GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
CLIMENT COLOMA, JOAN JOSEP
ZAMORA GOMEZ, ANTONIO

AÑO DE LA MEMORIA: 2005

PERSONAL INVESTIGADOR

1. ALBEZA PIQUERAS, MIGUEL ANGEL
2. ALVAREZ SANCHEZ, RAFAEL IGNACIO
3. BELLIDO IBORRA, PEDRO
4. CLIMENT COLOMA, JOAN JOSEP
5. FERRANDEZ AGULLO, FRANCISCO
6. TORTOSA GRAU, LEANDRO
7. VICENT FRANCES, JOSE FRANCISCO
8. 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 , 15 meses, 2.334,91 €, CLIMENT COLOMA, JOAN JOSEP.
3. "Criptología y seguridad computacional", vigrob–025 , 24 meses, 3.084,14 €, ZAMORA GOMEZ, ANTONIO.
4. "Criptosistemas asimétricos basados en el problema del logaritmo discreto en semianillos finitos. (Estancia en la Universidad de Zurich (Suiza))", ctespp/2005/060 , 2 meses, 4.700,00 €, CLIMENT COLOMA, JOAN JOSEP.
5. "Sistema Estándar de Seguridad en las Comunicaciones (SESCO)", gv04b/462 , 24 meses, 9.995,96 €, ZAMORA GOMEZ, ANTONIO.

Privados

1. "PROMOCIÓ DE L¿US DEL VALENCIÀ", 46.600,00 €, JOAN JOSEP CLIMENT COLOMA.

PUBLICACIONES

Libros:

1. Carbonell, L.; Bellido, P.;Albeza, M. A. "HOJA DE CÁLCULO EXCEL 2003" , ISBN: 84–7908–848–6, Alicante, Publicaciones de la Universidad de Alicante, (2005)

Capítulos en libros:

2. Climent, J.J.; Herranz, V.; Perea, C. "Códigos convolucionales concatenados desde el punto de vista de sistemas" en "Actas del XIX Congreso de Ecuaciones Diferenciales y Aplicaciones / IX Congreso de Matemática Aplicada" , ISBN: 84–689–7726–8, Madrid, Editorial del Congreso, pp. 1–5, (2005)
3. Climent, J.J.; Herranz, V.; Perea, C. "Woven Convolutional Codes from Linear System Point of View" en "Actas del XIX Congreso de Ecuaciones Diferenciales y Aplicaciones / IX Congreso de Matemática Aplicada" , ISBN: 84–689–7726–8, Madrid, Editorial del Congreso, pp. 1–5, (2005)

Editores de revistas

4. "Advanced Topics in Information Security and Privacy" , 01/12/2005 , 31/12/2005 , (2005)

Artículos en publicaciones periódicas:

5. Álvarez, R. "Aplicaciones de las matrices por bloques a los criptosistemas de cifrado en flujo" , , pp. –, (2005)
6. Álvarez, R.; Climent, J.J.; Tortosa, L.; Zamora, A. "An efficient binary sequence generator with cryptographic applications" , Applied Mathematics and Computation , vol. 167, pp. 16–27, (2005)
7. Álvarez, R.; Tortosa, L.; Vicent, J.; Zamora, A. "Block Upper Triangular Matrices for Authentication and Integrity" , WSEAS Transactions on Mathematics , vol. 4, pp. 339–346, (2005)
8. Climent, J.J. "Àlgebra. Fonaments" , Quaderns de la Col·lecció Joan Fuster. Secretariat de Promoció del Valencià. Universitat d'Alacant , vol. 65, pp. 1–134, (2005)
9. Climent, J.J.; Perea, C; Tortosa, L.; Zamora, A. "An overlapped two–way method for solving tridiagonal linear systems in a BSP computer" , Applied Mathematics and Computation , vol. 161/2, pp. 475–500, (2005)
10. Jose–Vicente Aguirre, Rafael Álvarez, José Noguera, Leandro Tortosa, Antonio Zamora "A Viabilty Analysis of a Secure VoIP and Instant Messaging System On a Pocket PC Platform" , Advanced Topics in Information Security and Privacy , pp. 218–223, (2005)
11. Rafael Álvarez, Jesús–Alberto Oliver, Jose–Francisco Vicent, Antonio Zamora "Secure Communication System Over a GSM Network" , Advanced Topics in Information Security and Privacy , pp. 213–217, (2005)
12. Rafael Álvarez, Leandro Tortosa, Jose–Francisco Vicent, Antonio Zamora "A Public Key Cryptosystem Based on Block Upper Triangular Matrices" , Advanced Topics in Information Security and Privacy , pp. 163–168, (2005)
13. "A nonlinear elliptic curve cryptosystem based on matrices" , Computational Methods in Applied Mathematics (Online) , vol. In Press, Corrected Proof, pp. –, (2005)

TESIS DOCTORALES DEFENDIDAS

1. ALVAREZ SANCHEZ, RAFAEL IGNACIO, "APLICACIONES DE LAS MATRICES POR BLOQUES A LOS CRIPTOSISTEMAS DE CIFRADO EN FLUJO", Directores: TORTOSA GRAU, LEANDRO / ZAMORA GOMEZ, ANTONIO Octubre 2005.

2. FERRANDEZ AGULLO, FRANCISCO, "SISTEMAS CRIPTOGRÁFICOS DE CURVA ELÍPTICA BASADOS EN MATRICES", Director: CLIMENT COLOMA, JOAN JOSEP Mayo 2005.

COMUNICACIONES A CONGRESOS

Nacionales

1. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "Woven convoutional codes from linear system point of view", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Madrid, Septiembre 2005.
2. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "Códigos convolucionales concatenados desde el punto de vista de sistemas", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Madrid, Septiembre 2005.

Internacionales

1. ALVAREZ, R.; TORTOSA, L.; VICENT, J.F.; ZAMORA, A. "A Public Key Cryptosystem Based on Block Upper Triangular Matrices", INFORMATION SECURITY, COMMUNICATIONS AND COMPUTERS (ISCOCO 2005), Puerto de la Cruz, Tenerife, Islas Canarias, Diciembre 2005.
2. AGUIRRE, J–V.; NOGUERA, J.; TORTOSA, L.; ZAMORA, A. "An Exercises Editor for an E–Learning Environment", 4TH WSEAS INT. CONF. ON E–ACTIVITIES, , Noviembre 2005.
3. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "Concatenated convolutional codes from a linear system view", WORKSHOP ON CODING AND SYSTEMS, Würzburg, Noviembre 2005.
4. CLIMENT, J.J.; HERRANZ, V.; PEREA, C. "Woven convolutional codes and some variations from linear systems point of", CONFERENCE OF THE INTERNATIONAL LINEAR ALGEBRA SOCIETY, Regina, Saskatchewan,, Junio 2005.
5. JOSE–VICENTE AGUIRRE, RAFAEL ÁLVAREZ, JOSÉ NOGUERA, LEANDRO TORTOSA, ANTONIO ZAMORA. "A Viability Analysis of a Secure VoIP and Instant Messaging System on a Pocket PC Platform", INFORMATION SECURITY, COMMUNICATIONS AND COMPUTERS (ISCOCO 2005), Puerto de la Cruz, Tenerife, Islas Canarias, Diciembre 2005.
6. RAFAEL ÁLVAREZ, JESÚS–ALBERTO OLIVER, JOSE–FRANCISCO VICENT, ANTONIO ZAMORA. "Secure Communication System over a GSM Network", INFORMATION SECURITY, COMMUNICATIONS AND COMPUTERS (ISCOCO 2005), Puerto de la Cruz, Tenerife, Islas Canarias, Diciembre 2005.