En cualquier caso, se deberá probar físicamente la integridad del proceso.
- **Independencia del software:** Deberá definirse un esquema que asegure que el modelo no podrá ser vulnerado por intentos fraudulentos (conocidos o novedosos).
- **Verificabilidad E2E:** El proceso podrá verificarse íntegramente. La verificabilidad "End to End" es uno de los puntos de mayor valor a los efectos de agregar transparencia al proceso de votación electrónica. Se define mediante las tres condiciones siguientes:
    - Verificabilidad individual: cualquier votante puede verificar que su sufragio fue incluido en el recuento.
    - Verificabilidad universal: cualquier persona puede determinar que el recuento total de los votos es correcto.
    - Secreto del voto: ningún votante podrá demostrar cuál fue la opción que eligió, a los efectos de evitar maniobras relacionadas con el "clientelismo político".
- **Interface:** ya se están realizando relevamientos que permitan deducir qué aspecto debe presentar dicha interface y de qué manera los usuarios se relacionarán con el sistema.
- **Seguridad de las comunicaciones**: dos de los autores de este trabajo ya están trabajando en el diseño de un esquema basado en redes virtuales (VLANs).

3. RESULTADOS Y OBJETIVOS

Los avances del grupo de trabajo que han surgido durante 2020 fueron:

- Análisis crítico de los resultados obtenidos en una encuesta online

destinada a personas de todo nivel (desde expertos informáticos hasta votantes comunes) para obtener opiniones sobre la forma concreta que debería tener la interface de un sistema de voto electrónico.

- Desarrollo de una serie de entrevistas a expertos informáticos para complementar los resultados obtenidos en la encuesta online. Esta etapa aún se está realizando en la actualidad.
- Incorporación al proyecto de dos especialistas específicos en comunicaciones de datos para proporcionar metodologías de transmisión de datos que garanticen los niveles de seguridad exigibles. Los mismos se encuentran realizando el análisis de alternativas para implementar un esquema de basado en VLANs. El objetivo será proporcionar un modelo de comunicación que cumpla con los requisitos de máxima seguridad que se exigen en un sistema de este tipo.
- Se continuó trabajando en el análisis de métodos homomórficos existentes. Se pudieron obtener conclusiones parciales en busca de la selección final del esquema definitivo.

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

- Elegir la interface exacta del modelo en base a los datos obtenidos en encuestas y entrevistas.
- Aplicar la interface seleccionada en la aplicación a desarrollar y publicar los fundamentos de la opción elegida.
- Definir un modelo de transmisión de datos e implementarlo.
- Realizar un relevamiento de aplicaciones orientadas al voto electrónico, que permita detectar falencias y proponer mejoras en el nuevo modelo.
- Seleccionar, finalmente, un método criptográfico con características homomórficas para aplicar en la implementación.

4. FORMACIÓN DE RECURSOS HUMANOS

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

- Pablo García realizó tres estadías de investigación en el ámbito del Departamento de Ciência da Computação (DCC) perteneciente al Instituto de Ciências Exatas (ICEx) de la Universidade Federal de Minas Gerais (UFMG) en Belo Horizonte, Brasil. La primera fue en 2012 y duró diez meses. Las dos restantes tuvieron una duración de 30 días cada una y se llevaron a cabo en 2017 y 2018.
- Pablo García defendió con éxito en 2013 su tesis correspondiente a la Maestría en Ingeniería de Software (FCFMyN, UNSL). Obtuvo una calificación de sobresaliente y fue orientada por los Jeroen van de Graaf, PhD. (UFMG) y el Dr. Germán Montejano (UNSL).
- 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) y 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.
- Andrés Farías defendió con éxito en 2019 su tesis correspondiente a la

Maestría en Ingeniería de Software (FCFMyN, UNSL). Obtuvo una calificación de sobresaliente y fue orientada por los directores del futuro proyecto que se presenta en este documento.

- Claudio Ponzio y Martín Lobos desean presentar una Tesis de Especialización o maestría relacionada con los objetivos de este proyecto.

Se espera que otros integrantes del grupo de trabajo a conformar, realicen tesis de posgrado en el ámbito del proyecto a presentar.

5. BIBLIOGRAFÍA

[1] **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). 2013.

[2] **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, Latin-crypt 2014. Florianopolis, Brasil. Lecture Notes in Computer Science, Springer (2014).

[3] **García P., van de Graaf, J., Montejano G., Riesco D., Debnath N.., Bast S**.: "Storage Optimization for Non-Interactive Dining Cryptographers (NIDC)". The International Conference on Information Technology: New Generations. 2015. Las Vegas, Nevada, USA.

[4] **García P., Bast S., Fritz E., Montejano G., Riesco D., Debnath N.,** "A Systematic Method for Choosing Optimal Parameters for Storage in Parallel Channels of Slots". IEEE I-ternational Conference on Industrial Technology (ICIT 2016). / Taiwan, Taipei. http://ieeexplore.ieee.org/document/7475019/.

[5] **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 WICC. Ps 769-773. ISBN: 9789872817961. 2013. http://sedici.unlp.edu.ar/handle/10915/27537.

[6] **Rivest, R. Adleman L., Dertouzos, M:** "On Data Banks and Privacy Homomorphisms. Foundations of Secure Computation, Academia Press (1978)

[7] **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.

[8] **Benaloh, J.:** "Dense Probabilistic Encryption". Workshop on Selected Areas of Cryptography. pp. 120–128. 1994.

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

[10] **Gentry G.:** "Fully Homomorphic Encryption Using Ideal Lattices". In the 41st ACM Symposium on Theory of Computing (STOC), 2009.

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

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

[13] **Ryan P., Schneider S., Teague V.:** "End-to-End Verifiability in Voting Systems, from Theory to Practice". Voting Systems, from Theory to Practice. IEEE Security & Privacy, 13(3):59–62, 2015.