GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2006

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. FERRANDEZ AGULLO, FRANCISCO
7. GARCIA GARCIA, FCO. JESUS
8. HUERTAS ILLESCAS, JAVIER
9. REQUENA AREVALO, VERONICA
10. SANCHEZ ALBERTOS, JULIA
11. TORTOSA GRAU, LEANDRO
12. VICENT FRANCES, JOSE FRANCISCO
13. 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. "Construcción de códigos convolucionales. Algoritmos secuenciales y paralelos de decodificación", mtm2005–05759 , 36 meses, 41.650,00 €, CLIMENT COLOMA, JOAN JOSEP.
2. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.795,56 €, ZAMORA GOMEZ, ANTONIO.
3. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 3.084,14 €, ZAMORA GOMEZ, ANTONIO.
4. "Sistema Multiplataforma de Comunicaciones Seguras (SIMCOS)", gv06/018 , 24 meses, 26.425,00 €, ZAMORA GOMEZ, ANTONIO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Capítulos en libros:

1. Arnal, J.; Bernabeu, R.; Gomis, J.; Migallon, V.; Penadés, J.; Ramón, S.; Requena, V.; Reverte, J.R. "Análisis de metodologías docentes ECTS para la asignatura Matemática Discreta en los estudios de Informática" en "La reconfiguración curricular en el escenario universitario. Redes de Investigación Docente en el Espacio Europeo de Educación Superior. Vol. II" , ISBN: 84–268–1269–4, Alicante, Universidad de Alicante, pp. 107–129, (2006)
2. Arnal, J.; Bernabeu, R.; Gomis, J.; Migallón, V.; Penadés, J.; Ramón, S.; Requena, V.; Reverte, J.R. "Investigación en metodologías docentes ECTS para la asignatura Matemática Discreta en las titulaciones de informática" en "IV Jornadas de Redes de Investigación en Docencia Universitaria. La construcción colegiada del modelo docente universitario del siglo XXI" , ISBN: 84–690–0931–1, Alicante, Universidad de Alicante, pp. 1–13, (2006)
3. Arnal, J.; Bernabeu, R.; Gomis, J.; Migallón, V,; Penadés, J.; Requena, V.; Reverte, J. "Estrategias docentes para motivar al alumnado de Matemática Discreta de las titulaciones de Informática" en "Actas de las XII Jornadas de Enseñanza Universitaria de la Informática (JENUI 2006)" , ISBN: 84–9732–545–1, , Thomson, pp. 25–32, (2006)
4. Climent, J.J.; García, F.J.; Requena, V. " A new iterative method to construct bent functions" en "Proceedings of the 5th International Conference on Information Security and Privacy" , ISBN: 960–8457–56–4, , WSEAS Press, pp. 19–22, (2006)
5. Climent, J.J.; García, F.J.; Requena, V. "On the iterative construction of bent functions" en "Proceedings of the 5th International Conference on Information Security and Privacy" , ISBN: 960–8457–56–4, , WSEAS Press, pp. 15–18, (2006)
6. Climent, J.–J.; Herranz, V.; Perea, C "A composite linear time invariant system and its applications to convolutional codes" en "Proceedings of the Fifth International Conference on Engineering Computational Technology" , ISBN: 1–905088–11–6 , , Civil–Comp Press, pp. 1–17, (2006)
7. Climent, J.–J.; Herranz, V.; Perea, C. "Some applications of the inclusion principe to convolutional codes" en "Electronic Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2006)" , ISBN: aa, Kyoto (Japón), Editorial del Congreso (versión electrónica), pp. 197–202, (2006)
8. Josep Arnal García, Ricardo Bernabeu Rico, José Javier Gomis Castelló, Violeta Migallón Gomis, José Penadés Martínez, Serge Ramon, Veronica Requena Arevalo, Juan Rafael Reverte Bernabeu "Metodologías docentes ECTS para Matemática Discreta en las titulaciones de Informática" en "Actas del IV Congreso Internacional de Docencia Universitaria e Innovación (CIDUI)" , ISBN: 84–7653–886–3, Barcelona, Servei de Publicacions de la Universitat Politècnica de Catalunya., pp. 1–16, (2006)

Artículos en publicaciones periódicas:

9. Aguirre, J.; Álvarez, R.; Noguera, J.; Tortosa, L.; Zamora, A. "Secure VoIP and Instant Messaging on Small PDA Devices" , WSEAS Transactions on Computers , vol. 5, pp. 171–176, (2006)
10. Aguirre, J–V.; Noguera, J.; Tortosa, L.; Zamora, A. "An Exercises Editor for an E–Learning Environment." , Transactions on Advances in Engineering Education , vol. 3, pp. 34–40, (2006)
11. Álvarez, R.; Ferrández, F.; Vicent, J.–F.; Zamora, A. "Applying quick exponentiation for block upper triangular matrices" , Applied Mathematics and Computation , vol. 183, pp. 729–737, (2006)
12. Álvarez, R.; Oliver, J.; Vicent, J.; Zamora, A. "Improving GSM Security for Voice and Text Data Transmission" , WSEAS Transactions on Computers , vol. 5, pp. 165–170, (2006)

13. Climent, J.J. "Edició de Textos Científics i Tècnics amb LaTeX" , Quaderns de la Col·lecció Joan Fuster. Secretariat de Promoció del Valencià. Universitat d'Alacant , vol. 76, pp. 1–248, (2006)
14. Climent, J.–J.; Ferrández, F.; Vicent, J.F.; Zamora, A. "A nonlinear elliptic curve cryptosystem based on matrices" , Applied Mathematics and Computation , vol. 174, pp. 150–164, (2006)
15. Climent, J.–J.; Herranz, V.; Perea, C. "Positive cones and convergence conditions for iterative methods based on splittings" , Linear Algebra and Its Applications , vol. 413, pp. 319–326, (2006)
16. Climent, J.J.; Requena, V. "Àlgebra Lineal Bàsica" , Quaderns de la Col·lecció Joan Fuster. Secretariat de Promoció del Valencià. Universitat d'Alacant , vol. 83, pp. 1–282, (2006)
17. José–Vicente Aguirre, Rafael Álvarez, José Noguera, Antonio Zamora "A Database Backup System with Secure Remote Data Transmission" , TRANSACTIONS on INFORMATION SCIENCE APPLICATIONS , vol. 4, pp. 796–801, (2006)
18. JOSE–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, JULIA SÁNCHEZ, ANTONIO ZAMORA "Silence Detection in Secure P2P VoIP Multiconferencing" , Information Security and Privacy 2006 Proceedings , pp. 11–14, (2006)
19. JOSÉ–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, LEANDRO TORTOSA, ANTONIO ZAMORA "Lightweight Peer–to–Peer Secure Multi–Party VoIP Protocol" , Information Security and Privacy 2006 Proceedings , pp. 7–10, (2006)
20. JOSÉ–VICENTE AGUIRRE, RAFAEL ÁLVAREZ2, JOSÉ NOGUERA and ANTONIO ZAMORA "A Secure Remote Database Backup System" , Recent advances in computer engineering , vol. 1, pp. 43–46, (2006)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Nacionales

1. ARNAL, J.; BERNABEU, R.; GOMIS, J.; MIGALLÓN, V.; PENADÉS, J.; RAMON, S. "Análisis de la asignatura Matemática Discreta de las Ingenierías Informáticas en vistas a su adaptación al Espacio Europeo de Educación Superior", JORNADAS DE ENSEÑANZA UNIVERSITARIA DE LA INFORMÁTICA (JENUI), Bilbao, Julio 2006.

Internacionales

1. ALVAREZ, R.; NOGUERA, J.; TORTOSA, L.; ZAMORA, A. "GNG3D – A Software Tool for Mesh Optimization Based on Neural Networks", 2006 IEEE WORLD CONGRESS ON COMPUTATIONAL INTELLIGENCE, Vancouver, BC, Julio 2006.
2. ARNAL, J.; BERNABEU, R.; GOMIS J.; MIGALLÓN, V.; PENADÉS, J.; RAMON, S.; REQUENA, V,; REVERTE, J. "Metodologías docentes ECTS para matemática discreta en las titulaciones de informática", IV CONGRESO INTERNACIONAL DE DOCENCIA UNIVERSITARIA E INNOVACIÓN, Barcelona, Julio 2006.
3. CLIMENT, J.; HERRANZ, V.; PEREA, C. "Some applications of the inclusion principle to convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Kyoto, Julio 2006.
4. CLIMENT, J. J.; GARCÍA CRESPÍ, F.; GREDIAGA, A. "A ghost bit based finite field arithmetic for FPGAs", INTERNATIONAL E–CONFERENCE ON COMPUTER SCIENCE, , Julio 2006.
5. CLIMENT, J.J.; GARCÍA CRESPÍ, F; GREDIAGA, A. "A scalable finite field multiplier with interleaving reduction", INTERNATIONAL E–CONFERENCE ON COMPUTER SCIENCE, , Julio 2006.

6. CLIMENT, J.J.; GARCÍA, F.J.; REQUENA, V. "A new iterative method to construct bent funcions", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Venecia, Noviembre 2006.
7. CLIMENT, J.J.; GARCÍA, F.J.; REQUENA, V. "On the iterative construction of bent functions", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Venecia, Noviembre 2006.
8. CLIMENT, J.–J.; GORLA, E.; ROSENTHAL, J. "Cryptanalysis of the CFVZ cryptosystem", RHINE WORKSHOP ON COMPUTER ALGEBRA, Basel, Marzo 2006.
9. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "A composite linear time invariant linear system and its applications to convolutional codes", INTERNATIONAL CONFERENCE ON ENGINEERING COMPUTATIONAL TECHNOLOGY, Las Palmas de Gran Canaria, Septiembre 2006.
10. CLIMENT, J.J.; HERRANZ, V.; PEREA, C. "Linear system modelization of digital mobile system GSM", CONFERENCE OF THE INTERNATIONAL LINEAR ALGEBRA SOCIETY, Amsterdam, Julio 2006.
11. CLIMENT, J.J.; HERRANZ, V.; PEREA, C. "Linear system modelization of GSM digital mobile system", WORKSHOP ON CODING AND SYSTEMS, Zürich, Diciembre 2006.
12. JOSÉ VICENTE AGUIRRE, RAFAEL ÁLVAREZ, JOSÉ NOGUERA AND ANTONIO ZAMORA. "A Secure Remote Database Backup System", 5TH INT. CONF. ON ARTIFICIAL INTELLIGENCE, KNOWLEDGE ENGINEERING AND DATA BASES, Madrid, Febrero 2006.
13. JOSE–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, JULIA SÁNCHEZ, ANTONIO ZAMORA. "Silence Detection in Secure P2P VoIP Multiconferencing", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Venecia, Noviembre 2006.
14. JOSÉ–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, LEANDRO TORTOSA, ANTONIO ZAMORA. "Lightweight Peer–to–Peer Secure Multi–Party VoIP Protocol", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Venecia, Noviembre 2006.