GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2011

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. "Acabar un treball començat durant la visita a la Universidade de Aveiro en desembre de 2010. Impartir una conferència. Anàlisi de posibles col·laboracions futures (Invitado Rocha Pinto, Maria Raquel)", inv11–11 , 1.200,00 €, CLIMENT COLOMA, JOAN JOSEP.
2. "Aplicaciones de las matrices por bloques a la criptofrafía (CriptoMat).", gre10–34 , 24 meses, 7.500,00 €, VICENT FRANCES, JOSE FRANCISCO.
3. "Ayuda para la formación de personal investigador de caracter predoctoral", bfpi/2008/138 , 24 meses, DIAZ CARDELL, SARA.

4. "Computación de altas prestaciones y paralelismo", ati07–06 , 36 meses, 22.000,00 €, PENADES MARTINEZ, JOSE LEANDRO.
5. "CONSTRUCCIÓN DE CÓDIGOS CORRECTORES DE ERRORES BASADOS EN GRAFOS", pr2010–0126 , 3 meses, 10.700,00 €, CLIMENT COLOMA, JOAN JOSEP.
6. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas", acomp/2011/005 , 12 meses, 5.000,00 €, CLIMENT COLOMA, JOAN JOSEP.
7. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas.", mtm2008–06674–c02–01 , 36 meses, 34.727,00 €, CLIMENT COLOMA, JOAN JOSEP.
8. "Criptología y seguridad computacional", vigrob–025 , 12 meses, 2.899,00 €, ZAMORA GOMEZ, ANTONIO.
9. "Diseño de primitivas criptográficas avanzadas basadas en matrices TSB (CriptoATSB)", gv/2011/001 , 24 meses, 12.000,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.
10. "Diseño de primitivas criptográficas basadas en matrices TSB (Cripto TSB)", gre09–02 , 24 meses, 3.500,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Libros:

1. Vicent, J.F.; Martínez, F.M.; Tortosa, L "MANUAL D`OO–WRITER" , ISBN: 9788497171557, Alicante, Secretariat de Promoció del Valencià – Universitat d'Alacant, (2011)

Capítulos en libros:

2. Cardell, Sara D.; Climent, Joan–Josep; Requena, Verónica "A Construction of MDS Array Codes Based on Companion Matrices" en "3rd International Castle Meeting on Coding Theory and applications" , ISBN: 978–84–490–2688–1, Barcelona, Universitat Autònoma de Barcelona, pp. 87–92, (2011)
3. Cardell, Sara D.; Climent, Joan–Josep; Requena, Verónica "MDS array codes based on superregular matrices" en "Proceedings of the 11th Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE2011)" , ISBN: 978–84–614–6167–7, España, Editorial del Congreso, pp. 290–295, (2011)
4. Climent, Joan–Josep; García, Francisco J.; Requena, Verónica "Construction of bent functions of n variables from a basis of F2^n" en "Proceedings of the 11th Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE2011)" , ISBN: 978–84–614–6167–7, España, Editorial del Congreso, pp. 350–356, (2011)
5. Climent, Joan–Josep; Napp, Diego; Perea, Carmen; Pinto, Raquel "Maximum Distance Separable 2D Convolutional Codes of Rate 1/n" en "3rd International Castle Meeting on Coding Theory and applications" , ISBN: 978–84–490–2688–1, Barcelona, Universitat Autònoma de Barcelona, pp. 93–97, (2011)
6. Climent, Joan–Josep; Navarro, Pedro R.; Tortosa, Leandro "Key exchange protocols over noncommutative rings. The case End(Zp x Zp^2)." en "Proceedings of the 11th Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE2011)" , ISBN: 978–84–614–6167–7, España, Editorial del Congreso, pp. 357–364, (2011)
7. Gilart V.; Soriano A.; Jimeno A.; Compañ P.; Penadés J.; Vicent J.; Requena J.; Suárez A.; Marco M.; Pertusa A.; Gallego S. "Red de seguimiento de la calidad de las asignaturas de primer curso del Grado en Ingeniería Informática" en "Redes de investigación docente universitaria: innovaciones metodológicas" , ISBN: 978–84–695–1151–0, Alicante, Universidad de Alicante, pp. 1182–1198, (2011)

8. Martínez, F.; Oliver,J.L.;Tortosa, L.;Vicent, J.F. "A Neural Network Algorithm to Simplify 2D Meshes" en "RECENT ADVANCES IN COMPUTER COMUNICATIONS, APPLIED SOCIAL SCIENCE AND MATHEMATICS" , ISBN: 978–1–61804–030–5, Barcelona, WSEAS Press, pp. 110–115, (2011)

Artículos en publicaciones periódicas:

9. Álvarez, R.; Vicent, J–F.; Zamora A. "Improving the Message Expansion of the Tangle Hash Function" , Lecture Notes in Computer Science , vol. 6694, pp. 183–189, (2011)
10. Climent, Joan–Josep; Navarro, Pedro R.; Tortosa, Leandro "On the arithmetic of the endomorphisms ring End(Zp × Zp2)" , Applicable Algebra in Engineering Communication and Computing , vol. 22, pp. 91–108, (2011)
11. Oliver, J.L.; Tortosa, L.; Vicent, J.F. "An application of a self–organizing model to the design of urban transport networks." , Journal of Intelligent & Fuzzy Systems , vol. 22, pp. 141–154, (2011)
12. Tortosa, L.; Vicent, J.F.; Oliver, J.L. "A neural network model to develop actions in urban complex systems represented by 2D meshes." , International Journal of Computer Mathematics , vol. 88, pp. 3361–3379, (2011)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Internacionales

1. ÁLVAREZ, R.; VICENT, J–F.; ZAMORA, A. "Improving the Message Expansion of the Tangle Hash Function", COMPUTATIONAL INTELLIGENCE IN SECURITY FOR INFORMATION SYSTEMS, Torremolinos (Málaga), Junio 2011.
2. ÁLVAREZ, R.; VICENT, J–F.; ZAMORA, A. "Advances in the Tangle Hash Function", SPANISH CRYPTOGRAPHY DAYS, Murcia, Noviembre 2011.
3. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP, REQUENA, VERÓNICA. "MDS array codes based on superregular matrices", INTERNATIONAL COFERENCE ON COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Benidorm, Junio 2011.
4. CARDELL, SARA D.; CLIMENT, JOAN–JOSEP; REQUENA, VERÓNICA. "A construction of MDS array codes based on companion matrices", INTERNATIONAL CASTLE MEETING ON CODING THEORY AND APPLICATIONS, Barceloa, Septiembre 2011.
5. CARDELL, S.D.; CLIMENT, J.–J.; REQUENA, V. "Another construction of MDS array codes", WORKSHOP ON CODING AND SYSTEMS, Aveiro, Junio 2011.
6. CARDELL, S.D.; REQUENA, V. "Cmmse 2011", COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Benidorm (Alicante), Junio 2011.
7. CLIMENT, J.–J.; NAPP, D.; PEREA, C.; PÎNTO, R. "2D MDS convolutional codes of rate 1/n ", WORKSHOP ON CODING AND SYSTEMS, Aveiro, Junio 2011.
8. CLIMENT, JOAN–JOSEP. "Maximum distance separable 2D convolutional codes of tate 1/n based on superregular matrices", INTERNATIONAL CONFERENCE ON NON ASSOCIATIVE ALGEBRA AND ITS APPLICATIONS, Zaragoza, Noviembre 2011.
9. CLIMENT, JOAN–JOSEP. "Maximum distance separable codes", DAGSTUHL SEMINAR ON CODING THEORY, Dagstuhl, Noviembre 2011.
10. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO J.; REQUENA, VERÓNICA. "Construction of bent functions of n variables from a basis of F2^n", INTERNATIONAL COFERENCE ON COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Benidorm, Junio 2011.

11. CLIMENT, JOAN–JOSEP; NAPP, DIEGO; PEREA, CARMEN; PINTO, RAQUEL. "Maximum Distance Separable 2D Convolutional Codes of Rate 1/n", INTERNATIONAL CASTLE MEETING ON CODING THEORY AND APPLICATIONS, Barceloa, Septiembre 2011.
12. CLIMENT, JOAN–JOSEP; NAVARRO, PEDRO R.; TORTOSA, LEANDRO. " Key exchange protocols over noncommutative rings. The case end(zpxzp2)", INTERNATIONAL COFERENCE ON COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Benidorm, Junio 2011.
13. MARTÍNEZ, F.; OLIVER,J.L.;TORTOSA, L.;VICENT, J.F. "A Neural Network Algorithm to Simplify 2D Meshes", RECENT ADVANCES IN COMPUTERS COMMUNICATIONS, APPLIED SOCIAL SCIENCE AND MATHEMATICS, Barcelona, Septiembre 2011.