GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2007

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. TOMAS ESTEVAN, VIRTUDES
12. TORTOSA GRAU, LEANDRO
13. VICENT FRANCES, JOSE FRANCISCO
14. 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. "CONSOLIDER MATHEMATICA: Escuela Internacional sobre "Stability and well–posedness in convex optimization"", csd2006–00032 , 6 meses, 6.000,00 €, LOPEZ CERDA, MARCO ANTONIO.
2. "Construcción de códigos convolucionales. Algoritmos secuenciales y paralelos de decodificación", mtm2005–05759 , 36 meses, 41.650,00 €, CLIMENT COLOMA, JOAN JOSEP.
3. "Construcción iterativa de funciones bent. Aplicaciones criptográficas.", pr2007–0181 , 3 meses, 10.100,00 €, CLIMENT COLOMA, JOAN JOSEP.
4. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.773,00 €, ZAMORA GOMEZ, ANTONIO.

5. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 3.084,14 €, ZAMORA GOMEZ, ANTONIO.
6. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.795,56 €, ZAMORA GOMEZ, ANTONIO.
7. "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. Aguirre, J.V.; Álvarez, R.; Tortosa, L.; Zamora, A. "Generador pseudoaleatorio matricial optimizado sobre Z2" en "Actas del II Simposio sobre Seguridad Informática" , ISBN: 978–84–9732–607–0, Madrid, Thomson, pp. 27–34, (2007)
2. Aguirre, J.V.; Álvarez, R.; Zamora, A. "Protocolo de multivideoconferencia P2P para dispositivos móviles" en "Actas del segundo Simposio sobre Computación Ubicua e Inteligencia Artificial" , ISBN: 978–84–9732–605–6, Madrid, Thomson, pp. 287–292, (2007)
3. Arnal, J.; Bernabeu, R.; Gomis, J.; Migallon, V.; Penadés, J.; Ramón, S.; Requena, V.; Reverte, J.R. "Implementación de metodologías docentes para la asignatura Matemática Discreta en las titulaciones de informática conforme con el sistema ECTS" en "Implementación de las metodologías ECTS en Primer Curso de las Titulaciones de Informática" , ISBN: 978–84–690–3772–0 , Alicante, Universidad de Alicante, pp. 1–104, (2007)
4. Climent, J.J.; Ferrández, F.; Tomás, V. "Construction of a Convolutional Code Based Symmetric Cryptosystem" en "Proceedings of the 6th International Conference on Information Security and Privacy" , ISBN: 978–960–6766–23–7, Grecia, WSEAS Press, pp. 48–51, (2007)
5. Climent, J.–J.; García, F.J.; Requena, V. "Construcción de funciones bent de n+2 variables a partir de las funciones duales de funciones bent de n variables" en "Anales del IV Congreso Iberoamericano de Seguridad Informática" , ISBN: 978–950–623–043–2, Salta (Argentina), Universidad Católica de Salta, pp. 3–17, (2007)
6. Climent, J.J; García, F.J.; Requena, V. "A Characterization of Bent Functions of n+1 Variables" en "Proceedings of the 6th International Conference on Information Security and Privacy" , ISBN: 978–960–6766–23–7, Grecia, WSEAS Press, pp. 44–47, (2007)
7. Climent, J.J; García, F.J.; Requena, V. " Some constructions of bent functions of n+2 variables from bent functions of n variables" en "Proceedings of the 3rd International Conference on Boolean Functions: Cryptography and Applications" , ISBN: pendent, París (Francia), Université Denis Diderot, París 7, pp. 57–72, (2007)
8. Garcia, F.J; Requena, V.; Tomas, V. "Generating Pseudo–random Sequences from Cellular Automata and Bent Functions" en "Proceedings of the 6th International Conference on Information Security and Privacy" , ISBN: 978–960–6766–23–7, Grecia, WSEAS Press, pp. 40–43, (2007)
9. José Vicente Aguirre, Rafael Álvarez, Antonio Zamora "Protocolo de videoconferencia multiusuario, seguro y distribuido" en "Novas Perspectivas em Sistemas e Tecnologias de Informaçao" , ISBN: 978–972–8830–88–5, , Universidade Fernando Pessoa, pp. 417–428, (2007)
10. M. Saiz Noeda et.al. "Diseño Docente EEES en el 2º Curso de Informática" en "LA MULTIDIMENSIONALIDAD DE LA EDUCACIÓN UNIVERSITARIA. Redes de Investigación Docente–Espacio Europeo de Educación Superior. Vol. I" , ISBN: 84–268–1335–6, Alicante, Editorial Marfil, pp. 343–378, (2007)
11. Migallón, V.; Penadés, J.; Álvarez, R. "Guía docente de Ampliación de Estadística" en "Investigación en diseño docente de los estudios de segundo curso de informática" , ISBN: 978–84–268–1146–2, Alicante, Marfil, pp. 59–88, (2007)

Artículos en publicaciones periódicas:

12. Aguirre, J.V.; Alvarez, R.; Tortosa, L.; Zamora, A. "Fast Pseudorandom Generator based on Packed Matrices" , Advanced Topics in Information Security and Privacy , vol. 1, pp. 98–101, (2007)
13. Aguirre J.V.; Álvarez R.; Zamora A. "Videoconferencia P2P Segura para Dispositivos Móviles" , Eatis'07 ACM–DL Proceedings , pp. –, (2007)
14. Alvarez, R.; Martinez, F.M.; Vicent, J.F.; Zamora, A. "A New Public Key Cryptosystem based on Matrices" , Advanced Topics in Information Security and Privacy , vol. 1, pp. 36–39, (2007)
15. Alvarez, R.; Noguera, J.V.; Tortosa, L.; Zamora, A. "A mesh Optimization Algorithm Based on Neural Networks." , Information Sciences , vol. 177, pp. 5347–5364, (2007)
16. Alvarez, R.; Noguera, J.V.; Tortosa, L.; Zamora, A. "Computational Cost of GNG3D Algorithm for Mesh simplification" , PROCEEDINGS OF THE IADIS INTERNATIONAL CONFERENCE APPLIED COMPUTING 2007 , pp. 75–82, (2007)
17. Climent, J.–J.; Crespí, F.G.; Grediaga, A. "A scalable finite field multiplier with interleaving reduction" , Lecture Series on Computer and Computational Sciences , vol. 8, pp. 50–53, (2007)
18. Climent, J.–J.; Crespí, F.G.; Grediaga, A. "A ghost bit based finite field arithmetic for FPGAs" , Lecture Series on Computer and Computational Sciences , vol. 8, pp. 44–49, (2007)
19. Climent, J.–J.; Ferrández, F.; Tomás, V. "Construction of a convolutional code based symmetric cryptosystem" , Advanced Topics in Information Security and Privacy , vol. 1, pp. 48–51, (2007)
20. Climent, J.–J.; García, F.J.; Requena, V. "An iterative method to construct new bent functions from old bent functions" , TRANSACTIONS on INFORMATION SCIENCE APPLICATIONS , vol. 4, pp. 245–250, (2007)
21. Climent, J.–J.; García, F.J.; Requena, V. "A characterization of bent functions of n+1 variables" , Advanced Topics in Information Security and Privacy , vol. 1, pp. 44–47, (2007)
22. Climent, J.–J.; García, F.J.; Requena, V. "Iterative methods to construct Boolean bent functions" , TRANSACTIONS on INFORMATION SCIENCE APPLICATIONS , vol. 4, pp. 251–256, (2007)
23. Climent, J.–J.; Gorla, E.; Rosenthal, J. "Cryptanalysis of the CFVZ Cryptosystem" , Advances in Mathematics of Communications , vol. 1, pp. 1–11, (2007)
24. Climent, J.–J.; Herranz, V.; Perea, C. "A first approximation of concatenated convolutional codes from linear systems theory viewpoint" , Linear Algebra and Its Applications , vol. 425, pp. 673–699, (2007)
25. JOSÉ VICENTE AGUIRRE, RAFAEL ÁLVAREZ, LEANDRO TORTOSA, ANTONIO ZAMORA "Secure Lightweight P2P Multiconferencing" , TRANSACTIONS ON COMUNICATIONS , vol. 6, pp. 195–200, (2007)
26. JOSE–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, JULIA SÁNCHEZ, ANTONIO ZAMORA "Broadcast Multiplexing and Subchanneling for Secure P2P Multiconferencing" , WSEAS Transactions on Computers , vol. 6, pp. 522–527, (2007)
27. Noguera, J.V.; Tortosa, L. "Hidding Information Inside Exercises" , INTED 2007 Proceedings , pp. 80–87, (2007)
28. Vicent, J "Propuesta y Análisis de Criptosistemas de Clave Pública Basados en Matrices Triangulares por Bloques" , , pp. –, (2007)

TESIS DOCTORALES DEFENDIDAS

1. MARÍA VICTORIA HERRANZ CUADRADO, "Estudio y construcción de códigos convolucionales: códigos perforados, códigos concatenados desde el punto de vista de sistemas", Director: CLIMENT COLOMA, JOAN JOSEP Febrero 2007.
2. VICENT FRANCÉS, JOSE FRANCISCO, "PROPUESTA Y ANÁLISIS DE CRIPTOSISTEMAS DE CLAVE PÚBLICA BASADOS EN MATRICES TRIANGULARES SUPERIORES POR BLOQUES", Directores: ZAMORA GOMEZ, ANTONIO / TORTOSA GRAU, LEANDRO Junio 2007.

COMUNICACIONES A CONGRESOS

Nacionales

1. AGUIRRE, J.V.; ÁLVAREZ, R.; TORTOSA, L.; ZAMORA, A. "Generador pseudoaleatorio matricial optimizado sobre Z2 ", SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA, Zaragoza, Septiembre 2007.
2. ÁLVAREZ, R; MIGALLÓN, V.; PENADÉS, J. "Ampliación de Estadística en las titulaciones de Informática: adaptación al sistema ECTS", JORNADAS DE REDES DE INVESTIGACIÓN EN DOCENCIA UNIVERSITARIA, Alicante, Junio 2007.

Internacionales

1. AGUIRRE, J.V.; ALVAREZ, R.; TORTOSA, L.; ZAMORA, A. "Fast Pseudorandom Generator based on Packed Matrices", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Puerto de la Cruz, Tenerife, Diciembre 2007.
2. AGUIRRE, J.V.; ÁLVAREZ, R., ZAMORA, A. "Protocolo de Multivideoconferencia P2P para dispositivos móviles", SIMPOSIO INTERNACIONAL SOBRE COMPUTACIÓN UBICUA E INTELIGENCIA ARTIFICIAL, Zaragoza, Septiembre 2007.
3. AGUIRRE, J.V.; ÁLVAREZ, R.; ZAMORA A. "Videoconferencia P2P Segura para Dispositivos Móviles", EURO AMERICAN CONFERENCE ON TELEMATICS AND INFORMATION SYSTEMS 2007, Faro, Mayo 2007.
4. ALVAREZ, R.; MARTINEZ, F.M.; VICENT, J.F.; ZAMORA, A. "A New Public Key Cryptosystem based on Matrices", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Puerto de la Cruz, Tenerife, Diciembre 2007.
5. ALVAREZ, R.; NOGUERA, J.V.; TORTOSA, L.; ZAMORA, A. "Computational Cost of GNG3D Algorithm for Mesh simplification", INTERNATIONAL CONFERENCE ON APPLIED COMPUTING 2007, SALAMANCA, Febrero 2007.
6. CLIMENT, J.J.; GARCÍA, F.J.; REQUENA, V. "Some constructions of bent functions of n+2 variables from bent functions of n variables", INTERNATIONAL CONFERENCE ON BOOLEAN FUNCTIONS: CRYPTOGRAPHY AND APPLICATIONS, París, Mayo 2007.
7. CLIMENT, J.J; GARCÍA, F.J.; REQUENA, V. "A Characterization of Bent Functions of n+1 variables ", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Puerto de la Cruz, Tenerife, Diciembre 2007.
8. CLIMENT, JOAN–JOSEP; FERRÁNDEZ, FRANCISCO; TOMÁS, VIRTUDES. "Construction of a convolutional code based symmetric cryptosystem", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Puerto de la Cruz, Tenerife, Diciembre 2007.
9. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO J.; REQUENA, VERÓNICA. "Construcción de funciones bent de n+2 variables a partir de las funciones duales de bunciones bent de n variables", CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA, Mar del Plata, Noviembre 2007.
10. GARCIA, F.J; REQUENA, V.; TOMAS, V. "Generating Pseudo–random Sequences from Cellullar Automata and Bent Functions", INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND PRIVACY, Puerto de la Cruz, Tenerife, Diciembre 2007.
11. JOSÉ VICENTE AGUIRRE, RAFAEL ÁLVAREZ, ANTONIO ZAMORA. "Protocolo de videoconferencia multiusuario, seguro y distribuido", CONFERENCIA CONFERÊNCIA IBÉRICA DE SISTEMAS E TECNOLOGIAS DE INFORMAÇAO, Porto, Junio 2007.
12. NOGUERA, J.V.; TORTOSA, L. "Hidding Information Inside Exercises", INTED 2007 INTERNATIONAL TECHNOLOGY, EDUCATION AND DEVELOPMENT CONFERENCE., VALENCIA, Marzo 2007.