GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2008

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. "Aplicación de funciones no lineales y optimización de criptosistemas matriciales", jc2007–00022 , 5 meses, 11.775,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.
2. "Computación de altas prestaciones y paralelismo", ati07–06 , 36 meses, 22.000,00 €, PENADES MARTINEZ, JOSE LEANDRO.
3. "Construcción de códigos convolucionales. Algoritmos secuenciales y paralelos de decodificación", mtm2005–05759 , 36 meses, 41.650,00 €, CLIMENT COLOMA, JOAN JOSEP.

4. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.795,56 €, ZAMORA GOMEZ, ANTONIO.
5. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 2.773,00 €, ZAMORA GOMEZ, ANTONIO.
6. "Sistema de comunicaciones seguras para la gestión de rutas y pedidos a través de plataformas móviles.", gvpre/2008/363 , 12 meses, 20.600,00 €, TORTOSA GRAU, LEANDRO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Libros:

1. Al–Bahadly, I.; Chen, Q.L.; Climent, J.–J.; Costa, S.; Eboueya, M.; Igreja, J. M.; Montanaro, A.; Pasternak, N.E.; Patrick, J.; Domínguez, J.A.; Requena, V.; Senivongse, T.; Shimomura, T.; Tomá, V. "Easy, Enjoyable, Effective E–Learning" , ISBN: 1–60456–634–5, Nueva York, Nova Publishers, (2008)
2. Martínez Pérez, F.M.;Benavente Victoria, A.;Iborra Baeza, I.;Morales Benavente, J.L.; Vicent Francés, J.F. "PROCESAMIENTO DE TEXTOS CON OO–WRITER" , ISBN: 978–84–8454–742–6, San Vicente del Raspeig, Alicante, Editorial Club Universitario, (2008)
3. Tortosa Grau, L.; Vicent Francés, J.F. "INTRODUCCIÓN A LA GEOMETRÍA ANALÍTICA" , ISBN: 9788495434500, San Vicente del Raspeig, Alicante, Puntero y Chip, S.L., (2008)
4. Tortosa Grau, L.; Vicent Francés, J.F. "GRÁFICOS CON MATLAB PARA ARQUITECTURA" , ISBN: 978–84–95434–47–0, San Vicente del Raspeig, Alicante, Puntero y Chip, S.L., (2008)

Capítulos en libros:

5. Climent, J.–J.; García, F.J.; Requena, V. "New bent functions from positive and negative functions of old bent functions" en "Proceedings of the 2008 International Symposium on Information Theory and its Applications (ISITA2008)" , ISBN: 978–1–4244–2069–8, Auckland, Nueva Zelanda, IEEE Press, pp. 1344–1349, (2008)
6. Climent, J.–J.; García, F.J.; Requena, V. "Caracterización y construcción de funciones bent de n+1 variables a partir de funciones booleanas de n variables" en "Actas X Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–691–5158–7, Salamanca, Editorial del Congreso, pp. 133–140, (2008)
7. Climent, J.–J.; García, F.J.; Requena, V. "On the characterization and construction of bent functions of n+1 variables from Boolean functions of n variables" en "Extended Abstracts of the Second Workshop on Mathematical Cryptology" , ISBN: isbn2, Santander, Universidad de Cantabria, pp. 11–14, (2008)
8. Climent, J.–J.; Herranz, V.; Perea, C.; Tomás, V. "Criptosistema basado en el esquema de McEliece generado con códigos convolucionales" en "Actas X Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–691–5158–7, Salamanca, Editorial del Congreso, pp. 151–156, (2008)
9. Climent, Joan–Josep; Herranz, Victoria; Perea, Carmen; Tomás, Virtudes. "A construction of periodically time–varying convolutional codes" en "Electronic Proceedings of the 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2008)" , ISBN: isbn1, Blacksburg, Virginia, USA, Editorial del Congreso (versión electrónica), pp. 4–1–4–12, (2008)
10. Climent, Joan–Josep; Herranz, Victoria; Perea, Carmen; Tomás, Virtudes. "A McEliece–like cryptosystem based on convolutional code" en "Electronic Proceedings of the 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2008)" , ISBN: isbn1, Blacksburg, Virginia, USA, Editorial del Congreso (versión electrónica), pp. 5–1–5–12, (2008)

Editores de revistas

11. "Advances in Mathematics of Communications" , 01/11/2008 , (2008)

Artículos en publicaciones periódicas:

12. Aguirre, J.V.; Álvarez, R.; Tortosa, L; Vicent, J. "P2P Audio/Video Protocol With Global Positioning Data in Real Time for Mobile Devices" , International Journal of Applied Mathematics and Informatics , vol. 2, pp. 37–46, (2008)
13. Aguirre, J.V.; Álvarez, R.; Tortosa, L.; Zamora, A. "An Optimized Pseudorandom Generator using Packed Matrices." , TRANSACTIONS on INFORMATION SCIENCE APPLICATIONS , vol. 5, pp. 487–496, (2008)
14. Álvarez, R.; McGuire, G.; Zamora, A. "The Tangle Hash Function" , NIST SHA–3 Hash Competition , pp. –, (2008)
15. Alvarez, R.; Tortosa, L.; Vicent, J–F.; Zamora, A. "Error measurements and parameters choice in the GNG3D model for mesh simplification." , TRANSACTIONS on INFORMATION SCIENCE APPLICATIONS , vol. 5, pp. 579–588, (2008)
16. Climent, J.–J.; Crespí, F. G.; Grediaga, A. "A scalable finite field multiplier" , IEEE América Latina , vol. 6, pp. 632–637, (2008)
17. Climent, J.–J.; Crespí, F. G.; Grediaga, A. "A scalable finite field multiplier with interleaving reduction" , Computing Letters , vol. 4, pp. 45–51, (2008)
18. Climent, J.–J.; Crespí, F. G.; Grediaga, A. "A ghost bit based finite field arithmetic for FPGAs" , Computing Letters , vol. 4, pp. 36–44, (2008)
19. Climent, J.–J.; García, F.J.; Requena, V. "On the construction of bent functions of n+2 variables from bent functions of n variables" , Advances in Mathematics of Communications , vol. 2, pp. 421–431, (2008)
20. Climent, J.–J.; Herranz, V.; Perea, C. "Linear system modelization of concatenated block and convolutional codes" , Linear Algebra and Its Applications , vol. 429, pp. 1191–1212, (2008)
21. Gallardo, C.; Tortosa, L.; Vicent, J.; Zamora, A. "A Secret Sharing Scheme Based on Exponentiation in Galois Fields" , International Journal of Applied Mathematics and Informatics , vol. 2, pp. 57–66, (2008)
22. Gallardo, C.; Tortosa, L.; Vicent, J.F.; Zamora, A "SECRET SHARING SCHEME BASED ON MATRICES
(Computers and Simulation in Modern Science)" , Advanced Topics in Information Security and Privacy , vol. 2, pp. 124–129, (2008)
23. Navarro, P.; Tortosa, L.; Vicent, J.F.; Zamora, A.

"Evaluating Approximations generated by the GNG3D method for mesh simplification." , Recent advances in computer engineering , pp. 25–30, (2008)

24. Noguera, J.V.; Tortosa, L.; Zamora, A. "Analysis and efficiency of the GNG3D algorithm for mesh simplification." , Applied Mathematics and Computation , vol. 197, pp. 29–40, (2008)

25. Vicent, J; Zamora, A.; Alvarez, R; Martinez, F.M. "A matricial Public Key Cryptosystem with Digital Signature" , WSEAS Transactions on Mathematics , vol. 7, pp. 195–204, (2008)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Nacionales

1. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Caracterización y construcción de funciones bent de n+1 variables a partir de funciones booleanas de n variables", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Salamanca, Septiembre 2008.
2. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "Criptosistema basado en el esquema de McEliece generado con códigos convolucionales", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Salamanca, Septiembre 2008.
3. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; VIRTUDES, T. "Construcción de códigos convolucionales periódicos desde el punto de vista de sistemas lineales", ALGEBRA LINEAL, ANÁLISIS MATRICIAL Y APLICACIONES, Vitoria–Gasteiz, Septiembre 2008.

Internacionales

1. AGUIRRE, J.V.; ÁLVAREZ, R.; TORTOSA, L.; VICENT, J.F. "Incorporating Global Positioning Data in Real Time P2P Audio/Video Streams for Mobile Devices", INTERNATIONAL CONFERENCE ON APPLIED COMPUTER SCIENCE, Venecia, Noviembre 2008.
2. ÁLVAREZ, R. "Optimizing Stream Ciphers based on Block Upper–Triangular Matrices", THE CLAUDE SHANNON INSTITUTE WORKSHOP ON CODING & CRYPTOGRAPHY, Cork, Mayo 2008.
3. ÁLVAREZ, R.; MCGUIRE, G. "S–Boxes, APN Functions and Related Codes", ADVANCED RESEARCH WORKSHOP ON ENHANCING CRYPTOGRAPHIC PRIMITIVES WITH TECHNIQUES FROM ERROR CORRECTING CODES, Veliko Tarnovo, Octubre 2008.
4. ÁLVAREZ, R.; ZAMORA, A.; AGUIRRE, J. V. "Teaching and Evaluation of Computer Science for Mathematics", INTED 2007 INTERNATIONAL TECHNOLOGY, EDUCATION AND DEVELOPMENT CONFERENCE., Valencia, Marzo 2008.
5. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "On the construction of bent functions based on the dual functions of old bent functions", WORKSHOP ON CODING AND SYSTEMS, Alicante /Elche, Marzo 2008.
6. CLIMENT, J.J; GARCÍA, F.J; REQUENA, V. "New Bent Functions from Positive and Negative Bent Functions from Old Bent Functions", 2008 INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY AND ITS APPLICATIONS (ISITA 2008), Auckland, Diciembre 2008.
7. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "Periodically time–varying convolutional codes and their time–invariant equivalent", WORKSHOP ON CODING AND SYSTEMS, Alicante /Elche, Marzo 2008.
8. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "A construction of periodically time–varying convolutional codes ", INTERNATIONAL WORKSHOP ON DYNAMICAL SYSTEMS AND MULTIDISCIPLINARY APPLICATIONS, Elche, Septiembre 2008.
9. CLIMENT, JOAN–JOSEP; GARCÍA, FRANCISCO J.; REQUENA, VERÓNICA. "On the characterization and construction of bent functions of n+1 variables from Boolean functions of n variables", WORKSHOP ON MATHEMATICAL CRYPTOLOGY, Santander, Octubre 2008.
10. CLIMENT, JOAN–JOSEP; HERRANZ, VICTORIA; PEREA, CARMEN; TOMÁS, VIRTUDES. "A construction of periodically time–varying convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Blacksburg, Virginia, Julio 2008.
11. CLIMENT, JOAN–JOSEP; HERRANZ, VICTORIA; PEREA, CARMEN; TOMÁS, VIRTUDES. "A McEliece–like cryptosystem based on convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Blacksburg, Virginia, Julio 2008.

12. GALLARDO, C.; TORTOSA, L.; VICENT, J.F.; ZAMORA, A. "Secret Sharing Scheme Based on Matrices", INTERNATIONAL CONFERENCE ON APPLIED COMPUTER SCIENCE, Venecia, Noviembre 2008.
13. NAVARRO, P.; TORTOSA, L.; VICENT, J.F.; ZAMORA, A. "Evaluating approximations generated by the GNG3D method for mesh simplification", 7TH INTERNATIONAL CONFERENCE ON ATIFICIAL INTELLIGENCE, KNOWLEDGE ENGINEERING AND DATA BASES, Cambridge, UK, Febrero 2008.