

GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:

ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2017

PERSONAL INVESTIGADOR

1. AGUIRRE PASTOR, JOSE VICENTE
2. ALBEZA PIQUERAS, MIGUEL ANGEL
3. ALVAREZ SANCHEZ, RAFAEL IGNACIO
4. BELLIDO IBORRA, PEDRO
5. FERRANDEZ AGULLO, FRANCISCO
6. HUERTAS ILLESCAS, JAVIER
7. MARTINEZ PEREZ, FRANCISCO MIGUEL
8. REQUENA AREVALO, VERONICA
9. SANCHEZ ALBERTOS, JULIA
10. TOMAS ESTEVAN, VIRTUDES
11. ZAMORA GOMEZ, ANTONIO

LÍNEAS DE INVESTIGACIÓN

1. El estudio, diseño y evaluación de códigos LDPC y convolucionales con aplicaciones a la criptografía de clave pública y protocolos criptográficos.
2. Firma digital
3. Kernel criptográfico
4. Sistema Multiplataforma de Comunicaciones Seguras

PROYECTOS

Públicos

1. "Análisis y visualización de datos en redes complejas. Aplicación a las redes", tin2014-53855-p , 36 meses, 25.289,00 €, TORTOSA GRAU, LEANDRO.
2. "Códigos convolucionales sobre canales de borrado y códigos orbitales para codificación de red.", aico/2017/128 , 24 meses, 29.600,00 €, CLIMENT COLOMA, JOAN JOSEP.
3. "Criptología y seguridad computacional", vigrob-025 , 12 meses, 113,00 €, ZAMORA GOMEZ, ANTONIO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Capítulos en libros:

1. Climent, Joan-Josep; Requena, Verónica; Soler-Escrivà, Xaro "A Construction of orbit codes" en "Coding Theory and Applications. Proceedings of the 5th International Castle Meeting, ICMCTA 2017", ISBN: 978-3-319-66277-0, Switzerland, Springer International Publishing, pp. 72-83, (2017)

Artículos en publicaciones periódicas:

2. Aguirre, J. V.; Alvarez, R.; Zamora, A. "Darkcube: A k-Hypercube based P2P VoIP protocol", Peer-to-Peer Networking and Applications, vol. 10, pp. 170-183, (2017)
3. Alvarez, R.; Andrade, A.; Santos, I.; Zamora, A. "AES-CTR as a Password-Hashing Function", Advances in Intelligent Systems and Computing, vol. 649, pp. 610-617, (2017)
4. Álvarez, R.; Cabellero-Gil, C.; Santonja, J.; Zamora, A. "Algorithms for Lightweight Key Exchange", Sensors, vol. 17, pp. 1517-, (2017)
5. Climent, Joan-Josep; Requena, Verónica; Soler-Escrivà, Xaro "A Construction of orbit codes", Lecture Notes in Computer Science, vol. 10495, pp. 72-83, (2017)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Internacionales

1. ALVAREZ, R. "El Protocolo IPFS", MOBILE TOOLS FOR EMERGENCIES AND CRITICAL INFRASTRUCTURES, Madrid, Diciembre 2017.
2. ALVAREZ, R.; ANDRADE, A.; SANTOS, I.; ZAMORA, A. "AES-CTR as a Password-Hashing Function", COMPUTATIONAL INTELLIGENCE IN SECURITY FOR INFORMATION SYSTEMS, León, Septiembre 2017.
3. CLIMENT, JOAN-JOSEP; REQUENA, VERÓNICA; SOLER-ESCRIVÀ, XARO. "A construction of orbit codes", INTERNATIONAL CASTLE MEETING ON CODING THEORY AND APPLICATIONS, Vihula Manor, Agosto 2017.
4. SANTOS-GONZÁLEZ I., MOLINA-GIL J., RIVERO-GARCÍA A., ZAMORA A., ÁLVAREZ R. "A Comparative Study for Real-Time Streaming Protocols Implementations", COMPUTER AIDED SYSTEMS THEORY, Las Palmas de Gran Canaria, Febrero 2017.
5. ZAMORA, A. "Topología en k-hipercubo para comunicaciones en entornos de emergencia", MOBILE TOOLS FOR EMERGENCIES AND CRITICAL INFRASTRUCTURES, Madrid, Diciembre 2017.