ACTA DEL JURADO DE LOS PREMIOS "LEONARDO TORRES QUEVEDO"

ESPECIALIDAD DE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

El día 26 de septiembre de 2024 se reunió el Jurado que ha evaluado los proyectos presentados a la sexta convocatoria (2023) de los **Premios "Leonardo Torres Quevedo"** en la especialidad de **Criptología y Seguridad de la Información**, organizados y patrocinados por el **Instituto de Tecnologías Físicas y de la Información** "Leonardo Torres Quevedo" (ITEFI), de la Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC) y por el **Centro Criptológico Nacional** (CCN), del Centro Nacional de Inteligencia (CNI).

La edición de este año es de especial relevancia por cuanto celebra el 20º aniversario de la creación del CCN.

El Jurado ha decidido, por unanimidad, otorgar el **Premio** en la convocatoria de 2023 en el apartado de **Trabajo de Fin de Grado**, **dotado con 1.000€**, al presentado por

Manuel Gala Daza (TFG-UC3M)

Implementación de Physical Unclonable Functions en Field Programmable Gate Array

El Jurado quiere destacar la calidad de este trabajo y la claridad de su presentación. En él se ha diseñado e implementado una *Physical Unclonable Function* (PUF) confinada basada en los sensores que se encuentran presentes en una FPGA. Se recopilan datos de las respuestas procesadas por la PUF cuando se ejecutan ciertas operaciones en varias FPGA y se clasifican dichas respuestas mediante técnicas de Inteligencia Artificial.

Además, el Jurado ha decidido conceder el **Accésit** señalado en la convocatoria de este año**, dotado con 500€**, al siguiente trabajo:

Gabriel Alberto Luis Freitas (TFG-ULL)

Propuesta de mejora para la implementación en software del cifrado SNOW-Vi

El Jurado quiere subrayar el carácter práctico de este trabajo en el que se propone una mejora de la implementación de la actualización del registro de desplazamiento, una de las operaciones más costosas del sistema de cifrado en flujo SNOW-Vi. El planteamiento propuesto produce una mejora de rendimiento entre el 14,6% y el 34,6%, dependiendo de la arquitectura utilizada.

Por otra parte, el Jurado ha decidido, por unanimidad, otorgar el **Premio** en la convocatoria de 2023 en el apartado de **Proyecto de Fin de Máster**, **dotado con 1.000€**, al presentado por

Miguel Morona Mínguez (PFM-UCM/IMDEA)

Verifiable Computation on encrypted data

En este claro y sólido trabajo se propone un esquema de Computación Verificable que combina técnicas de cifrado y autenticación homomórficos. Se trata de una técnica criptográfica que pretende paliar los riesgos de la computación remota y garantizar la corrección y la privacidad. La técnica propuesta en el trabajo permite una mayor eficiencia en términos del coste de la comunicación entre las partes intervinientes. Además, se incluye tanto una estimación de dicho coste como del tiempo computacional de la ejecución de los algoritmos necesarios.

Además, el Jurado ha decidido conceder el **Accésit** señalado en la convocatoria de este año**, dotado con 500€**, al siguiente trabajo:

Manuel Ruiz Ruiz (PFM-UMA)

Automatización de la certificación de seguridad para aplicaciones Android

Este trabajo aborda el reto de verificar la seguridad de las aplicaciones que se instalan en los dispositivos móviles. Así, se propone la herramienta AndroCIES, que es capaz de automatizar, en gran medida, las evaluaciones necesarias para certificar las aplicaciones móviles según los patrones establecidos por diferentes estándares. La herramienta es capaz de reducir el tiempo empleado en este proceso alrededor de un 20%.

Madrid, 26 de septiembre de 2024

CCN
centro criptológico nacional

itefi
Instituto de Tecnologías Físicas y de la Información

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