GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2013

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. "Ataques pro correlación sobre LFSR generalizados basados en códigos...", apostd/2013/081 , 24 meses, 92.970,00 €, DIAZ CARDELL, SARA.
3. "Criptología y seguridad computacional", vigrob–025 , 12 meses, 1.471,00 €, ZAMORA GOMEZ, ANTONIO.

4. "Decodificación de códigos producto sobre un canal con borrado. (Invitado: Rosenthal, Joachim)", inv13–05 , 1.000,00 €, CLIMENT COLOMA, JOAN JOSEP.
5. "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.
6. "Matrices triangulares por bloques y sus aplicaciones criptográficas", gv/2012/111 , 24 meses, 8.500,00 €, VICENT FRANCES, JOSE FRANCISCO.
7. "RANDOM NETWORK CODING AND DESIGNS OVER GF(Q)", cost action ic1104 , 48 meses, 16.000,00 €,

Privados

No hay proyectos para mostrar

PUBLICACIONES

Capítulos en libros:

1. V. Gilart Iglesias; D. Ruiz Fernández; H. Mora Mora; D. Marcos Jorquera; F.J. Ferrández Pastor; A. Fuster Guilló; F.A. Pujol López; J.V. Berná Martínez; M.M. Pujol López; A. Botía Martínez; D. Viejo Hernándo; F.J. Gallego Durán; R.I. Álvarez Sánchez; A. Zamora Gómez; D. Gallardo López; M.P. Arques Corrales; M.A. Cazorla Quevedo; O. Colomina Pardo; R. Satorre Cuerda; J. Penadés; A. Montoyo Guijarro; J. Calera Rubio; F. Moreno Seco; P.M. Martínez Barco; J. Gómez Ortega; M.P. Moreda Pozo; J.C Trujillo Mondéjar; A.M. Corbí Bellot; C. Cachero Castro; J.A. Pérez Ortiz; J.R. Rico Juan; J.L. Vicedo González; J.A. Berná Galiano; J. Pomares Baeza; E. Colomina Climent "Red de coordinación e implementación eficaz del Cuarto Curso de la titulación de Grado en Ingeniería Informática" en "La producción científica y la actividad de innovación docente en proyectos de redes" , ISBN: 978–84–695–9336–3, Alicante, ICE/Vicerrectorado de Estudios e Innovación Educativa, Universidad de Alicante, pp. 477–493, (2013)
2. V. Gilart Iglesias; J.M. Mora Pascual; J. Azorín López; H. Mora Mora; J.L. Albentosa Mora; M.P. Arques Corrales; R.I. Álvarez Sánchez; F. Llorens Largo; J.M. Salinas Serrano; J. Arnal García; A. Montoyo Guijarro; J.N. Mazón López; J.C. Trujillo Mondéjar; C. Cachero Castro; J.A. Pérez Ortiz; F.J. Gil Chica "Seguimiento de calidad de las asignaturas del Máster Universitario en Ingeniería Informática" en "La producción científica y la actividad de innovación docente en proyectos de redes" , ISBN: 978–84–695–9336–3, Alicante, ICE/ Vicerrectorado de Estudios e Innovación Educativa, Universidad de Alicante, pp. 456–476, (2013)

Editores de revistas

3. "The Scientific World Journal (Online)" , 01/10/2013 , 30/09/2016 , (2013)

Artículos en publicaciones periódicas:

4. Agryzkov, T.; Oliver, J.L.; Tortosa, L.; Vicent, J.F. "A model to visualize information in a complex streets` network." , Advances in Intelligent Systems and Computing , vol. 217, pp. 129–136, (2013)
5. Cardell, Sara D.; Climent, Joan–Josep; Requena, Verónica "A construction of MDS array codes" , WIT Transactions on Information and Communication Technologies , vol. 45, pp. 47–58, (2013)
6. Climent, Joan–Josep; García, Francisco J.; Requena, Verónica "The degree of a Boolean function and some algebraic properties of its support" , WIT Transactions on Information and Communication Technologies , vol. 45, pp. 25–36, (2013)
7. Climent, Joan–Josep; López–Ramos, Juan Antonio; Navarro, Pedro R.; Tortosa, Leandro "Key agreement protocols for distributed secure multicast over the ring Ep(m)" , WIT Transactions on Information and Communication Technologies , vol. 45, pp. 13–24, (2013)
8. Tortosa, L. "Fútbol, geometría y otros problemas." , Sociedad de la Información , vol. 41, pp. –, (2013)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Nacionales

1. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO, J.; REQUENA, VERÓNICA. "Construcción de funciones bent de 2k variables a partir de una base de $\mathbb{F}_{2} ^{2k}$", CONGRESO DE LA REAL SOCIEDAD MATEMÁTICA ESPAÑOLA, Santiago de Compostela, Enero 2013.
2. TORTOSA, L. " Voronoi, el fútbol y otras cuestiones. ", V JORNADES DE L`ASSOCIACIÓ CATALANA DE GEOGEBRA, Barcelona, Febrero 2013.
3. TORTOSA, LEANDRO. " Fútbol, geometría y otros problemas. ", I DÍA DE GEOGEBRA DE CASTILLA LA MANCHA, Albacete, Marzo 2013.

Internacionales

1. AGRYZKON, T.; OLIVER, J.L.; TORTOSA, L.; VICENT, J. "A model to visualize information in a complex streets` network", INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING AND ARTIFICIAL INTELLIGENCE, Salamanca, Mayo 2013.
2. AGRYZKOV, T.; OLIVER, J.L.; TORTOSA, L.; VICENT, J.F. "Evaluating the Impact of Inner Urban Reform Plans Using a Pagerank Algorithm", EUROPEAN CONFERENCE ON COMPLEX SYSTEMS, Barcelona, Septiembre 2013.
3. ÁLVAREZ, R.; ZAMORA, A. "Randomness Analysis of Key–Derived S–Boxes", COMPUTATIONAL INTELLIGENCE IN SECURITY FOR INFORMATION SYSTEMS, Salamanca, Septiembre 2013.
4. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP; REQUENA, VERÓNICA. " A construction of MDS array codes", INTERNATIONAL CONFERENCE ON DATA MANAGEMENT AND SECURITY: APPLICATIONS IN MEDICINE, SCIENCES AND ENGINEERING, Elche, Mayo 2013.
5. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP; REQUENA, VERÓNICA. "Coding and decoding of MDS Fq–linear codes based on superregular matrices", CONFERENCE ON RANDOM NETWORK CODES AND DESIGNS OVER GF(Q), Ghent, Septiembre 2013.
6. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO J.; REQUENA, VERÓNICA. "The degree of a Boolean function and some algebraic properties of its support", INTERNATIONAL CONFERENCE ON DATA MANAGEMENT AND SECURITY: APPLICATIONS IN MEDICINE, SCIENCES AND ENGINEERING, Elche, Mayo 2013.
7. CLIMENT, JOAN–JOSEP; LÓPEZ–RAMOS, JUAN ANTONIO; NAVARRO, PEDRO R.; TORTOSA, LEANDRO. " Key agreement protocols for distributed secure multicast over the ring ep(m). ", INTERNATIONAL CONFERENCE ON DATA MANAGEMENT AND SECURITY: APPLICATIONS IN MEDICINE, SCIENCES AND ENGINEERING, Elche, Mayo 2013.