

## GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:

CLIMENT COLOMA, JOAN JOSEP

AÑO DE LA MEMORIA: 2003

### PERSONAL INVESTIGADOR

1. CLIMENT COLOMA, JOAN JOSEP
2. TORTOSA GRAU, LEANDRO
3. 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. "Criptología seguridad computacional", , 12 meses, 1.716,00 €, CLIMENT COLOMA, JOAN JOSEP.
2. "Criptología seguridad computacional", , 12 meses, 1.495,20 €, CLIMENT COLOMA, JOAN JOSEP.
3. "El problema del logaritmo discreto en semianillos finitos. Aplicaciones criptográficas", pr2003-0081 , 4 meses, 15.000,00 €, CLIMENT COLOMA, JOAN JOSEP.
4. "USER FRIENDLY E-COMMERCE TO OPTIMISE PARKING SPACE.", e parking , 24 meses, 298.844,00 €,

#### Privados

1. "PROMOCIÓ DE L¿US DEL VALENCIÀ", 46.578,44€, JOAN JOSEP CLIMENT COLOMA.

### PUBLICACIONES

#### Artículos en publicaciones periódicas:

1. Álvarez, R.; Climent, J.J.; Tortosa, L.; Zamora, A. "A pseudorandom bit generator based on block upper triangular matrices." , Lecture Notes in Computer Science , vol. 2722, pp. 299-300, (2003)
2. Climent, J.J.; Perea, C. "Iterative methods for least square problems based on proper splittings." , Journal of Computational and Applied Mathematics , vol. 158, pp. 43-48, (2003)

3. Climent, J.J.; Perea, C. "Convergence and comparison theorems for a generalized alternating iterative method." , Applied Mathematics and Computation , vol. 143, pp. 1–14, (2003)
4. Climent, J.–J.; Santacruz, J.; Tortosa, L.; Zamora, A. "An algorithm to hide information in binary images" , WSEAS Transactions on Mathematics , vol. 3, pp. 219–224, (2003)
5. Climent, J.J.; Tortosa, L. "Iniciació al MATLAB" , Quaderns de la Col·lecció Joan Fuster. Secretariat de Promoció del Valencià. Universitat d'Alacant , vol. 53, pp. 1–88, (2003)
6. Climent, J.J.; Tortosa, L.; Zamora, A. "A note on the recursive decoupling method for solving tridiagonal linear systems." , Applied Mathematics and Computation , vol. 140, pp. 159–164, (2003)

## TESIS DOCTORALES DEFENDIDAS

No hay tesis

## COMUNICACIONES A CONGRESOS

### Nacionales

1. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "Construcción de códigos convolucionales a partir de sistemas lineales de control discretos en el tiempo", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Tarragona, Septiembre 2003.
2. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "Órdenes parciales y condiciones de convergencia para métodos iterativos basados en particiones", CONGRESO DE ECUACIONES DIFERENCIALES Y APLICACIONES / CONGRESO DE MATEMÁTICA APLICADA, Tarragona, Septiembre 2003.

### Internacionales

1. ÁLVAREZ, R.; CLIMENT, J.–J.; TORTOSA, L.; ZAMORA, A. "A pseudorandom bit generator based on block upper triangular matrices", INTERNATIONAL CONFERENCE ON WEB ENGINEERING (ICWE), Oviedo, Julio 2003.
2. CLIMENT J.J. , SANTACRUZ J., TORTOSA L., ZAMORA A. "An algorithm to hide information in binary images", WSEAF INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN BUSINESS AND ECONOMICS, Tenerife, Diciembre 2003.