ACTA DEL JURADO DE LOS PREMIOS "LEONARDO TORRES QUEVEDO"

ESPECIALIDAD DE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

El día 23 de marzo de 2021, se reunió a través de medios telemáticos el Jurado que ha evaluado los proyectos presentados a la Tercera convocatoria (2020) de los Premios "Leonardo Torres Quevedo" en la especialidad de Criptología y Seguridad de la Información.

El Jurado ha decidido, por unanimidad, otorgar el Premio en la convocatoria de 2020 al Trabajo de Fin de Máster presentado por

Marino Tejedor Romero

titulado

Sistema distribuido y remoto de votación electrónica basado en secreto compartido homomórfico de Shamir

El jurado quiere destacar de este trabajo la forma en que el autor aborda un complicado tema de gran actualidad, como es el voto electrónico remoto, proponiendo un sistema distribuido, remoto y verificable de votación electrónica basado en el secreto compartido homomórfico de Shamir que satisface la mayoría de las propiedades deseables de este tipo de sistemas, con la excepción de la imposibilidad de demostrar el voto a un tercero. El proceso de comprobación del voto es sencillo y accesible para cualquier votante sin conocimientos específicos previos, lo cual puede contribuir a su aceptación por parte de usuarios no especializados. El sistema propuesto es una interesante contribución al tema y puede resultar adecuado para ciertos casos de uso, dado que el modelo de amenazas y la mayoría de las suposiciones en las que se basa son razonablemente asumibles y realistas. Por todo ello, se ha considerado este trabajo merecedor del Premio de esta convocatoria.

Por otra parte, a la vista de la calidad de los trabajos presentados, el Jurado ha decidido conceder tres Menciones Especiales a los siguientes Trabajos de Fin de Grado y Fin de Máster (en orden alfabético):

Ferran Alborch Escobar

Lattice-Based Threshold Cryptography (TFG)

En este trabajo de fin de grado se proponen protocolos postcuánticos de descifrado umbral y de generación distribuida de claves cuya seguridad está basada en la dificultad para resolver el problema del aprendizaje con errores en anillos. En el trabajo se muestra que los protocolos son correctos, en el sentido de que su resultado es el que se espera de ellos, y son seguros, dado que son tan difíciles de romper como un problema basado en retículos.

Luis Hernández Álvarez

Towards Privacy–Preserving Sensor–Based Continuous Authentication (TFM)

En este trabajo de fin de máster se revisa en primer lugar el estado del arte de la Autenticación Continua (AC) y de los métodos relacionados con la preservación de la privacidad y, a continuación, se propone un esquema de AC, usando datos obtenidos de sensores y algoritmos de aprendizaje automático, que garantiza la protección de la información mediante Cifrado con Preservación de Formato usando una clave única y secreta por usuario. Los resultados experimentales, utilizando un conjunto de datos reales de teléfonos inteligentes disponible públicamente, muestran que el esquema propuesto permite lograr la autenticación continua de los usuarios con una precisión adecuada y respetando su privacidad. Además de los resultados prácticos, destacan la excelente revisión bibliográfica y la claridad en la exposición del trabajo, así como que haya dado lugar a una publicación en una revista del primer cuartil según el *Journal of Citation Reports*.

Héctor Masip Ardévol

Linkable Attribute-Based Signature (TFM)

En este trabajo de fin de máster se presenta un protocolo útil para construir un esquema de voto electrónico por internet que permite a las autoridades electorales resolver el problema de distinguir si las firmas de los votos se han emitido por un mismo votante o por votantes diferentes, a la vez que se preserva su anonimato. Para ello se utiliza una firma basada en atributos enlazable, un esquema de compromiso y una prueba de conocimiento nulo. En el trabajo se presenta una construcción del esquema propuesto basada en retículos.

Madrid, 23 de marzo de 2021

CCN
centro criptológico nacional

iteft
Instituto de Tecnologías Físicas y de la Información

Fdo.: Agustín Martín Muñoz
(en representación del Jurado)
Instituto de Tecnologías Físicas y de la Información
"Leonardo Torres Quevedo"