ACTA DEL JURADO DE LOS PREMIOS "LEONARDO TORRES QUEVEDO"

ESPECIALIDAD DE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

El día 5 de abril de 2022, se reunió el Jurado que ha evaluado los proyectos presentados a la Cuarta convocatoria (2021) 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 2021 al Trabajo de Fin de Máster presentado por

David Balbás Gutiérrez

titulado

On Secure Administators for Group Messaging Protocols

El Jurado quiere destacar la calidad investigadora de este trabajo y la claridad y solidez de su presentación. En el trabajo se introduce el concepto de acuerdo de clave de grupo continuo administrado (*Administrated Continuous Group Key Agreement*, A-CGKA) como una extensión del de CGKA, que proporciona funcionalidad administrativa. Se describe esta primitiva, se presenta un juego de corrección y se discuten posibles nociones de seguridad asociadas. Posteriormente se presentan dos construcciones de administradores de grupo basados en la noción A-CGKA. La primera es para firmas de administrador individual y la segunda para firmas de grupo dinámico.

Por otra parte, el Jurado ha decidido conceder los dos accésits señalados en la convocatoria de este año a los siguientes Trabajos de Fin de Grado (en orden alfabético):

Aurora Fernández Donaire

Criptografía poscuántica basada en isogenias

En este trabajo se presenta una descripción muy clara y pormenorizada del protocolo de Diffie-Hellman para isogenias supersingulares (*Supersingular Isogeny Diffie-Hellman*, SIDH), base de algunos protocolos poscuánticos presentados en la convocatoria del NIST (*National Institute of Standards and Technology*) para establecer nuevos estándares criptográficos, resistentes a la computación cuántica. Además, se estudia e implementa el protocolo de encapsulamiento de claves para isogenias supersingulares (*Supersingular Isogeny Key Encapsulation*, SIKE) que ha sido considerado como uno de los protocolos alternativos en la tercera ronda de la citada convocatoria. El Jurado destaca la forma didáctica en la que se presentan ambos protocolos, con detalles y explicaciones matemáticas claras de cada uno de los pasos.

MINISTERIO
DE CIENCIA
E INNOVACIÓN
Y
MINISTERIO
DE DEFENSA

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

INSTITUTO DE TECNOLOGÍAS FÍSICAS Y DE LA INFORMACIÓN
"LEONARDO TORRES QUEVEDO"

Alejandro Rodríguez García

Análisis y Evaluación del Circuito Generador de Números Aleatorios Lampert Circuit

El Jurado quiere subrayar el carácter aplicado de este trabajo y su vertiente experimental. El objetivo del mismo es auditar el funcionamiento del circuito generador de números aleatorios llamado Lampert Circuit y desarrollado en el marco del proyecto *Secure Internet of Things*, liderado por la Universidad de Stanford. Para ello se ha analizado el funcionamiento de 100 circuitos fabricados por 4 empresas diferentes. Del análisis realizado, se deduce que el circuito genera números aleatorios válidos para ser utilizados en aplicaciones criptográficas en el ámbito de la Internet de las cosas (*Internet of Things*, IoT), si bien, se señala que el diseño de los circuitos debe evolucionar hacia un sistema más fácilmente implementable y con mayor seguridad.

Madrid, 5 de abril de 2022

CCN
centro criptológico nacional

itefi
Instituto de Tecnologías Físicas y de la Información

HERNANDEZ ENCINAS LUIS FERNANDO - DNI 08950984M

Firmado digitalmente por HERNANDEZ ENCINAS LUIS FERNANDO - DNI 08950984M
Nombre de reconocimiento (DN): c=ES, o=CONSEJO SUPERIOR DE INVESTIGACIONES CIENTIFICAS, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, ou=INSTITUTO DE TECNOLOGIAS FISICAS Y DE LA INFORMACION LEONARDO TO, ou=08950984, serialNumber=IDCES-08950984M, sn=HERNANDEZ ENCINAS, givenName=LUIS FERNANDO, cn=HERNANDEZ ENCINAS LUIS FERNANDO - DNI 08950984M
Fecha: 2022.04.06 08:56:24 +02'00'

Fdo.: Luis Hernández Encinas
(en representación del Jurado)
Instituto de Tecnologías Físicas y de la Información
"Leonardo Torres Quevedo"