GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2010

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. "Computación de altas prestaciones y paralelismo", ati07–06 , 36 meses, 22.000,00 €, PENADES MARTINEZ, JOSE LEANDRO.
2. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas", acomp/2010/039 , 12 meses, 8.500,00 €, CLIMENT COLOMA, JOAN JOSEP.
3. "Construcción de funciones bent y códigos LDPC. Aplicaciones criptográficas.", mtm2008–06674–c02–01 , 36 meses, 34.727,00 €, CLIMENT COLOMA, JOAN JOSEP.

4. "Criptología y seguridad computacional", vigrob–025 , 12 meses, 3.304,00 €, ZAMORA GOMEZ, ANTONIO.
5. "Diseño de primitivas criptográficas basadas en matrices TSB (Cripto TSB)", gre09–02 , 24 meses, 3.500,00 €, ALVAREZ SANCHEZ, RAFAEL IGNACIO.
6. "Sistema multiprocesador en cluster", uainfra10–13 , 5 meses, 42.000,00 €, PENADES MARTINEZ, JOSE LEANDRO.

Privados

No hay proyectos para mostrar

PUBLICACIONES

Libros:

1. Benavent, A.; Iborra, I.; Martínez, F.M.; Morales, J.L.; Vicent, J. "Procesamiento de Textos con OO–Writer (2ª Edición)" , ISBN: 978–84–8454–954–3, San Vicente (Alicante), Editorial Club Universitario, (2010)
2. Benavente, A.; Bernabeu, J.; Carbonell, L.; Martínez, F.M.; Vicent, J. "Hojas de Cálculo con OO–Calc" , ISBN: 978–84–8454–970–3, San Vicente (Alicante), Editorial Club Universitario, (2010)

Capítulos en libros:

3. Cardell, S.D.; Maze, G.; Rosenthal, J. ; Wagner, U. "Correlations in stream ciphers, a systems theory point of view" en "Electronic Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS2010)" , ISBN: 978–963–311–370–7, Budapest, Editorial del Congreso (versión electrónica), pp. 419–423, (2010)
4. Climent, J.–J.; García, F.J.; Requena, V. "Computing the degree of a Boolean function from its support" en "Proceedings of the 2010 International Symposium on Information Theory and its Applications (ISITA2010)" , ISBN: 978–1–4244–6014–4, Taichung (Taiwan), IEEE Press, pp. 123–128, (2010)
5. Climent, J.–J.; García, F.J.; Requena, V. "Construcción de funciones bent de n variables a partir de una base de $\mathbb{F}_{2}^{n}$" en "Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–693–3304–4, Tarragona, Universitat Rovira i Virgili (Tarragona), pp. 13–18, (2010)
6. Climent, J.–J.; García, F.J.; Requena, V. "Some algebraic properties related to the degree of a Boolean function" en "Proceedings of the 2010 International Conference on Computational and Mathematical Methods in Science and Engineering." , ISBN: 978–84–613–5510–5, Almería, Editorial del Congreso, pp. 373–384, (2010)
7. Climent, J.–J.; García, F.J.; Requena, V. "Cálculo del grado de una función booleana a partir de su soporte" en "Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–693–3304–4, Tarragona, Universitat Rovira i Virgili (Tarragona), pp. 7–12, (2010)
8. Climent, J.–J.; Herranz, V.; Perea, C.; Tomás, V. "On the determination of an input–state–output realization of a secure McEliece–like cryptosystem based on convolutional codes" en "Electronic Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS2010)" , ISBN: 978–963–311–370–7, Budapest, Editorial del Congreso (versión electrónica), pp. 1–6, (2010)
9. Climent, Joan–Josep; Herranz, Maria Victoria; Perea, Carmen; Tomás, Virtudes "The Computation of an Input–State–Output Realization of a Convolutional Code in order to obtain a Secure McEliece–like Cryptosystem" en "Proceedings of the Seventh International Conference on Engineering Computational Technology" , ISBN: 978–1–905088–40–9, Valencia, Civil–Comp Press, pp. 1–11, (2010)
10. Gallardo. C; Vicent, JF, Zamora, A "Un esquema multiusuario de intercambio de clave." en "Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información" , ISBN: 978–84–693–3304–4, Tarragona, Universitat Rovira i Virgili (Tarragona), pp. 65–68, (2010)

Artículos en publicaciones periódicas:

11. Konstantinos Drakakis, Veronica Requena, Gary McGuire "On the Nonlinearity of Exponential Welch Costas Functions" , IEEE Transactions on Information Theory , vol. 56, pp. 1230–1238, (2010)
12. Tortosa, L. "Some geometric models of ancient astronomy with GeoGebra" , GeoGebra The New Language For The Third Millennium. , vol. 1, pp. 83–92, (2010)
13. Tortosa, L. "Simulating a Journey to Mars with GeoGebra" , Seria Informatica , vol. VIII, pp. 189–203, (2010)
14. Tortosa, L.; Vicent, J.F.; Oliver, J.L.; Zamora, A. "A Neural Network Model to Develop Urban Acupuncture." , Lecture Notes in Computer Science , vol. 6276, pp. 31–40, (2010)
15. Tortosa, L.; Vicent, J.F.; Zamora, A. "A model to simplify 2D triangle meshes with irregular shapes." , Applied Mathematics and Computation , vol. 216, pp. 2937–2946, (2010)

TESIS DOCTORALES DEFENDIDAS

1. REQUENA AREVALO, VERONICA, "SOBRE ALGUNAS CONSTRUCCIONES DE FUNCIONES BENT", Director: CLIMENT COLOMA, JOAN JOSEP Noviembre 2010.
2. TOMAS ESTEVAN, VIRTUDES, "COMPLETE–MDP CONVOLUTIONAL CODES OVER THE ERASURE CHANNEL", Director: CLIMENT COLOMA, JOAN JOSEP Julio 2010.

COMUNICACIONES A CONGRESOS

Nacionales

1. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Cálculo del grado de una función booleana a partir de su soporte", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Tarragona, Septiembre 2010.
2. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Construcción de funciones bent de n variables a partir de una base de $\mathbb{F}_{2}^{n}$", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Tarragona, Septiembre 2010.
3. CLIMENT, J.–J.; NAPP, D.; PEREA, C.; PINTO, R. "(n,1) two dimensional convolutional codes with designed free distance", ALGEBRA LINEAL, ANÁLISIS MATRICIAL Y APLICACIONES, Valencia, Junio 2010.
4. GALLARDO, C.;VICENT, J.F.; ZAMORA, A. "Un esquema multiusuario de intercambio de clave", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Tarragona, Septiembre 2010.

Internacionales

1. CARDELL, S. D.; MAZE, G.; ROSENTHAL, J. ; WAGNER, U. "Correlations in Stream Ciphers, A Systems Theory Point of View", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Budapest, Julio 2010.
2. CARDELL, S.D.; ROSENTHAL, J.; MAZE, G.; WAGNER, U. "An Algebraic Description of Correlation Attacks", INTERNATIONAL CONFERENCE COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Almería, Junio 2010.
3. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Some algebraic properties related to the degree of a Boolean function", INTERNATIONAL COFERENCE ON COMPUTATIONAL AND MATHEMATICAL METHODS IN SCIENCE AND ENGINEERING, Almería, Junio 2010.
4. CLIMENT, J.–J.; GARCÍA, F.J.; REQUENA, V. "Computing the degree of a Boolean function from its support", INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY AND ITS APPLICATIONS, Taichung, Octubre 2010.

5. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C.; TOMÁS, V. "On the determination of an input–state–output realization of a secure McEliece–like cryptosystem based on convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Budapest, Julio 2010.
6. CLIMENT, JOAN–JOSEP; HERRANZ, MARIA VICTORIA; PEREA, CARMEN; TOMÁS, VIRTUDES. "The computation of an input–state–output realization of a convolutional code in order to obtain a secure {McEliece}–like cryptosystem", INTERNATIONAL CONFERENCE ON ENGINEERING COMPUTATIONAL TECHNOLOGY, Valencia, Septiembre 2010.
7. LEANDRO TORTOSA. "Simulating a journey to Mars with GeoGebra", EUROPEAN CONFERENCE ON COMPUTER SCIENCE & APPLICATIONS, Timisoara, Septiembre 2010.
8. TORTOSA,L; VICENT, J.F.; OLIVER, J.L.; ZAMORA, A. " A neural network model to develop urban acupuncture. ", INTERNATIONAL CONFERENCE ON KNOWLEDGE–BASED AND INTELLIGENT INFORMATION AND ENGINEERING SYSTEMS, Cardiff, Septiembre 2010.