GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2012

PERSONAL INVESTIGADOR

1. AGUIRRE PASTOR, JOSE VICENTE
2. ALBEZA PIQUERAS, MIGUEL ANGEL
3. ALVAREZ SANCHEZ, RAFAEL IGNACIO
4. BELLIDO IBORRA, PEDRO
5. CLIMENT COLOMA, JOAN JOSEP
6. DIAZ CARDELL, SARA
7. FERRANDEZ AGULLO, FRANCISCO
8. GARCIA GARCIA, FCO. JESUS
9. HUERTAS ILLESCAS, JAVIER
10. MARTINEZ PEREZ, FRANCISCO MIGUEL
11. REQUENA AREVALO, VERONICA
12. SANCHEZ ALBERTOS, JULIA
13. TOMAS ESTEVAN, VIRTUDES
14. TORTOSA GRAU, LEANDRO
15. VICENT FRANCES, JOSE FRANCISCO
16. 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. "Aplicaciones de las matrices por bloques a la criptofrafía (CriptoMat).", gre10–34 , 24 meses, 7.500,00 €, VICENT FRANCES, JOSE FRANCISCO.
2. "Ayuda para la formación de personal investigador de caracter predoctoral", bfpi/2008/138 , 24 meses, DIAZ CARDELL, SARA.
3. "Codis correctors d'errors versus codis de longitud variable. (Invitado: Pin, Jean–Eric)", inv12–22 , 1.000,00 €, CLIMENT COLOMA, JOAN JOSEP.

4. "Criptología y seguridad computacional", vigrob–025 , 12 meses, 2.725,00 €, ZAMORA GOMEZ, ANTONIO.
5. "Diseño de primitivas criptográficas avanzadas basadas en matrices TSB (CriptoATSB)", gv/2011/001 , 24 meses, 12.000,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.
6. "Diseño de primitivas criptográficas basadas en matrices TSB (Cripto TSB)", gre09–02 , 24 meses, 3.500,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.
7. "Estudio, construcción e implementación de turbo códigos, códigos convolucionales y códigos LDPC. Aplicaciones criptográficas", mtm2011–24858 , 36 meses, 37.752,00 €, CLIMENT COLOMA, JOAN JOSEP.
8. "Matrices triangulares por bloques y sus aplicaciones criptográficas", gv/2012/111 , 24 meses, 8.500,00 €, VICENT FRANCES, JOSE FRANCISCO.
9. "RANDOM NETWORK CODING AND DESIGNS OVER GF(Q)", cost action ic1104 , 48 meses, 16.000,00 €,

Privados

No hay proyectos para mostrar

PUBLICACIONES

Libros:

1. Tortosa Grau, L.; Vicent Francés, J–F. "Geometría moderna para Ingeniería." , ISBN: 9788499487090, Alicante., Editorial ECU, (2012)

Capítulos en libros:

2. Álvarez, R., Ferrández, F., Sánchez, J., Zamora, A. "Avances en la función hash Tangle" en "Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–615–9933–2, Arrasate – Mondragon, Mondragon Uniberstsitatea, pp. 41–44, (2012)
3. Álvarez, R., Martínez, F–M., Vicent, J–F., Zamora, A. "Extensión y parametrización de un generador pseudoaleatorio matricial" en "Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–615–9933–2, Arrasate – Mondragon, Mondragon Uniberstsitatea, pp. 29–34, (2012)
4. Climent, Joan–Josep; Napp, Diego; Perea, Carmen; Pinto, Raquel "MDS 2D convolutional codes" en "Electronic Proceedings of the 20th International Symposium on Mathematical Theory of Networks and Systems" , ISBN: 978–0–646–58062–3, Melbourne, Australia, Editorial del Congreso (versión electrónica), pp. 264.1–264.4, (2012)
5. Climent, Joan–Josep; García, Francisco, J.; Requena, Verónica "Una nueva construcción de funciones bent de 2k variables a partir de una base de F22k" en "Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–615–9933–2, Arrasate – Mondragon, Mondragon Uniberstsitatea, pp. 93–98, (2012)
6. Climent, Joan–Josep; López–Ramos, Juan Antonio; Navarro, Pedro R.; Tortosa, Leandro "A key agreement protocol for distributed secure multicast on a non–commutative ring" en "Proceedings of the 12th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2012)" , ISBN: 978–84–615–5392–1, La Manga, Murcia, Vigo Aguiar, Jesús, pp. 329–335, (2012)

Artículos en publicaciones periódicas:

7. Agryzkov, T.; Oliver, J.L.; Tortosa, L.; Vicent, J.F. "An algorithm for ranking the nodes of an urban network based on the concept of PageRank vector." , Applied Mathematics and Computation , vol. 219, pp. 2186–2193, (2012)
8. Álvarez, R.; Martínez, F.; Vicent, J–F.; Zamora, A. "Cryptographic Applications of 3x3 Block Upper Triangular Matrices" , Lecture Notes in Computer Science , vol. 7209, pp. 97–104, (2012)

9. Álvarez, R.;Gallardo, C.;Vicent, J.;Zamora, A. "A quick exponentiation algorithm for 3 × 3 block upper triangular matrices" , Applied Mathematics and Computation , vol. 219, pp. 2004–2016, (2012)
10. Climent, Joan–Josep; García, Francisco J.; Requena, Verónica "Construction of Bent Functions of 2k Variables from a Basis of F22k" , International Journal of Computer Mathematics , vol. 89, pp. 863–880, (2012)
11. Climent, Joan–Josep; Napp, Diego; Perea, Carmen; Pinto, Raquel "A construction of MDS 2D convolutional codes of rate 1/n based on superregular matrices" , Linear Algebra and Its Applications , vol. 437, pp. 766–780, (2012)
12. Climent, Joan–Josep; Navarro, Pedro R.; Tortosa, Leandro "Key exchange protocols over noncommutative rings. The case of End(ZpxZp2)" , International Journal of Computer Mathematics , vol. 89, pp. 1753–1763, (2012)

TESIS DOCTORALES DEFENDIDAS

1. DIAZ CARDELL, SARA, "CONSTRUCTIONS OF MDS CODES OVER EXTENSION ALPHABETS", Director: CLIMENT COLOMA, JOAN JOSEP Agosto 2012.

COMUNICACIONES A CONGRESOS

Sin concretar

1. M. J. CASTEL DE HARO; VC. MIGALLÓN GOMIS; R. SATORRE CUJERDA; L. TORTOSA ANDREU; C. VILLAGRÁ ARNEDO; A. GARRIDO ALENDA; P. MARTÍNEZ BARCO; P. PERNÍAS PECO; F. BROTONS MOLINERO; J. ESCLAPES JOVER; A. MÁRQUEZ RUIZ; E. COLOMINA CLIMENT. "Resultados Implantación Primer Curso nuevo Grado en Ingeniería Multimedia", X JORNADAS DE REDES DE INVESTIGACIÓN EN DOCENCIA UNIVERSITARIA. LA PARTICIPACIÓN Y EL COMPROMISO DE LA COMUNIDAD UNIVERSITARIA, Universidad de Alicante, Junio 2012.

Nacionales

1. ÁLVAREZ, R.; FERRÁNDEZ, F., SÁNCHEZ, J., ZAMORA, A. "Avances en la función hash Tangle", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Donostia–San Sebastián, Septiembre 2012.
2. ÁLVAREZ, R.; MARTÍNEZ, F–M., VICENT, J–F., ZAMORA, A. "Extensión y parametrización de un generador pseudoaleatorio matricial", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Donostia–San Sebastián, Septiembre 2012.
3. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP; ROCA, ALICIA. "A system approach to the fast correlation attack to linear feedback shift registers", ALGEBRA LINEAL, ANÁLISIS MATRICIAL Y APLICACIONES, Leganés (Madrid), Junio 2012.
4. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO, J.; REQUENA, VERÓNICA. "On the construction of bent functions of 2k vriables from a primitive polynomial of degree k", ALGEBRA LINEAL, ANÁLISIS MATRICIAL Y APLICACIONES, Leganés (Madrid), Junio 2012.
5. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO, J.; REQUENA, VERÓNICA. "Una nueva construcción de funciones bent de 2k variables a partir de una base de $\mathbb{F}_{2}^{2k}$", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Donostia–San Sebastián, Septiembre 2012.
6. TORTOSA, L. "¿Qué podemos hacer con un conjunto de puntos?", IV JORNADES DE L`ASSOCIACIÓ CATALANA DE GEOGEBRA, Barcelona, Febrero 2012.

Internacionales

1. ÁLVAREZ, R.; MARTÍNEZ, F.; VICENT, J–F.; ZAMORA, A. "Cryptographic Applications of 3x3 Block Upper Triangular Matrices", HYBRID ARTIFICIAL INTELLIGENT SYSTEMS, Salamanca, Marzo 2012.

2. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP; REQUENA, VERÓNICA. "On the construction and decoding of MDS Fq – linear codes", CODES AND TOPOLOGY, Castro Urdiales (Cantabria), Mayo 2012.
3. CLIMENT, JOAN–JOSEP; NAPP, DIEGO; PEREA, CARMEN; PINTO, RAQUEL. "MDS 2D convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Melbourne, Julio 2012.
4. CLIMENT, JOAN–JOSEP; LÓPEZ–RAMOS, JUAN ANTONIO; NAVARRO, PEDRO R.; TORTOSA, LEANDRO. "A key agreement protocol for distributed secure multicast on a non–commutative ring", CONFERENCE ON COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, La Manga, Murcia, Julio 2012.