GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2016

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.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Capítulos en libros:

1. Rafael Álvarez, Francisco–Miguel Martínez y Antonio Zamora "Hacia la optimización de un generador pseudoaleatorio matricial" en "Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–608–9470–4, Palma de Mallorca, Universitat de les Illes Balears, pp. 264–269, (2016)
2. Requena, V; Ortega, P. "Las matemáticas de la Gran Pirámide" en "El secreto de los números" , ISBN: 978–84–9717–490–9, Alicante, Publicaciones de la Universidad de Alicante, pp. 245–257, (2016)

Artículos en publicaciones periódicas:

3. Álvarez, R.; Santonja, J.; Zamora, A. "Algorithms for Lightweight Key Exchange" , Lecture Notes in Computer Science , vol. 10070, pp. 536–543, (2016)
4. Alvarez, R.; Zamora, A. "Randomness analysis and generation of key–derived s–boxes" , Logic Journal of the IGPL , vol. 24, pp. 68–79, (2016)
5. Álvarez, R.; Zamora, A. "Using Spritz as a Password–Based Key Derivation Function" , Advances in Intelligent Systems and Computing , vol. 527, pp. 518–525, (2016)

TESIS DOCTORALES DEFENDIDAS

1. AGUIRRE PASTOR, JOSE VICENTE, "PROTOCOLO MULTIPLATAFORMA NO CENTRALIZADO PARA COMUNICACIONES MULTIMEDIA SEGURAS", Directores: ALVAREZ SANCHEZ, RAFAEL IGNACIO / ZAMORA GOMEZ, ANTONIO Enero 2016.
2. MARTINEZ PEREZ, FRANCISCO MIGUEL, "CRIPTOSISTEMAS DE CIFRADO EN FLUJO BASADOS EN MATRICES TRIANGULARES CON MULTIPLES BLOQUES", Directores: ALVAREZ SANCHEZ, RAFAEL IGNACIO / ZAMORA GOMEZ, ANTONIO Enero 2016.

COMUNICACIONES A CONGRESOS

Nacionales

1. PASCUAL VILLALOBOS, C.; PÉREZ BENEYTO, J.; POMARES BAEZA, J.; ÁLVAREZ SÁNCHEZ, R.I.; PÉREZ SÁNCHEZ, J.C.; ZORNOZA GÓMEZ, E.; VARÓ GALVAÑ;, P.J.; PRATS RICO, D.; GIMENO NIEVES, E.; GARCIA–BARBA, J. "Análisis del abandono en las titulaciones de Máster de la EPS–UA", JORNADAS DE REDES DE INVESTIGACIÓN EN DOCENCIA UNIVERSITARIA, Alicante, Junio 2016.
2. RAFAEL ÁLVAREZ, FRANCISCO–MIGUEL MARTÍNEZ Y ANTONIO ZAMORA. "Hacia la optimización de un generador pseudoaleatorio matricial", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Mahón, Menorca, Octubre 2016.

Internacionales

1. ÁLVAREZ, R.; SANTONJA, J.; ZAMORA, A. "Algorithms for Lightweight Key Exchange", INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING & AMBIENT INTELLIGENCE, San Bartolomé de Tirajana, Gran Canaria, Noviembre 2016.
2. ÁLVAREZ, R., ZAMORA, A. "Efficient Cryptography for Critical Infrastructure and Emergency Applications", MOBILE TOOLS FOR EMERGENCIES AND CRITICAL INFRASTRUCTURES, Maspalomes, Gran Canaria, Noviembre 2016.
3. ÁLVAREZ, R.; ZAMORA, A. "Using Spritz as a Password–Based Key Derivation Function", COMPUTATIONAL INTELLIGENCE IN SECURITY FOR INFORMATION SYSTEMS, San Sebastián, Octubre 2016.