GRUPO DE INVESTIGACIÓN: Criptología y seguridad computacional

Director:
CLIMENT COLOMA, JOAN JOSEP

AÑO DE LA MEMORIA: 2004

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 y seguridad computacional", vigrob–025 , 15 meses, 2.334,91 €, CLIMENT COLOMA, JOAN JOSEP.
3. "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. Bru, R.; Climent, J.–J.; Mas, J.; Urbano, A. "Álgebra Lineal (Segunda Edición)" , ISBN: 970–15–0990–0, México, Alfaomega Grupo Editor, S, (2004)

Capítulos en libros:
2. Álvarez, R.; Climent, J.J.; Tortosa, L.; Zamora, A. "Un generador matricial de claves frente a Blum Blum Shub" en "Avances en Criptología y Seguridad de la Información" , ISBN: 84–7978–650–7, Madrid, Diaz de Santos, pp. 113–123, (2004)

3. Arcaina, E.; Climent, J.–J.; Tortosa, L.; Zamora, A. "A system to communicate hidden information using color images" en "Proceedings of the 5th Conference on Mathematics and Computers in Business and Economics" , ISBN: 960–8457–05–X, Venecia, WSEAS Press, pp. 1–6, (2004)
4. Climent, J.–J.; Ferrández, F. "A nonlinear cryptosystem based on elliptic curves" en "Proceedings of the 5th Conference on Mathematics and Computers in Business and Economics" , ISBN: 960–8457–05–X, Venecia, WSEAS Press, pp. 1–8, (2004)
5. Climent, J.–J.; Ferrández, F. "A new cryptosystem based on elliptic curves and polynomial matrices" en "Proceedings of the 5th Conference on Mathematics and Computers in Business and Economics" , ISBN: 960–8457–05–X, Venecia, WSEAS Press, pp. 1–5, (2004)
6. Climent, J.–J.; Herranz, V.; Perea, C. "New convolutional codes from old convolutional codes" en "Electronic Proceedings of the 16th Intenational Symposium on Mathematical Theory of Networks and Systems (MTNS2004)." , ISBN: 90–5682–517–8, , Mathematical Theory of Networks and Systems (MTNS), pp. 1–14, (2004)
7. Climent, J.–J.; Herranz, V.; Perea, C. "A classification of convolutional codes based on Justesen`s construction" en "Electronic Proceedings of the 16th Intenational Symposium on Mathematical Theory of Networks and Systems (MTNS2004)." , ISBN: 90–5682–517–8, , Mathematical Theory of Networks and Systems (MTNS), pp. 1–9, (2004)
8. J.–J. Climent, V. Herranz, C. Perea "New convolutional codes from old convolutional codes." en "Electronic Proceedings of the 16th Intenational Symposium on Mathematical Theory of Networks and Systems (MTNS2004)." , ISBN: 90–5682–517–8, , Mathematical Theory of Networks and Systems (MTNS), pp. –, (2004)
9. J.–J. Climent, V. Herranz, C. Perea "A classification of convolutional codes based on Justesen's construction." en "Electronic Proceedings of the 16th Intenational Symposium on Mathematical Theory of Networks and Systems (MTNS2004)." , ISBN: 90–5682–517–8, , Mathematical Theory of Networks and Systems (MTNS), pp. –, (2004)

Artículos en publicaciones periódicas:

10. Álvarez, R.; Tortosa, L.; Vicent, J.F.; Zamora, A. "An Integral Security Kernel" , TRANSACTIONS on BUSINESS and ECONOMICS , vol. 1, pp. 241–246, (2004)
11. Arcaina, E.; Climent, J.J.; Tortosa, L.; Zamora, A. "A System to Commnicate Hidden Information using Color Images" , TRANSACTIONS on BUSINESS and ECONOMICS , vol. 1, pp. 247–252, (2004)
12. Climent, Joan–Josep; Ferrández, Francisco "A nonlinear cryptosystem based on elliptic curves" , TRANSACTIONS on BUSINESS and ECONOMICS , vol. 1, pp. 253–260, (2004)
13. Climent, Joan–Josep; Ferrández, Francisco "A new cryptosystem based on elliptic curves and polynomial matrices" , TRANSACTIONS on BUSINESS and ECONOMICS , vol. 1, pp. 261–265, (2004)
14. Climent, Joan–Josep; Perea, Carmen; Tortosa, Leandro; Zamora, Antonio "Sequential and parallel synchronous alternating iterative methods" , Mathematics of Computation , vol. 73, pp. 691–717, (2004)
15. Climent, Joan–Josep; Perea, Carmen; Tortosa, Leandro; Zamora, Antonio "A BSP recursive divide and conquer algorithm to solve a tridiagonal linear system" , Applied Mathematics and Computation , vol. 159, pp. 459–484, (2004)
16. Climent, Joan–Josep; Perea, Carmen; Tortosa, Leandro; Zamora, Antonio "Convergence therorems for parallel alternating iterative methods" , Applied Mathematics and Computation , vol. 148, pp. 497–517, (2004)
17. J.J. Climent, García Crespi F., Gutierrez R., Grediaga A. "A Note about Binary Finite Fields Multiplication on FPGA" , WSEAS TRANSACTIONS on CIRCUITS AND SYSTEMS , vol. 3, pp. 1924–1928, (2004)

TESIS DOCTORALES DEFENDIDAS

No hay tesis

COMUNICACIONES A CONGRESOS

Nacionales

1. ÁLVAREZ, R.; CLIMENT, J.J.; TORTOSA, L.; ZAMORA, A. "Un generador matricial de claves frente a Blum Blum Shub", REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (RECSI), Madrid, Septiembre 2004.

Internacionales

1. ÁLVAREZ, R.; TORTOSA, L.; VICENT, J.F.; ZAMORA, A. "An Integral Security Kernel", WSEAS INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN BUSINESS AND ECONOMICS, Venecia, Noviembre 2004.
2. ARCAINA, E.; CLIMENT, J.J.; TORTOSA, L.; ZAMORA, A. "A System to Communicate Hidden Information usin Color Images", WSEAS INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN BUSINESS AND ECONOMICS, Venecia, Noviembre 2004.
3. CLIMENT, J.–J.; HERRANZ, V. ; PEREA, C. "Positive cones and convergence conditions for iterative methods based on splittings", CONFERENCE OF THE INTERNATIONAL LINEAR ALGEBRA SOCIETY, Coimbra, Julio 2004.
4. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "A classification of convolutional codes based on Justesen`s construction", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Katholieke Universiteit Leuven, Julio 2004.
5. CLIMENT, J.–J.; HERRANZ, V.; PEREA, C. "New convolutional codes from old convolutional codes", INTERNATIONAL SYMPOSIUM ON MATHEMATICAL THEORY OF NETWORKS AND SYSTEMS, Katholieke Universiteit Leuven, Julio 2004.
6. CLIMENT, JOAN–JOSEP; FERRÁNDEZ, FRANCISCO. "A new cryptosystem based on elliptic curves and polynomial matrices", WSEAS INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN BUSINESS AND ECONOMICS, Venecia, Noviembre 2004.
7. CLIMENT, JOAN–JOSEP; FERRÁNDEZ, FRANCISCO. "A nonlinear cryptosystem based on elliptic curves", WSEAS INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN BUSINESS AND ECONOMICS, Venecia, Noviembre 2004.