GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2009

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. "Análisi de possibles col.laboracions entre el nostre grup d'investigació i el grup d'Algebra Aplicada de la Universidad de Zurich. Impartició d'una conferència", inv09–41 , 1.500,00 €, CLIMENT COLOMA, JOAN JOSEP.
2. "Análisi de possibles col.laboracions entre el nostre grup d'investigació i L'Institut Claude Shannon, University College Dublin. IMpartició d'una conferència", inv09–40 , 1.500,00 €, CLIMENT COLOMA, JOAN JOSEP.

3. "Computación de altas prestaciones y paralelismo", ati07–06 , 36 meses, 22.000,00 €, PENADES MARTINEZ, JOSE LEANDRO.
4. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas", acomp/2009/142 , 12 meses, 6.000,00 €, CLIMENT COLOMA, JOAN JOSEP.
5. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas.", mtm2008–06674–c02–01 , 36 meses, 34.727,00 €, CLIMENT COLOMA, JOAN JOSEP.
6. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.773,00 €, ZAMORA GOMEZ, ANTONIO.
7. "Criptología y seguridad computacional", vigrob–025 , 12 meses, 3.271,00 €, ZAMORA GOMEZ, ANTONIO.
8. "El viaje de las sondas Voyager", fct–09–762 , 7 meses, 6.000,00 €, TORTOSA GRAU, LEANDRO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Libros:

1. Tortosa Grau, L.; Vicent Francés, J.F. "Geometría para Arquitectura" , ISBN: 978–84–95434–59–3, Alicante, Ramón Torres Gosálvez, (2009)

Capítulos en libros:

2. Climent, J.–J.; Díaz, S. "Otra construcción de códigos array cíclicos, MDS y LDPC" en "Actas del XXI Congreso de Ecuaciones Diferenciales y Aplicaciones / XI Congreso de Matemática Aplicada" , ISBN: 978–84–692–6473–7, Ciudad Real, Ediciones de la Universidad de Castilla–La Mancha, pp. 1–8, (2009)
3. Climent, J.–J.; García, F.J.; Requena, V. "Sobre el número de funciones bent obtenidas a partir de funciones de máximo peso" en "Actas del V Congreso Iberoamericano de Seguridad Informática" , ISBN: 978–9974–0–0593–8, Montevideo (Uruguay), Editorial del Congreso (versión electrónica), pp. 133–147, (2009)
4. Climent, J.–J.; García, F.J.; Requena, V. "Construcción de funciones bent a partir de una función bent y de sus traslaciones cíclicas basadas en bases de Gauss–Jordan de cardinalidad 2" en "Actas del XXI Congreso de Ecuaciones Diferenciales y Aplicaciones / XI Congreso de Matemática Aplicada" , ISBN: 978–84–692–6473–7, Ciudad Real, Ediciones de la Universidad de Castilla–La Mancha, pp. 1–8, (2009)
5. Climent, J.–J.; García, F.J.; Requena, V. "Sobre algunas construcciones de funciones bent" en "Nuevos Avances en Criptografía y Codificación de la Información" , ISBN: 978–84–8409–277–3, Lleida, Publicaciones de la Universitat de Lleida, pp. 43–52, (2009)
6. Climent, J.–J.; Herranz, V.; Perea, C.; Tomás, V. "Un criptosistema de clave pública basado en códigos convolucionales" en "Actas del XXI Congreso de Ecuaciones Diferenciales y Aplicaciones / XI Congreso de Matemática Aplicada" , ISBN: 978–84–692–6473–7, Ciudad Real, Ediciones de la Universidad de Castilla–La Mancha, pp. 1–8, (2009)

Artículos en publicaciones periódicas:

7. Álvarez, R.; Castel, M. J.; Tortosa, L.; Zamora, A. "Optimizing matrix operations in Z2 by word packing" , Applied Mathematics Letters , vol. 22, pp. 242–244, (2009)
8. Álvarez, R.; Tortosa, L.; Vicent, J. F.; Zamora, A. "Analysis and Design of a Secure Key Exchange Scheme" , Information Sciences , vol. 179, pp. 2014–2021, (2009)
9. Alvarez, R.; Tortosa, L.; Vicent, J.; Zamora, A. "A Non–Abelian Group Based on Block Upper Triangular Matrices with Cryptographic Applications" , Lecture Notes in Computer Science , vol. 5527, pp. 117–126, (2009)

10. Climent, J.–J.; Herranz, V.; Perea, C.; Tomás, V. "A systems theory approach to periodically time–varying convolutional codes by means of their invariant equivalent" , Lecture Notes in Computer Science , vol. 5527, pp. 73–82, (2009)
11. Tortosa, L.; Oliver, J.L.; Vicent, J.F.; Zamora, A. "Reducing urban concentration using a Neural Network Model" , Communications in Computer and Information Science , vol. 43, pp. 143–152, (2009)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Nacionales

1. ÁLVAREZ, R.; CLIMENT, J.; DÍAZ S.; HERRANZ, V.; PEREA, C.; REQUENA V., TOMÁS V.; TORTOSA, L.; VICENT, J.; ZAMORA, A. "II Jornadas MatSI en Alicante", JORNADAS DE MATEMÁTICAS EN LA SEGURIDAD DE LA INFORMACIÓN, Alicante, Noviembre 2009.
2. ÁLVAREZ, R.; VICENT, J. "Criptología y Seguridad Computacional", JORNADAS DE MATEMÁTICAS EN LA SEGURIDAD DE LA INFORMACIÓN, Alicante, Noviembre 2009.
3. CLIMENT, J.–J.; DÍAZ, S. "Otra construcción de códigos array cíclicos, MDS y LDPC", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Ciudad Real, Septiembre 2009.
4. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Sobre algunas construcciones de funciones bent", CONGRESO DE LA REAL SOCIEDAD MATEMÁTICA ESPAÑOLA, Oviedo, Febrero 2009.
5. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Construcción de funciones bent a partir de una función bent y de sus traslaciones cíclicas basadas en bases de Gauss–Jordan de cardinalidad 2", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Ciudad Real, Septiembre 2009.
6. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "Un criptosistema de clave pública basado en códigos convolucionales", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Ciudad Real, Septiembre 2009.

Internacionales

1. ALVAREZ, R.; TORTOSA, L.; VICENT, J.; ZAMORA, A. "A Non–abelian Group Based on Block Upper triangular Matrices with Cryptographic Applications", INTERNATIONAL SYMPOSIUM APPLIED ALGEBRA ALGEBRAIC ALGORITHMS, AND ERROR–CORRECTING CODES, Tarragona, Junio 2009.
2. ALVAREZ, R.; TORTOSA, L.; VICENT, J.F.; ZAMORA, A. " Comparing gng3d and quadric error metrics methods to simplify 3d meshes. ", INTERNATIONAL JOINT CONFERENCE ON COMPUTER VISION, IMAGING AND COMPUTER GRAPHICS THEORY AND APPLICATIONS, Lisboa, Febrero 2009.
3. CLIMENT J.–J. ; DÍAZ S. "Another construction of cyclic low–density MDS array codes", 5TH WORKSHOP ON CODING AND SYSTEMS, Dublín, Septiembre 2009.
4. CLIMENT, J–J.; GARCÍA, F.J.; REQUENA, V. "On the construction of bent functions of 2k variables from a primitive polynomial of degree k", 5TH WORKSHOP ON CODING AND SYSTEMS, Dublín, Septiembre 2009.
5. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Sobre el número de funciones bent obtenidas a partir de funciones de máximo peso", CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA, Montevideo, Noviembre 2009.
6. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "A systems theory approach to periodically time–varying convolutional codes by means of their invariant equivalent", INTERNATIONAL SYMPOSIUM APPLIED ALGEBRA ALGEBRAIC ALGORITHMS, AND ERROR–CORRECTING CODES, Tarragona, Junio 2009.

7. TOMÁS, V.; ROSENTHAL, J.; SMARANDACHE, R. "Decoding of MDP Convolutional Codes over the Erasure Channel", IEEE INTERNATION SYMPOSIUM ON INFORMATION THEORY, Seoul, Junio 2009.
8. TOMÁS, V.; ROSENTHAL, J.; SMARANDACHE, R. "On convolutional codes over the erasure channel", WORKSHOP ON CODING AND SYSTEMS, Dublín, Septiembre 2009.
9. TORTOSA, L.; OLIVER, J.L.; VICENT, J.F.; ZAMORA, A. "Reducing urban concentration using a neural network model", ENGINEERING APPLICATIONS OF NEURAL NETWORKS, Londres, Agosto 2009.