Grupo de Investigación en Criptografía y Seguridad de la Información (GiCSI)

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Grupo de Investigación en Criptografía y Seguridad de la Información (GiCSI)**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Departamento de Tecnologías de la Información y las Comunicaciaones (TIC)**
CENTRO/INSTITUTO/UNIVERSIDAD/ ORGANISMO DE PERTENENCIA	**Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Luís Hernández Encinas**	TELÉFONO	915618806 ext 920458
ROL EN EL EQUIPO	Investigador Científico	MAIL	luis@iec.csic.es
WEB DEL EQUIPO	www.itefi.csic.es/es/departamentos/dtic		

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Agustin Martín Muñoz**	TELÉFONO	915618806 ext 920457
ROL EN EL EQUIPO	Científico Titular	MAIL	agustin@iec.csic.es
WEB DEL EQUIPO	www.itefi.csic.es/es/departamentos/dtic		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Leonardo Torres Quevedo	CENTRO	Instituto de Tecnologías Físicas y de la Información (ITEFI) del C.S.I.C.
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Serrano
NÚMERO	144	CIUDAD	Madrid
PROVINCIA	Madrid	CÓDIGO POSTAL	28006

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	**Luís Hernández Encinas**
MAIL	luis@iec.csic.es
TELÉFONO	915618806 ext 920458
WEB	http://www.itefi.csic.es/es

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Leonardo Torres Quevedo	CENTRO	Instituto de Tecnologías Físicas y de la Información (ITEFI) del C.S.I.C.
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Serrano
NÚMERO	144	CIUDAD	Madrid
PROVINCIA	Madrid	CÓDIGO POSTAL	28006

Grupo de Investigación en Criptografía y Seguridad de la Información (GiCSI)

Características generales | Características del Equipo de Investigación | Características de la Investigación

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Luis Hernández Encinas	Doctor en Ciencias Matemáticas

TRAYECTORIA PROFESIONAL

- IP de 8 Proyectos Nacionales y de 3 Proyectos Internacionales
- Más de 200 Publicaciones en Revistas Nacionales e Internacionales (60 SCI-JCR)
- 11 libros publicados
- Más de 150 comunicacions a congresos nacionales e internacionales
- IP de más de 40 Contratos de Apoyo Tecnológico con Empresas y Organismos Nacionales e Internacionales
- 9 Patentes y Modelos de utilidad
- 7 Tesis doctorales dirigidas
- Índices de impacto en investigación científica: h = 11 (Scopus), h=22 (Google Scholar), i10=52, número de citas=2021
- 4 Tramos de Actividad Investigadora (Sexenios)
- 1 Tramo de Actividad Investigadora Tecnológica (Sexenio Tecnológico)
- 6 Tramos de Méritos Investigadores (Quinquenios)
- Líneas de investigación: Criptografía, Protocolos criptográficos, Privacidad y Autenticación, Ataques por Canal Lateral, Problemas de Teoría de Números,

WEB Y REDES SOCIALES

http://www.itefi.csic.es/es/personal/hernandez-encinas-luis

MIEMBROS DEL EQUIPO

Arroyo Guardeño, David	Fernández Mármol, Verónica	Martín Muñoz, Agustín
Blanco Blanco, Alfonso	Fúster Sabater, Amparo	Negrillo Espigares, Jesús Antonio
DenisenKo Yakucheva, Natalia	Gayoso Martínez, Victor Antonio	Sánchez García, José Ignacio
Fernández-Gallardo Alía, Carlos Juan	Hernández Encinas, Luis	

Grupo de Investigación en Criptografía y Seguridad de la Información (GiCSI)		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
PROCESADO DE DATOS	Procesado seguro de datos y señales cifrados Procesamiento seguro de datos
SISTEMAS FIABLES Y ACTUALIZABLES	
INFRAESTRUCTURAS CRÍTICAS	Métodos y herramientas de Protección Desarrollo de herramientas de protección Cumplimiento normativo de Seguridad
ATAQUES Y DEFENSA ANTE AMENAZAS	Filtraciones de Información
GESTIÓN DE LA IDENTIDAD	Autenticación biométrica Autenticación criptográfica Protocolos de autenticación
OTRAS	Criptografía y criptoanálisis de sistemas de cifrado simétricos y asimétricos Sistemas experimentales de cifrado e intercambio de clave por métodos cuánticos Protocolos criptográficos: autenticación, firma, compartición de secretos, e-votación, etc. Criptoanálisis de criptosistemas caóticos continuos y discretos Análisis de vulnerabilidades de dispositivos físicos criptográficos mediante canales laterales Teoría de la complejidad Generadores de bits pseudoaleatorios Complejidad lineal de secuencias binarias pseudoaleatorias Seguridad en redes de información Gestión de riesgos de sistemas de información Seguridad en las comunicaciones y las aplicaciones web Mecanismos criptográficos para la atribución, legitimidad y transparencia en sistemas.

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2020

Querejeta-Azurmendi, I; Arroyo Guardeño, D.; Hernández-Ardieta, J.L. and Hernández Encinas, L. *"NetVote: A Strict-Coercion Resistance Re-Voting Based Internet Voting Scheme with Linear Filtering", Mathematics, 8 (9), 1618 (2020), 37 pp., Special Issue "Mathematics Cryptography and Information Security", doi: 10.3390/math8091618.*

Gayoso Martínez, V.; Hernández Encinas, L.; Martín Muñoz, A. and Durán Díaz , R. *"Using the Spanish national identity card in social networks", Logic Journal of the IGPL 28, 4 (2020), 519–530, doi: 10.1093/jigpal/jzz058.*

Durán Díaz, R.; Hernández Encinas, L. and Muñoz Masqué, J. *"A Group Law on the Projective Plane with Applications in Public Key Cryptography". Mathematics, 8 (5), 734 (2020), 20 pp., Special Issue "Mathematics Cryptography and Information Security", doi:10.3390/math8050734.*

Durán Díaz, R., Hernández-ÁIvarez, L., Hernández Encinas, L., and Queiruga-Dios, A. *Chor-Rivest Knapsack Cryptosystem in a Post-Quantum World, 2020 International Conference on Security and Management (Worldcomp-SAM'20), In Transactions on Computational Science and Computational Intelligence, Springer (accepted), Las Vegas (USA), July 27–30, 2020.*

Durán Díaz, R.; Gayoso Martínez, V.; Hernández Encinas, L. and Muñoz Masqué, J. *"Square-Zero Basis of Matrix Lie Algebras", Mathematics, 8(6), 1032 (2020), 9 pp., Special Issue "Algebra and Its Applications",doi: 10.3390/math8061032.*

Gayoso Martínez, V.; Hernández-ÁIvarez, F. and Hernández Encinas, L. *"An improved bytewise approximate matching algorithm suitable for files of dissimilar sizes". Mathematics, 8 (4), 503 (2020), 37 pp., Special Issue "Evolutionary Computation & Swarm Intelligence", doi:10.3390/math8040503.*

Gayoso Martínez, V. ; Hernández-ÁIvarez, L. and Hernández Encinas, L. *"Analysis of the Cryptographic Tools for Blockchain and Bitcoin". Mathematics, 8, 131 (2020), 14 pp., Special Issue "Mathematical Models in Security, Defense, Cyber Security and Cyber Defense", doi:10.3390/math8010131,*

Gayoso Martínez, V.; Hernández Encinas, A.; Hernández Encinas, L. and Martín Muñoz, A. *"Mathematics and Physics in side-channel and fault attacks to cryptosystems", 19th Conference on Applied Mathematics (Aplimat 2020), Proc. 505–512, Bratislava (Slovakia), February 4–6, 2020, ISBN: 978-80-227-4983-1.*

Gayoso Martínez, V.; Hernández Encinas, L.; Martín Muñoz, A. and A. Queiruga Dios. *"Elliptic curves as a basic tool for the security of blockchain", 19th Conference on Applied Mathematics (Aplimat 2020), Proc. 513–520, Bratislava (Slovakia), February 4–6, 2020, ISBN: 978-80-227-4983-1.*

Querejeta-Azurmendi I.; Hernández Encinas L.; Arroyo Guardeño D.; Hernández-Ardieta J.L. *(2020) An Internet Voting Proposal Towards Improving Usability and Coercion Resistance. In: Martínez Álvarez F., Troncoso Lora A., Sáez Muñoz J., Quintián H., Corchado E. (eds) International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems*

Iglesias García J., Diaz J., Arroyo D.*(2020) Hyot: Leveraging Hyperledger for Constructing an Event-Based Traceability System in IoT. In: Martínez Álvarez F., Troncoso Lora A., Sáez Muñoz J., Quintián H., Corchado E. (eds) International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean*

Cardell S.D.; Fúster-Sabater A. *(2020) Linearization of Cryptographic Sequences. In: Martínez Álvarez F., Troncoso Lora A., Sáez Muñoz J., Quintián H., Corchado E. (eds) International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019). CISIS*

Blanco Blanco, Alfonso., Orúe López, Amalia Beatriz., Martín Muñoz, Agustin., Gayoso Martínez, Victor., Hernández Encinas, Luis., Martínez-Graullera, Oscar., Montoya Vitini, Fausto. *(2020) On-the-Fly Testing an Implementation of Arrow Lightweight PRNG Using a LabVIEW Framework. In: Martínez Álvarez F., Troncoso Lora A., Sáez Muñoz J., Quintián H., Corchado E. (eds) International Joint*

Arribas, Ismael., Arroyo, David., and Reshef Kera, Denisa ., *"Sandbox for Minimal Viable Governance of Blockchain Services and DAOs: CLAUDIA". In: Blockchain and Applications. BLOCKCHAIN 2020. Advances in Intelligent Systems and Computing, vol 1238. Springer, 2020, pp. 24–30. doi: 10 . 1007 / 978 - 3 - 030 - 52535 - 4 _ 3. url: http : / / link . springer . com / 10 . 1007 / 978 - 3 - 030 - 52535*

Arroyo, David *"En la encrucijada de la "blockchain": posibilidades, expectativas y retos en la configuración de nuevos espacios de confianza digital". In: Novática (https://www.novatica.es/en-la-encrucijada de-la-blockchain-posibilidades-expectativas-y-retos-en-la-configuracion de-nuevos-espacios-de-confianza-digital/) (2020).*

Cardell,Sara D., Climent, Joan-Josep., Fúster-Sabater, Amparo., and Requena, Verónica *"Representations of Generalized Self-Shrunken Sequences". In: Mathematics 8.6 (June 2020), p. 1006. issn: 2227- 7390. doi: 10.3390/math8061006. url: https://www.mdpi.com/ 2227-7390/8/6/1006.*

Fernández, Verónica., Orue, Amalia B., and Arroyo, David., *"Securing Blockchain with Quantum Safe Cryptography: When and How?" In: Conference on Complex, Intelligent, and Software Intensive Sys tems. Springer, Cham. 2020, pp. 371–379.*

Palacio Marín, Ignacio., and Arroyo, David *"Fake News Detection". In: Conference on Complex, Intelligent, and Software Intensive Sys tems. Springer, Cham. 2020, pp. 229–238.*

de la Torre-Abaitua, Gonzalo., Lago-Fernández, Luis F., and Arroyo, David., *"On the application of compression-based metrics to iden tifying anomalous behaviour in web traffic". In: Logic Journal of the IGPL 28.4 (July 2020), pp. 546–557. issn: 1367-0751. doi: 10. 1093/jigpal/jzz062. url: https://academic.oup.com/jigpal/ article/28/4/546/5709611.*

Gayoso Martínez, Víctor., Hernández Encinas, Luis., and Martín Muñoz, Agustín *"Study of the Reconciliation Mechanism of NewHope". In: Computational Intelligence in Security for Information Systems Conference CISIS 2019: 13th International Conference on Com putational Intelligence in Security for Information Systems (CISIS 2020). Springer, 2021, pp. 361–370. doi: 10.1007/978- 3- 030- 57805-3_34. url:*

Martín-Navarro, Jose Luis., Fúster-Sabater, Amparo., and Cardell Sara D. *"An Innovative Linear Complexity Computation for Cryp tographic Sequences". In: Computational Intelligence in Security for Information Systems Conference CISIS 2019: 13th International Conference on Computational Intelligence in Security for Infor mation Systems (CISIS 2020). Springer, 2021, pp. 339–349. doi: 10.1007/978-3-*

Cardell, S.D.; Aranha, D. F.; Fúster-Sabater, A. *"Recovering decimation-based cryptographic sequences by means of linear CAs". Logic Journal of the IGPL,vol. 28, Issue 4, pp. 430-448, 2020. DOI:10.1093/jigpal/jzz051.*

Fúster-Sabater, A.; Cardell, S.D. *"Linear complexity of generalized sequences by comparison of PN-sequences". Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales Serie A, vol. 114, pp. 79-97, April 2020. ISSN: 1578-7303. DOI:10.1007/s13398-020-00807-5. URL: http://link.springer.*

Martín-Navarro, J. L., Fúster-Sabater, *"Folding-BSD Algorithm for Binary Sequence Decomposition". Proceedings of the 20th International Conference on Computational Science and Its Applications, ICCSA 2020, Cagliari, Italy, July 1-4, 2020. O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12249, pp. 345-359, 2020. https://doi.org/10.1007/978-3-030-58799-4_26*

Cardell, S. D., Fúster-Sabater, A., Orúe, A. B., Requena, V. *"Randomness Analysis for GSS-sequences Concatenated", Proceedings of the 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020), Burgos, Spain, September 16 – 18, 2020. Á. Herrero et al. (Eds.), Advances in Intelligent Systems and Computing (AISC), 1267, pp. 350-360, 2021. ISBN: 978-3-030-57804-6. https://doi.org/10.1007/978-3-030-57805-3_33*

PUBLICACIONES AÑO 2019

Arroyo Guardeño D,; Díaz Vico, J. y Hernández Encinas, L. (Libro): *Blockchain, Colección: ¿Qué sabemos de?, 103* . Editorial CSIC-Catarata, Madrid, 2019, 144 ISBN: 978-84-9097-684-5.

de La Torre Abaitua G.; Lago Fernández L.; Arroyo D. *(2019) Un resumen de "Aplicación de técnicas de compresión de información a la identificación de anomalías en fuentes de datos heterogéneas: análisis y limitaciones". V Jornadas Nacionales de Investigación en Ciberseguridad.*

Rodriguez Cesar, H.; Gayoso Martinez, V.; Hernandez Encinas, L. and Martin Muñoz, A. *"Format-Preserving Encryption: Image Encryption Under FF1 Scheme", International Journal of Advances in Electronics and Computer Science (IJAECS), 6, 12 (2019), 1–4, http://www.iraj.in/journal/journal_file/journal_pdf/12-618-15808813701-4.pdf*

Beasley, Leroy B.; Hernandez Encinas, Luis and Song Seok-Zun, *"Strong preservers of symmetric arctic rank of nonnegative real matrices", J. Korean Math. Soc. 56, 6 (2019), 1503–1514 (on-line: 2019 Apr 04), https://doi.org/10.4134/JKMS.j180771*

Cardell Díaz, Sara and Fúster-Sabater, Amparo *"Cryptography with Shrinking Generators. Fundamentals and Applications of Keystream Sequence Generators Based on Irregular Decimation". Serie: Springer Briefs in Mathematic, Springer International Publishing, Springer Nature Switzerland, 2019, ISBN: 978-3-030-12849-4. DOI: 10.1007/978-3-030-12850-0*

Cardell, S.D.; Fúster-Sabater, A.*"Binomial representation of cryptographic binary sequences and its relation to cellular automata". Complexity, vol.2019, ID 2108014, pp. 1-13, Mar. 2019. DOI:10.1155/2019/2108014. URL: https://www. hindawi.com/journals/complexity/2019/2108014/.*

Conde Pena, M.; Durán Díaz, R.; Faugère, J.-C.; Hernández Encinas, L. and L. Perret, *"Non-quantum Cryptanalysis of the Noisy Version of Aaronson-Christiano's Quantum Money Scheme". IET Information Security, 13, 4 (2019), 362-366.*

Fuentes Rodríguez, A.; Hernández Encinas, L.; Martín Muñoz, A. and Alarcos Alcázar, B. *"A Modular and Optimized Toolbox for Side-Channel Analysis". IEEE Access 7 (2019), 21889-21903, doi:10.1109/ACCESS.2019.2897938.*

Fúster-Sabater, A.; Cardell, S.D. *"Linear complexity of generalized sequences by comparison of PN-sequences". Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales Serie A-Matemáticas,*

Gayoso Martínez, V,; Hernández Encinas, L.;. Martín Muñoz, A and Martínez-Graullera, O. *"Comparing low and medium cost computer-based technologies suitable for cryptographic attacks". Logic Journal of the IGPL, 27, 2 (2019), 177-188 (on-line: 2018 Sep 17).*

Gayoso Martínez, V.; Hernández Encinas L.; Martín Muñoz A.; R. Durán Díaz, *"Secure elliptic curves and their performance". Logic Journal of the IGPL, 27, 2 (2019), 277-238 (on-line: 2018 Sep 17).*

Orúe López,A.B., Blanco Blanco, A., Martín Muñoz, A., Gayoso Martínez, V., Martínez Graullera, O. Hernández Encinas,L., and Montoya Vitini, F.*"On-the-fly testing an implementation of a lightweight PRNG using a LabVIEW framework". 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019), Proc. 175-184, Sevilla (Spain), May 13-15,*

Orúe, A.B., Orúe, A.M. and Montoya, L., Gayoso, V. and Martín, A. *"Enhancing the Learning of Cryptography Through Concept Maps", 12th International Conference on Computatio nal Intelligence in Security for Information Systems (CISIS 2019), Proc. 263-272, Sevilla (Spain), May 13-15, 2019.*

Durán Díaz, R, Hernández Encinas, L. and Muñoz Masqué, J. *"Quadratic Maps in Two Variables on Arbitrary Fields". Carpathian J. Math, arXiv:1901.05702 .Mathematics > Representation Theory. arXiv. Cornell University*

de La Torre Abaitua G., Lago Fernández L., Arroyo D. *(2019) Un resumen de "Aplicación de técnicas de compresión de información a la identificación de anomalías en fuentes de datos heterogéneas: análisis y limitaciones". V Jornadas Nacionales de Investigación en Ciberseguridad.*

Fúster-Sabater A., Cardell S.D., *"Propiedades estructurales de los generadores t-modificados". Sesión Especial 20: Matemáticas en la Teoría de la Información. Ponencia no. 12. Actas del Congreso Bienal de la Real Sociedad Matemática Española (RSME 2019), 13, Santander, España, 4-8 de febrero, 2019.*

PUBLICACIONES RELACIONADAS DESTACADAS

de Andrés, Pablo., Arroyo, David., Correia, Ricardo., Rezola, Alvaro., *"Regulatory and Market Challenges of Initial Coin Offerings". In: European Corporate Governance Institute-Law Working Paper (2019).*

Arteaga-Díaz, Pablo; Ocampos-Guillén, Alejandro; Fernandez, Veronica, *"Enabling QKD under Strong Turbulence for Wireless Net works with Tilt Wavefront Correction". In: 2019 21st International Conference on Transparent Optical Networks (ICTON). IEEE, July 2019, pp. 1–4. isbn: 978-1-7281-2779-8. doi: 10 . 1109 / ICTON . 2019.8840410. url: https://ieeexplore.ieee.org/document/ 8840410/.*

Cardell, Sara D., and Fuster-Sabater, Amparo. *"Binomial Characterization of Cryptographic Sequences". In: 19th International Confer ence on Computational Science and Its Applications, ICCSA 2019. ICCSA, 2019, pp. 803–816. doi: 10.1007/978-3-030-24289-3_59. url: http://link.springer.com/10.1007/978-3-030-24289-*

Cardell, Sara D.; Requena, Verónica; Fúster Sabater, Amparo; Orúe, Amalia B. *"Randomness Analysis for the Generalized Self-Shrinking Sequences". In: Symmetry 11.12 (Nov. 2019), p. 1460. issn: 2073-8994. doi: 10.3390/sym11121460. url: https://www. mdpi.com/2073-8994/11/12/1460.*

Diaz, Jesus., Geol Choi, Seung., Arroyo, David., Keromytis, Angelos D., Rodriguez, Francisco B., Yung, Moti *.,"A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions". In: Advances in Cy ber Security: Principles, Techniques, and Applications. Singapore: Springer Singapore, 2019, pp. 143–183. isbn: 978-981-13-1483-4. doi: 10 . 1007 / 978 - 981 - 13 - 1483 - 4 _ 7. url: https :*

Fernandez, Veronica., *Enabling-free space QKD under strong turbulent conditions with double-loop wavefront tilt correction. 1st In ternational Quantum International Quantum Information Sciences Workshop. 2019. url: https://www.suny.edu/events/quantum2019/.*

Ocampos-Guillén, Alejandro., Gómez-García, J., Denisenko, N., Fernández, Veronica., *Double-Loop Wavefront Tilt Correction for Free-Space Quantum Key Distribution. In: IEEE Access 7 (2019), pp. 114033–114041. issn: 2169-3536. doi: 101109/ACCESS.2019.2933694. url: https://ieeexplore.ieee. org/document/8790692/.*

Hernández Encinas, L. *(E), Special Issue "Mathematics Cryptography and Information Security" of the Journal "Mathematics (Basel)" , February 26–December 31, https://www.mdpi.com/journal/mathematics/special_issues/Mathematics_Cryptography_Information_ Security.*

Hernández Encinas, L. *(E), Special Issue "Cryptography and Information Security in Wireless Sensor Networks" of the Journal "Sensors", https://www.mdpi.com/journal/ sensors/special_issues/Cryptography_Information_Security.*

Gayoso Martínez V.,y Hernández Encinas, L. "*La amenaza de la computación cuántica: ¿hay cripto después?", XIII Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, Diciembre 11–12, 2019, https://youtu.be/eudffSU51K0*

Hernández Encinas, L. *"Fundamentos criptográficos de la Blockchain y de bitcoin", Simposio de Ingenierías y Seguridad Informática, Universidad Vasco de Quiroga, Morelia (México), Octubre 3, 2019.*

PUBLICACIONES AÑO 2018

Gayoso Martínez, V.; Hernández Encinas, L. ; y Martín Muñoz, A. *"Criptografía con Curvas Elípticas". CSIC, Biblioteca de Ciencias no 44 , 2018, 261 pp., ISBN: 978-84-00-10432-0 (papel), 978-84-00-10433-7 (electrónico).*

de Fuentes,J.M.; Hernández Encinas, L. and Ribagorda, A.*"Security Protocols for Network and Internet: A Global Vision". Chapter 8 of the book "Computer and Network Security Essentials", Springer International Publishing, The Netherlands, 2018, 135-151, ISBN: 978-3-319-58423-2.*

Sánchez-Gómez, A.; Diaz, J.; Hernández Encinas, L. and D. Arroyo, *"Review of the Main Security Treats and Challenges in Free-Access Public Cloud Storage Servers". Chapter 15 of the book "Computer and Network Security Essentials", Springer International Publishing, The Netherlands, 2018, 263-281, ISBN: 978-3-319-58423-2.*

Gayoso Martínez, V.; González-Manzano, L. and Martín Muñoz, A.*"Secure Elliptic Curves in Cryptography". Chapter 16 of the book "Computer and Network Security Essentials", Springer International Publishing, The Netherlands, 2018, 283-298, ISBN: 978-3-319-58423-2.*

Daimi, K.; Francia, G.; Ertaul, L.; Hernández Encinas, L. and E. El-SheikhP, *"Computer and Network Security Essentials". Springer International Publishing, The Netherlands, 2018, 618 pp., ISBN: 978-3-319-58423-2, doi:10.1007/978-3-319-58424-9.*

Cardell, S.D.; Fúster-Sabater, A.; Ranea, A. H. *"Linearity in decimation-based generators: an improved cryptanalysis on the shrinking generator". Open Mathematics 16 (2018), 646-655.*

Hernández Encinas, L. and Martín del Rey, A. *"Boolean differential operators". Turkish Journal of Mathematics, 42 57-68 (2018), doi:10.3906/mat-1607-22.*

Romera, M.; Pastor, G.; Danca, M.-F.; Martin, A.; Orue, A.B.; Montoya, F.; Hernández Encinas, L. and Tundrea, E. *"Bifurcation Diagram of a Map with Multiple Critical Points". International Journal of Bifurcation and Chaos 28, 05, 1850065 (2018), doi:10.1142/S0218127418500657.*

Arroyo Guardeño, D., Rezola Borrego,Á.,y Hernández Encinas, L. *"Principales problemas de seguridad en los smart contracts de Ethereum", XII Jornadas de Seguridad TIC del CCNCERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, diciembre 12-13, 2018.*

Blanco Blanco, A., Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A., Montoya Vitini, F., y Orúe López. A.B., *"Generador de ruido Zener para incrementar la entropía de un TRNG". XV Reunión Española de Criptología y Seguridad de la Información (RECSI 2018), Actas 22-25, P. García Teodoro, R. Barragán Gil y N.M. Fuentes García (Eds.), ISBN: 978-84-09-02463-6, Granada, octubre 3-*

Cardell, S.D., Fúster-Sabater. A., *"The t-modified Self-shrinking Generator". Proceedings of the International Conference on Computational Science, ICCS Wuxi, China, 11-13 June, 2018, Y. Shi et al. (Eds.): ICCS 2018, LNCS 10860, 653-663, 2018.*

Querejeta Azurmendi, I., López Hernández-Ardieta, J., y Hernández Encinas, L., *"Don't shoot the messenger. How a trusted channel may not be a necessary assumption for remote codevoting". IV Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2018), Actas 95-96, U. Zurutuza, M. Iturbe, E, Ezpeleta e I. Garitano (Eds.) ISBN: 978-84-09-02697-5, San Sebastián, junio 13-15, 2018.*

Cardell S.D., Fúster-Sabater. A. *"A generalization of the modified self-shrinking generator". Short Communication. In Section: Mathematical Aspects of Computer Science. Ponencia SC.14.5. International Congress of Mathematicians ICM 2018, Rio de Janeiro, Brazil, August 1-9, 2018.*

Cardell, S.D., Fúster-Sabater, A. *"Applications of binomial sequences to Cryptography". Poster. In World Meeting for Women in Mathematics - (WM)², a satellite event of the ICM 2018, International Congress of Mathematicians ICM 2018. Rio de Janeiro, Brazil, July 31, 2018.*

Cardell, S.D., Fúster-Sabater. A. *"Linearisation of the irregular decimation-based generators". Encuentro de la Red Temática de Álgebra Lineal, Análisis Matricial y Aplicaciones (ALAMA 2018), 30 mayo-1 junio, 2018. Universidad de Alicante, España.*

Fúster-Sabater, A., Cardell,S.D. *"Computing the linear complexity in a class of cryptographic sequences". Proceedings of the 18th International Conference on Computational Science and Its Applications, ICCSA 2018, Melbourne, Australia, July 2-5, 2018. Gervasi O. et al. (Eds.): ICCSA 2018, Part I, LNCS 10960, 110-122, 2018. ISBN: 978-3-319-951*

Fúster Sabater, A. Cardell, S.D. *"Calculando la complejidad lineal de secuencias criptográficas mediante PN-secuencias". Actas de la XV Reunión Española de Criptología y Seguridad de la Información (RECSI), 12-17, Granada, 3-5 octubre 2018, ISBN: 978-84-09-02463-6.*

Diaz, Jesus, Geol Choi, Seunget, Arroyo, David, Keromytis, Angelos D., de Borja Rodríguez Ortiz, Francisco, Yung, Moti *"Privacy in e-shopping transactions: Exploring and addressing the trade-offs". In: International Symposium on Cy ber Security Cryptography and Machine Learning. Springer, Cham. 2018, pp. 206–226.*

de la Torre Abaitua, Gonzalo., Lago-Fernández, Luis. F., and Arroyo, David., *"Aplicacióon de técnicas de compresión de información a la identificación de anomalías en fuentes de datos heterogéneas: análisis y limitaciones (póster)". In: V Jornadas Nacionales de In vestigación en Ciberseguridad. 2019.*

Orúe López, Amalia Beatriz., Fúster Sabater, Amparo., Fernández Mármol, Verónica ., Montoya Vitini,Fausto., Hernández Encinas, Luis y Martín Muñoz, Agustín. *Herramientas gráficas de la criptografía caótica para el análisis de la calidad de secuencias pseudoaleatorias. XIV Reunión Española sobre Criptología y Seguridad de la Información (RECSI). Mahón (Menorca). Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información. pp. 180-185. ISBN: 978-84-608-9470-4. http://recsi16.uib.es/actas/*

Cardell, S. D., Fúster-Sabater. A. *"Recovering decimation-based cryptographic sequences by means of linear CAs". Subjects: Cryptography and Security (cs.CR), arXiv.org, arXiv:1802.02206, 2018.*

PUBLICACIONES AÑO 2017

Cardell, S. D., Fúster-Sabater, A. *"Discrete linear models for the generalized self-shrunken sequences". Finite Fields and Their Applications, vol. 47,1 (2017), 222-241), doi:10.1016/j.ffa.2017.06.010.*

Martin del Rey, A., Hernández Guillén, J.D., Hernández Encinas, Luis *"Study of the stability of a SEIRS model for computer worm propagation", Physica A - Nonlinear Analysis, 479411-421 (2017), doi:10.1016/j.physa.2017.03.023*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A., Álvarez Mariño, M.A., Arroyo Guardeño, D. *"A comparative study of three Spanish eGoverment smart cards", Logic Journal of the IGPL, 25,1 (2017), 42-53), doi:10.1093/jigpal/jzw038.*

Durán Díaz, R., Hernández Encinas, L., Martín Muñoz, A., Muñoz Masqué, J. and Seok-Zun Song (A), *"A characterization of non-prime powers", Turkish Journal of Mathematics 41, 5, 1248–1259 (2017), http://doi.org/10.3906/mat-1603-143*

Mojica López, M., Rodrigo Oliva, J.L., Gayoso Martínez, V., Hernández Encinas L. y Martín Muñoz, A. *"Análisis de la Privacidad de WhatsApp Messenger", Revista Iberoamericana de Sistemas, Cibernética e Informática, RISCI, vol. 14, num.23, pp 73-78, ISSN 1690-8627, (2017). http://www.iiisci.org/Journal/riSCI/FullText.asp?var=&id=CA890ED17.*

Cardell, S. D., Fúster-Sabater, A., Li Bin. *"A New Simple Attack on a Wide Class of Cryptographic Sequence Generators", Proceedings of the International Joint Conference SOCO'17-CISIS'17-ICEUTE'17, León, Spain, September 6–8, 2017. H. Pérez García et al. (Eds.), Advances in Intelligent Systems and Computing, 649, pp. 533-543, 2017. ISBN: 978-3-319-67179-6. doi:10.1007/978-3-319-67180-2_5*

Cardell, S. D., Fúster-Sabater, A., *"Linear Models for High-Complexity Sequences", Proceedings of the 17th International Conference on Computational Science and Its Applications, ICCSA 2017, Trieste, Italy, July 3-6, 2017. Gervasi O. et al. (Eds.): ICCSA 2017, Part I, LNCS 10404, pp. 314-324, 2017. ISBN: 978-3-319-62391-7. doi: 10.1007/978-3-319-62392-4_23.*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A. and Durán Díaz, R. *"A Proposal for Using a Cryptographic National Identity Card in Social Networks", International Workshop on Computational Intelligence in Security for Information Systems (CISIS'17), Advances in Intelligent Systems and Computing 649, 651-660, ISBN: 978-3-319-67179-6, León (Spain), September 6-8, 2017. Core B.*

Orúe, A. Beatriz, Hernández Encinas, L., Fernández, V., Montoya, F. *"A Review of Cryptographically Secure PRNGs in Constrained Devices for the IoT", International Workshop on Computational Intelligence in Security for Information Systems (CISIS'17), Advances in Intelligent Systems and Computing 649, 672-682, ISBN: 978-3-319-67179-6, León (Spain), September 6-8, 2017. Core B.*

PUBLICACIONES RELACIONADAS DESTACADAS

Hernández Guillén, J.D., Martín del Rey, A., Hernández Encinas, L. *"New Approaches of Epidemic Models to Simulate Malware Propagation", International Workshop on Computational Intelligence in Security for Information Systems (CISIS'17), Advances in Intelligent Systems and Computing 649, 631-640, ISBN: 978-3-319-67179-6, https://link.springer.com/chapter/10.1007/978-3-319-67180-2_61, León*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A. and Zhang, J. *"Breaking a Hitga2 Protocol with Low Cost Technology". 3rd International Conference on Information Systems Security and Privacy (ICISSP'2017) Proceedings 579-584, P.Mori, S. Furnell and O. Camp (Ed.), ISBN: 978-989-758-209-7. Porto (Portugal), February 19-21, 2017.*

Cardell, S. D., Fúster-Sabater. A. *"Linear models for the modified self-shrinking generator", Extended Abstracts of the 16th International Conference on Computer Aided Systems Theory, EUROCAST 2017, Las Palmas de Gran Canaria, Canary Islands, Spain, February 19-24, 2017. R. Moreno-Díaz et al. (Eds.): EUROCAST 2017, pp. 9-11, 2017. ISBN: 978-84-617-8087-7.*

Ocampos-Guillen,Alejandro., Gómez-García, Jorge., Denisenko, Natalia and Fernandez, Veronica *Double-loop wavefront tilt correction for free-space quantum key . IEEE Access PP(99):1-1 DOI: 10.1109/ACCESS.2019.2933694*

Orúe, A. B., Hernández-Encinas, L., Martín, A.,and Montoya, F. *"A lightweight Pseudorandom Number Generator for securing the Internet of Things", IEEE Access 5, 27800–27806 (2017), http: //doi.org/10.1109/ACCESS.2017.2774105.*

Fuentes Rodríguez, A.,. Hernández Encinas, L., Martín Muñoz, A., Alarcos Alcázar ,B. *Generación de valores intermedios de forma paralela en ataques DPA.IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2017). Buenos Aires (Argentina). Libro de Actas del IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2017). Páginas: 67-74. ISBN: 978-950-23-2811-9*

Blanco Blanco, A., de Fuentes, J. M., González Manzano, L., Hernández Encinas, L., Martín, Muñoz, A., Rodrigo Oliva, J. L. and Sánchez García, J. I. *A framework for acquiring and analyzing traces from cryptographic devices.13th EAI International Conference on Security and Privacy in Communication Networks. Workshop on Security and Privacy on Internet of Things (SePrIoT). Niagara Falls, (Canada).*

Hernández Encinas, L., Gayoso Martínez, V. y Arroyo Guardeño, D. "*Frente al computador cuántico, Criptografía postcuántica, XI Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, Diciembre 13–14, 2017, https://www.ccn-cert. cni.es/xijornadas-ponencias, https://www.ccn-cert.cni.es/xijornadas-videos*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A. and Mojica López, M. *Security analysis of the device-stored data generated by Instant Messaging applications in Android devices, IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2017), Actas 75–82, ISBN: 978-95023-2811-9, A.E. Dams, H.A. Pagola, L.E. Sánchez Crespo y J. Ramió Aguirre (Eds.), Buenos Aires (Argentina),*

Querejeta Azurmendi, I., López Hernández-Ardieta, J., Gayoso Martínez, V., Hernández Encinas, L., Arroyo Guardeño, D., *A coercion-resistant and easy-to-use Internet e-voting protocol based on traceable anonymous certificates, III Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2017), Actas 1–8, M. Beltrán y F. Ortega (Ed.) ISBN: 978-84-608-4659-8, Madrid, 31 Mayo–2 Junio, 2017.*

González-Manzano, L., de Fuentes, José M., Pastrana, Sergio., Peris-Lopez, Pedro., Hernández-Encinas, Luis. *PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things. III Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2017), Actas 202–203, M. Beltrán y F. Ortega (Ed.) ISBN: 978-84-608-4659-8, Madrid, 31 Mayo–2 Junio, 2017.*

PUBLICACIONES AÑO 2016

Hernández Encinas, Luis, Espinosa García, Javier 2016 Claves para la gestión de la seguridad integral

Hernández Encinas, Luis, 2016. La Criptografía, ¿Qué sabemos de?, Editorial CSIC-Catarata, Madrid, 2016, 142 pp. ISBN: 978-84-00-10045-2.

Hernández Encinas, Luis, Espinosa García,Javier, *2016. Una visión de la Seguridad Integral para una Formación Global en Seguridad*

Castrillón López, M., Hernández Encinas, L., Martínez Gadea, P., Rosado María, M.E., *"Geometry, Algebra and Applications: From Mechanics to Cryptography", Springer International Publishing Switzerland, 2016, 181-187, SBN: 978-3-319-32084-7 (Print) 978-3-319-32085-4 (Online), http://link.springer.com/book/10.1007/978-3-319-32085-4*

Molina-Gil, J., Caballero-Gil, P., Caballero-Gil, C., Fúster-Sabater, A., *"Software Implementation of the SNOW 3G Generator on iOS and Android Platforms", Logic Journal of the IGPL, vol. 24,1 (2016), 29-41), doi:10.1093/jigpal/jzv042*

Cardell, S. D., Fúster-Sabater, A., *"Modelling the Shrinking Generator in Terms of CA", Advances in Mathematics of Communications, vol. 10,4 (2016), 797-809), doi:10.3934/amc.2016041.*

Peinado, A., Munilla, J. Fúster-Sabater, A., *"Optimal Modes of Operation of Pseudorandom Sequence Generators based on DLFSRs", Logic Journal of the IGPL, vol. 24,6 (2016), 933-943), doi:10.1093/jigpal/jzw050*

Cardell, Sara D., and Fúster-Sabater, Amparo. *"Linear Models for the Self-Shrinking Generator Based on CA", Journal of Cellular Automata 11, 195-211 (2016).*

Fuentes Rodríguez, A.,. Hernández Encinas, L., Martín Muñoz, A., Alarcos Alcázar ,B. *"Design and Optimization of the Input Modules of a DPA Toolbox", Logic Journal of the IGPL 24,1 (2016), 16-28, doi:10.1093/jigpal/jzv041.*

Pastor, G., Romera, M., Danca, M.-F., Martin, A., Orue,A.B., Montoya, F., Hernández Encinas, L. *"Hidden and non-standard bifurcation diagram of an alternate quadratic system", International Journal of Bifurcation and Chaos, 26, 2 (2016) 1550036 (14 pages), doi:10.1142/S021812741650036X.*

Durán Díaz, R. and Hernández Encinas, L. *"Special Primes: Properties and Applications", Geometry, Algebra and Applications: From Mechanics to Cryptography, Springer International Publishing Switzerland, 2016, 79-90, doi.org/10.3906/mat-1603-143.*

Fúster Sabater, A. and Montoya Viniti, F. "*Classes of Nonlinear Filters for Stream Ciphers", Geometry, Algebra and Applications: From Mechanics to Cryptography, Springer International Publishing Switzerland, 2016, 107-119, doi.org/10.1007/978-3-319-32085-4_10.*

Gayoso Martínez V., Hernández Encinas, L., Martín Muñoz, A. *"Implementation of Cryptographic Algorithms for Elliptic Curves", Geometry, Algebra and Applications: From Mechanics to Cryptography, Springer International Publishing Switzerland, 2016, 121-133, http://link.springer.com/chapter/10.1007/978-3-319-32085-4_11.*

Cardell, Sara D and Fúster-Sabater, Amparo. *"Recovering the MSS-sequence via CA", Procedia Computer Science 80, 599-606 (2016), The International Conference on Computational Science (ICCS 2016), San Diego, 6-8 de junio de 2015. doi:10.1016/j.procs.2016.05.346.*

Cardell, Sara D and Fúster-Sabater, Amparo. *"Cryptographic Properties of Equivalent Ciphers", Procedia Computer Science 80, 2236-2240 (2016), The International Conference on Computational Science (ICCS 2016), San Diego, 6-8 de junio de 2015. doi:10.1016/j.procs.2016.05.391.*

Queiruga-Dios, A., Rodríguez Sánchez, G. Hernández Encinas, A. Martín del Rey, A., Martín Vaquero, J. and Hernández Encinas, L. *"Case study: Malware propagation models for undergraduate engineering students". Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'16) Proceedings 931-936, F.J. García-Peñalvo (Ed.), ISBN: 978-1-4503-4747-1.*

Cardell, S. D., Fúster-Sabater. A. *"Modelling the MSSG in Terms of Cellular Automata", doi:10.1007/978-3-319-42085-1 40, Proceedings of the 16th International Conference on Computational Science and Its Applications, ICCSA 2016, Beijing, China, July 4-7, 2016. Gervasi O. et al. (Eds.): ICCSA 2016, Part I, LNCS 9786, pp. 514-520, 2016. ISBN: 978-3-319-42084-4.*

Cardell, S. D., Fúster-Sabater. A. *"The modified self-shrinking generator via the generalized self-shrinking generator", Proceedings of the 16th International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE 2016, Costa Ballena (Rota), Cadiz, Spain, July 4-8, 2016. J. Vigo-Aguiar. (Ed): CMMSE 2016, pp. 326-328, 2016. ISBN: 978-84-608-6082-2.*

Queiruga-Dios, A., Hernández Encinas, A. Martín-Vaquero, J.,Hernández Encinas, L. *"Malware Propagation Models in Wireless Sensor Networks: A Review", International Workshop on Computational Intelligence in Security for Information Systems (CISIS'16). International Joint Conference SOCO'16-CISIS'16-ICEUTE'16, M. Graña, J.M. López-Guede, O. Etxaniz, Á. Herrero, H. Quintián, E. Corchado*

Durán Díaz, R., Gayoso Martínez, V., Hernández Encinas, L. and Martín Muñoz, A.*"A study on the performance of secure elliptic curves for cryptographic purposes", International Workshop on Computational Intelligence in Security for Information Systems (CISIS'16). International Joint Conference SOCO'16-CISIS'16-ICEUTE'16, M. Graña, J.M. López-Guede, O. Etxaniz, Á. Herrero, H. Quintián, E.*

Cardell, S. D., Fúster Sabater, A. *"Modelos lineales basados en CA para las secuencias auto-shrinking". Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información, RECSI XIV, 2016. Pep Lluís Ferrer Gomila, M. Francisca Hinarejos Campos (Eds): pp. 30-35, Maó, Menorca, Illes Balears, 26–28 Octubre 2016. ISBN: 978-84-608-9470-4.*

Delgado, O., Arroyo, D., Díaz, J. y Hernández, L. *"Blockchain: Usos y Abusos", X Jornadas de Seguridad TIC del CCN-CERT Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, diciembre 13-14, 2016.*

Durán Díaz, Raúl; Gayoso Martínez, Víctor; Hernández Encinas, Luis *"Generación de primos demostrables: implementación y resultados", XIV Reunión Española de Criptología y Seguridad de la Información (RECSI 2016). Actas 58-63-46, P.L. Ferrer Gomila y M.F. Hinarejos Campos (Eds.), ISBN: 978-84-608-9470-4, Mahón, octubre 26-28, 2016.*

Orúe, A.B., Fúster, A., Fernández, V., Montoya, F., Hernández, L., Martín, A. *"Herramientas visuales usadas en criptografía caótica útiles para el análisis de secuencias pseudoaleatorias", XIV Reunión Española de Criptología y Seguridad de la Información (RECSI 2016). Actas 180-185, P.L. Ferrer Gomila y M.F. Hinarejos Campos (Eds.), ISBN: 978-84-608-9470-4, Mahón, octubre 26-28, 2016.*

Gayoso Martínez, V., Hernández Encinas, L., Martín del Rey A. and Durán Díaz, R. *"Análisis de los métodos de generación de curvas elípticas seguras", Segundas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), Actas 87-93, ISBN: ISBN: 978-84-608-8070-7. Granada, Junio 2016.*

Hernández Guillén, J.D., Martín del Rey, A.and Hernández Encinas, L., Martín del Rey, A. and Durán Díaz, R. *"Propuesta de mejora de un modelo SEIRS para la simulación de la propagación de malware", Segundas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), Actas 136-143, ISBN: ISBN: 978-84-608-8070-7. Granada, Junio 2016.*

Hernández Encinas, Luis y Espinosa García, Javier *"Claves para la gestión de la seguridad integral", Seguritecnia, 01/06/2016, pp. 50, 52, http://www.seguritecnia.es/revistas/seg/432/files/assets/basic-html/page-50.html.*

Hernández Encinas, Luis y Espinosa García, Javier *"Formación y competencias para la gestión de la seguridad integral", Seguritecnia, 01/08/2016, 56–57, http://www.seguritecnia.es/revistas/seg/434/index.html?#56*

Hernández Encinas, Luis y Espinosa García, Javier *"Una visión de la Seguridad Integral para una Formación Global en Seguridad", Revista (on-line) Gestión Documental, 02/04/2016, http://www.revistagestiondocumental.com/2016/04/02/una-vision-la-seguridad-integral-una-formacion-global-seguridad/.*

Gayoso Martínez,V., Hernández Encinas, L., Martín Muñoz, A., Martínez-Graullera, O., and Villazón-Terrazas, J., *"Comparison of Computer-Based Technologies Suitable for Cryptographic Attacks", Advances in Intelligent Systems and Computing, 527, 622–630 (2016), https://doi. org/10.1007/978-3-319-47364-2_60*

Hernández Encinas, L., Martín Muñoz, A., Fernández Mármol, V., Gayoso Martínez, V. Sánchez García, J.I. , Castelluccia, C. and Bourka A., *PETs controls matrix. A systematic approach for assessing online and mobile privacy tools, ENISA, December, 2106, 62 pp., https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-*

PUBLICACIONES RELACIONADAS DESTACADAS

Cardell, S. D., Fúster-Sabater, A. *"Recovering the MSS-sequence via CA". Procedia Computer Science, Elsevier B.V., Vol. 80, pp. 599-606, 2016. DOI:10.1016/j.procs. 2016.05.346*

Fúster-Sabater, A., Cardell, S. D. *"Cryptographic Properties of Equivalent Ciphers". Procedia Computer Science, Elsevier B.V., Vol. 80, pp. 2236–2240, 2016. DOI:10.1016/j.procs. 2016.05.391*

PUBLICACIONES AÑO 2015

Delgado-Mohatar, O., Fúster-Sabater, A., 2015. "Software Implementation of Cryptographic Sequence Generators over Extended Fields". Logic Journal of the IGPL, vol. 23, no. 1, pp. 73-87, 2015. DOI:10.1093/jigpal/jzu039.

Cardell, S. D., Fúster-Sabater, A., 2015. "Performance of the Cryptanalysis over the Shrinking Generator", Álvaro Herrero et al. (Eds.): CISIS'15 and ICEUTE'15, Advances in Intelligent Systems and Computing, 369, pp. 111-121, 2015. ISBN: 978-3-319-19712-8.

Peinado, A., Munilla,J., Fúster-Sabater, A., 2015. Revision of J3Gen and Validity of the Attacks by Peinado et al." Sensors, vol. 15, no. 5, pp. 11988-11992, 2015. DOI:10.3390/s150511988.

Cardell, S. D., Fúster-Sabater, A., 2015 Cryptanalysing the shrinking generator.Procedia Computer Science, Elsevier B.V., vol 51, 2893-2897, (2015). doi:10.1016/j.procs.2015.05.454.

Fuentes, A., Hernández, L., Martín, A. and Alarcos, B., *"Design of a Set of Software Tools for Side-Channel Attacks", IEEE Latin America Transactions, 13, 6 (2015), 1966–1978. doi:10.1109/TLA.2015.7164224.*

Gayoso Martínez, V., Hernández Encinas, L., Queiruga Dios, A., *"Security and practical considerations when implementing the elliptic curve integrated encryption scheme", Cryptologia, 39 , 3 (2015), 244-269. doi:10.1080/01611194.2014.988363.*

Gayoso Martínez,V., Hernández Álvarez, F., Hernández Encinas, L., Sánchez Ávila, C.*"A new edit distance for fuzzy hashing applications", The 2015 International Conference on Security and Management (SAM'15), Worldcomp 2015, Proc. 326–332, K. Daimi and H.R. Arabnia (Eds.), ISBN 1-60132-412-X, Las Vegas (USA), July 2015.*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A., Álvarez Mariño, M. A.*"A Java Implementation of a Multisignature Scheme", The 2015 International Conference on Security and Management (SAM'15), Worldcomp 2015, Proc. 333–339, K. Daimi and H.R. Arabnia (Eds.), ISBN 1-60132-412-X, Las Vegas (USA), July 2015.*

Cardell, S. D., Fúster-Sabater. A. *"Modelización lineal de generadores basados en decimación". Memorias del VIII Congreso Iberoamericano de Seguridad Informática CIBSI 2015, pp. 102-107. Sesión 4: Criptografía. Sangolqui, Quito, Ecuador, 10–12 Noviembre, 2015, ISBN: 978-9978-301*

Cardell, Sara D., and Fúster-Sabater, Amparo *"A Simple Linearisation of the Self-shrinking Generator", R. Moreno-Díaz, F.Pichler and A. Quesada-Arencibia (Eds.), Computer Aided Systems Theory (EUROCAST 2015), Lecture Notes in Computer Science 9520, 10-17 (2015), doi:10.1007/978-3-319-27340-2_2 2, 8-13 de febrero de 2015, Las Palmas de Gran Canaria.*

Peinado, A., Munilla, J., Fúster-Sabater, A. *"Stream Ciphers Based on DLFSR: A Classification", EUROCAST 2015, 15th International Conference on Computer Aided Systems Theory, Las Palmas de Gran Canaria, 8-13 February, 2015, pp.25-26.*

Hernández Encinas, L., Martín Muñoz, A. *"Ataques a dispositivos físicos", IX Jornadas STIC CCN-CERT, Diciembre 2015.*

Hernández Encinas, L., Martín Muñoz, A. *" Exfiltración por canal lateral. ¿Son las certificaciones la solución?".IX Jornadas STIC CCN-CERT, Diciembre 2015.*

Hernández Encinas, L., Martín Muñoz, A. " Colaboración en Ciberseguridad. Sector Académico Industria / AA.PP. Caso de éxito 3 - CSIC. CYBERCAMP 2015. Madrid.

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A., de Fuentes, J.M., González Manzano, L. *"Cifrado de datos con preservación del formato", Primeras Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), Actas 110-115, ISBN: 978-84-9773-742-5. León, Septiembre 2015.*

Gayoso Martínez, V., and Hernández Encinas, L. *"ECC programming in Java Card", Journal of Information Assurance and Security 10, 1 (2015), 1-8.*

González-Manzano, L., de Fuentes, J. M., Gayoso Martínez, V. *"Aplicación del cifrado con preservación del formato para eventos de ciberseguridad", Primeras Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), Actas 88-89, ISBN: 978-84-9773-742-5. León, Septiembre 2015.*

Hernández Encinas, A., Martín-Vaquero, J., Queiruga-Dios, A., Gayoso Martínez, V. *"Eficient high-order finite difference methods for nonlinear Klein-Gordon equations. I: Variants of the phi-four model and the form-I of the nonlinear Klein–Gordon equation", Nonlinear Analysis: Modelling and Control, 20, 2, 274-290 (2015), http://www.mii.lt/NA/2015/2/9.htm.*

Varios autores *"Informe: Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+I en ciberseguridad", Instituto Nacional de Ciberseguridad, INCIBE, Mayo 2015, 79 pp.*

Hernández Encinas,L., Martín Muñoz,A., Gayoso Martínez,V., Negrillo Espigares, J., Sánchez García, J. I., Castelluccia, C., Bourka, A. *"Online privacy tools for the general public. Towards a methodology for the evaluation of PETs for internet & mobile users", ENISA, December, 2015, 62 pp., https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-tools-for-the-general-*

Janati, Y., Munilla, J., Peinado, A., Ortiz-García, A., Hernández Encinas, L., Durán Díaz, R. *"Universal electronic ticket system to promote tourism at destination by means of progressive bonus without Internet connection", Tourism and Travel Studies II (TORAVEL'15), Proc. 326-332, B. Ercan (Ed.), ISBN 978-605-9207-03-4, Istambul (Turkey), June 2015.*

Hernández Encinas, L., Bae Jun, Young .,and Song, Seok-Zun, *"Codes generated by R0-algebra valued functions", Applied Mathematics Sciences 9, 107 (2105), 5343–5352, http://dx.doi.org/ 10.12988/ams.2015.56443*

Durán Díaz, R., Hernández Encinas, L. and Muñoz Masqué, J., *"Cryptanalysis of two combinatorial public key cryptosystems", Logic Journal of the IGPL 23, 1 (2015), 4–16, https://doi.org/ 10.1093/jigpal/jzu036, (Q4, Mathematics, Applied, F.I. 0.213).*

Fuentes, A., Hernández, L., Martín A., and Alarcos, B., *Breaking Points in Quartic Maps. International Journal of Bifurcation and Chaos, vol. 25, nº 4, pp.1550051-1 a 1550051-100218-ISSN: 0218-1274 (print). 1793-6551 (online). http://dx.doi.org/10.1142/S0218127415500510*

Arroyo Guardeño, D.,Gayoso Martínez, V. , Hernández Encinas, L., Martín Muñoz, A. *"Using Smart Cards for Authenticating in Public Services: A Comparative Study". International Joint Conference CISIS'15- ICEUTE'15. Burgos (Spain). Advances in Intelligent Systems and Computing, vol. 369 (Springer). pp. 437-446. Print ISBN: 978-3-319-19712-8, Online ISBN: 978-3-319-19713-5*

Gayoso Martínez, V., Hernández Encinas, L.,and Song, Seok-Zun *Group signatures in practice, International Workshop on Computational Intelligence in Security for Information Systems (CISIS'15), Proc. International Join Conference CISIS'15 and ICEUTE'15, Advances in Intelligent Systems and Computing 413–423, A. Herrero, B. Baruque, J. Sedano, H. Quintián, E. Corchado (Eds.), Springer, ISBN: 978-3-319-19712-8, Burgos (Spain), July 2015. Core B, https://doi.org/10.1007/ 978-3-319-19713-5_35*

PUBLICACIONES 2014

Fuentes Rodríguez, A.; Hernández Encinas, L.; Martín Muñoz, A. and Alarcos Alcázar, B. *" A toolbox for DPA attacks to smart cards", International Joint Conference SOCO'13-CISIS'13-ICEUTE'13, Proc. 399–408, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A.C.P.L.F. de Carvalho, P. García Bringas, I. Zelinka, H. Quintián, E. Corchado (Eds.), ISBN: 978-3-319-01854-6, Salamanca (Spain), September, 2013. http://link.springer.com/chapter/10.1007\%2F978-3-319-01854-6_41.*

Fúster-Sabater, A. "Generation of Cryptographic Sequences by means of Difference Equations" Applied Mathematics & Information Sciences, vol. 8, no. 2, pp. 475-484, 2014. DOI: 10.12785/amis/080204

Gayoso Martínez, V.; Hernández Encinas, L.; Hernández Encinas, A.; Queiruga Dios, A; " *Disclosure of sensitive information in the virtual learning environment Moodle", International Joint Conference SOCO'13-CISIS'13-ICEUTE'13, Proc. 517–526, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A.C.P.L.F. de Carvalho, P. García Bringas, I. Zelinka, H. Quintián, E. Corchado (Eds.), ISBN: 978-3-319-01854-6, Salamanca (Spain), September, 2013. http://link.springer.com/chapter/10.1007\%2F978-3-319-01854-6_53.*

Fuentes Rodríguez, A.; Hernández Encinas, L.; Martín Muñoz, A. and Alarcos Alcázar, B. *Design of a Set of Software Tools for Side-Channel Attacks. ENIGMA, Brazilian Journal of Information Security and Cryptography, vol.1 nº 1, pp 70-82. ISSN (print) 2358-8693 . DOI: 10.1109/TLA.2015.7164224, http://www.enigmajournal.unb.br/index.php/enigma/article/download/22/15*

Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A., "Securing network communications with TLS and Ipsec. 28th International Conference on Information Technologies (InfoTech-2014). Varna (Bulgaria). Proceedings of the International Conference on Information Technologies. pp 123-131. ISSN: 1314-1023

Kang, Kyung-Tae., Song, Seok Zun., Beasley, LeRoy B., and Hernandez Encinas, Luis.*"Characterizations of Zero-Term Rank Preservers of Matrices over Semirings", KYUNGPOOK Math. J. 54 (2014), 619–627, http://dx.doi.org/10.5666/KMJ.2014.54.4.619.*

Kang, Kyung-Tae., Song, Seok Zun., Beasley, LeRoy B., and Hernandez Encinas, *" Nonnegative integral matrices having generalized inverses", Comm. Korean Math. Soc., 29, 2 (2014), 227–237, http://dx.doi.org/10.4134/CKMS.2014.29.2.227.*

Queiruga-Dios, A., Hernández Encinas, A., Visus Ruíz, I., Hernández Encinas,L.,Gayoso Martínez, V.,and Yuste Martínez, E. *"A learning resource to acquire engineering skills through programming languages", Procedia-Social and Behavioral Sciences 116 (2014), 831–835, http://www. sciencedirect.com/science/article/pii/S1877042814004042*

Gayoso Martínez, V., Hernández Encinas, L., Martín Vaquero, J., Queiruga Dios, A., Pueyo Candil, J. *"A new approach for obtaining the bachelor's degree by technology professionals", Procedia-Social and Behavioral Sciences 116 (2014), 1305–1308, http://www.sciencedirect.com/ science/article/pii/S1877042814003231.*

Gayoso Martínez, V.; Hernández Alvarez, F.; Hernández Encinas, L., *" La transformada de WalshHadamard en la identificación biométrica, XIII Reunión Española de Criptología y Seguridad de la Información (RECSI 2014), Actas 185–189, R. Álvarez, J.J. Climent, F. Ferrández, F.M. Martínez, L. Tortosa, J.F. Vicent, A. Zamora (Eds.), ISBN: 978-84-9717-323-0, Alicante, Septiembre 2014.*

Gayoso Martínez, V.; Hernández Alvarez, F.; Hernández Encinas, L., *" A low-complexity procedure for pupil and iris detection suitable for biometric identification, The 2014 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2014 International Conference on Security and Management (Worldcomp-SAM'14), Proc. 151–157, K. Daimi and H.R. Arabnia (Eds.), ISBN 1-*

PUBLICACIONES RELACIONADAS DESTACADAS

Gayoso Martínez, V.; Hernández Alvarez, F.; Hernández Encinas, L., *"State of the art in similarity preserving hashing functions, The 2014 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2014 International Conference on Security and Management (Worldcomp-SAM'14), Proc. 139–145, K. Daimi and H.R. Arabnia (Eds.), ISBN 1-60132-285-2, Las Vegas (USA), July*

Rodríguez Sánchez, G. Hernández Encinas, A., Hernández Encinas, L., Martín del Rey, A. and Queiruga Dios, A. *Cryptography: optional subject in the degree in computer engineering in information technologies, Frontiers in Mathematics and Science Education Research Conference (FISER'14), Proc. 54–57, Famagusta (Cyprus), May 2014.*

Peinado, A., Munilla, J., Fúster-Sabater, A. *"EPCGen2 Pseudorandom Number Generators: Analysis of J3Gen". Sensors, vol. 14, no. 4, pp. 6500-6515, 2014. DOI:10.3390/s140406500*

Fúster-Sabater, A., *"Linear Solutions for Irregularly Decimated Generators of Cryptographic Sequences". International Journal of Nonlinear Sciences and Numerical Simulation, vol. 15, no. 6, pp. 377-385, 2014. DOI:10.1515/ijnsns-2013-0121 (Impact Factor: 1.545)*

Fúster-Sabater. A. *"Computation of Filtering Functions for Cryptographic Applications". Procedia Computer Science, Elsevier B.V., Vol. 29, pp. 2013-2023, 2014. doi:10.1016/j.procs.2014.05.185.*

Fúster-Sabater, A., Caballero, P., *"Weak Equivalents for Nonlinear Filtering Functions", B. Murgante et al. (Eds.): ICCSA 2014, Part VI, LNCS 8584, pp. 592-602, 2014. ISBN. 978-3-319-09152-5.*

Peinado, A., Munilla, J., Fúster-Sabater, A. "*Improving the Period and Linear Span of the Sequences Generated by DLFSRs", José Gaviria de la Puerta et al. (Eds.): SOCO'14 – CISIS'14 – ICEUTE'14, Advances in Intelligent Systems and Computing, 299, pp. 397-406, 2014. ISBN: 978-3-319-07994-3.*

Fúster, A., Caballero, P. *"Calculando Equivalentes Débiles de Filtrados No Lineales". Rafael Álvarez, Joan Josep Climent, Francisco Ferrández, Francisco M. Martínez, Leandro Tortosa, José Francisco Vicent, Antonio Zamora (Eds): RECSI 2014, pp. 13-18, 2014. ISBN: 978-84-9717-323-0.*

Cardell, S. D., Fúster, A. *"Modelización lineal de los generadores shrinking a través de las leyes 102 y 60". Rafael Álvarez, Joan Josep Climent, Francisco Ferrández, Francisco M. Martínez, Leandro Tortosa, José Francisco Vicent, Antonio Zamora (Eds): RECSI 2014, pp. 7-12, 2014. ISBN: 978-84-9717-323-0.*

Molina, J., Caballero, P., Fúster. A. *"Análisis e Implementación del Generador SNOW 3G Utilizado en las Comunicaciones 4G". Rafael Álvarez, Joan Josep Climent, Francisco Ferrández, Francisco M. Martínez, Leandro Tortosa, José Francisco Vicent, Antonio Zamora (Eds): RECSI 2014, pp. 51-56, 2014. ISBN: 978-84-9717-323-0.*

Peinado, A., Munilla, J., Fúster, A. *"Diseño de cifradores en flujo DLFSR con alta complejidad lineal para implementación hardware". Rafael Álvarez, Joan Josep Climent, Francisco Ferrández, Francisco M. Martínez, Leandro Tortosa, José Francisco Vicent, Antonio Zamora (Eds): RECSI 2014, pp. 63-68, 2014. ISBN: 978-84-9717-323-0.*

Fúster, A., Martín del Rey, A., Rodríguez, G., *"Simulación de la propagación del malware: Modelos continuos vs. modelos discretos". Rafael Álvarez, Joan Josep Climent, Francisco Ferrández, Francisco M. Martínez, Leandro Tortosa, José Francisco Vicent, Antonio Zamora (Eds): pp. 139-144, 2014. ISBN: 978-84-9717-323-0.*

PROYECTOS RELEVANTES

Advancing in cybersecurity technologies. *Entidad financiadora: Consejo Superior de Investigaciones Científicas, Programa i-Link+2019, LINKA20216. Entidades participantes: Instituto de Microelectrónica de Sevilla (IMSE), Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC, Tampere University (Finlandia), University of Michigan. Duración, desde: 30/12/2019 hasta: 31/12/2021. Investigador responsable: P. Brox Jiménez.*
Objetivos: The main objective is to develop, deploy and integrate novel cybersecurity technologies that ensure the integrity, resilience and reliability of ICT systems

P2018/TCS-4566. **Cybersecurity, Network Analysis And Monitoring for the next generation Internet (CYNAMON).** *co-financed with FSE and FEDER European Union funds. Investigador principal: David Arroyo Guardeño. Fecha de comienzo: 01/01/2019. Fecha de finalización: 31/12/2022*
Objetivos: Contribuir a un ciberespacio más seguro en nuestro contexto tecnológico actual y futuro: 1) desarrollando técnicas avanzadas de análisis de datos con un enfoque en dos dominios de aplicación clave: redes sociales y redes de nueva generación, 2) proponiendo mecanismos y herramientas de seguridad para los dispositivos IoT conectados y los servicios de red a los que acceden, y 3) explorando técnicas criptográficas para la seguridad de la información y protección de la privacidad de los usuarios.

Criptosistemas Avanzados y Seguros para la Protección de la Privacidad (CASP2). *Entidad financiadora: CSIC, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 01/10/2018 hasta: 31/12/2020. Investigador responsable: L. Hernández Encinas* **.**
Objetivos: 1) Aportar soluciones a las demandas de la ciberseguridad desarrollando sistemas de cifrado y protocolos criptográficos que permitan garantizar el paradigma CID+3A, 2) Criptoanalizar la seguridad de los sistemas y protocolos criptográficos propuestos y estudiar las fugas de información producidas a través de los canales lateralesy 3) Proponer criptosistemas resistentes a la computación cuántica (quantum resistant), principalmente sistemas basados en retículos, en códigos correctores de errores y en isogenias de curvas elípticas.

TIN2017-84844-C2-1-R. **Criptografía para Optimizar la Privacidad y la CIberSeguridad (COPCIS).** *MINEICO, Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, en el marco del Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016. Investigador principal: Luis Hernández Encinas. Fecha de comienzo: 01/01/2018 Fecha de finalización: 31/12/2020*
Objetivos: 1) aportar soluciones a las demandas de la ciberseguridad desarrollando sistemas de cifrado y protocolos criptográficos para garantizar la CID+3AU de los datos y así como la privacidad de personas y empresas, 2) siseñar generadores de bits pseudoaleatorios para ser utilizados en la generación de claves y en los cifradores en flujo, 3) optimizar protocolos criptográficos para la identificación y autenticación seguras de personas y dispositivos. 4) implementar los algoritmos y las aplicaciones desarrollados, 5) analizar y estudiar las fugas de información producidas a través de los canales laterales, etc.

TIN2014-55325-C2-1R. **Protocolos criptográficos para la ciberseguridad: identificación, autenticación y protección de la información (ProCriCiS).** *Cofunded by the European Union FEDER funds. Investigador principal: Luis Hernández Encinas. Fecha de comienzo: 01/01/2015. Fecha de finalización: 31/12/2017*
Objetivos: 1) dseñar e implementar protocolos y esquemas criptográficos que garanticen la seguridad de la información almacenada y transmitida a través de redes para mejorar la ciberseguridad en el mundo empresarial y en los organismos públicos, 2) implementar las técnicas criptográficas desarrolladas en los dispositivos que llevan a cabo la comunicación a la red (PC, tarjetas, móviles, tabletas, etc.), con el fin de aumentar las medidas de seguridad que protegen tales dispositivo, y 3) estudiar las fugas de información producidas por software dañino y por los ataques por los canales laterales, y proponer medidas que disminuyan estas debilidades.

S2013/ICE-3095-CM . **CIBERSEGURIDAD: datos, información y riesgos (CIBERDINE)**. *Consejería de Educación, Juventud y Deporte, Comunidad de Madrid. Investigador principal: Luis Hernández Encinas. Fecha de inicio: 01/10/2014. Fecha de finalización: 31/12/2018.*
Objetivos: fortalecer nuestras capacidades para prevenir, detectar y responder a ciberataques mediante el desarrollo de técnicas que mejoren el conocimiento de la situación y atiendan una gestión dinámica de amenazas.

CriptoHerramientas para la Internet de las Cosas (CripHIoT). *Entidad financiadora: CSIC, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 01/06/2018 hasta: 30/05/2019. Investigador responsable: A.Martín Muñoz.*
Objetivos: 1) Diseñar e implementar nuevos GPCS, adaptados a las restricciones de la IoT y basados en aplicaciones pseudo-caóticas, 2) Diseñar e implementar cifradores en flujo ligeros basados en GPCS para el cifrado de las señales que intercambian dispositivos IoT y 3) Profundizar en el análisis de la teoría de las aplicaciones caóticas cuando se expresan con precisión finita

NRF-20170929700. **Arctic rank preservers of symmetric matrices and cybersecurity**. *Entidad financiadora: National Science Foundation (NSF) of Korea. Entidades participantes: Jeju University of Korea, Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC. Duración, desde: 20/12/2017 hasta: 19/12/2018. Investigadores responsables: Seok-Zun Song y L. Hernández Encinas.*

Protección de la información en la Nube e Internet de las cosas mediante Generadores de bits pseudoaleatorios criptográficamente seguros (PiNGPS). *Entidad financiadora: CSIC, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 23/11/2015 hasta: 28/02/2017. Investigador responsable: L. Hernández Encinas.*

NRF-2013K2A1A2053670. **Generalized inverse of matrices, linear preserves and applying to the secure identification and authentication in electronic communications.** *Entidad financiadora: National Science Foundation (NSF) of Korea. Entidades participantes: Jeju University of Korea, Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC. Duración, desde: 01/09/2013 hasta: 30/08/2015. Investigadores responsables: Seok-Zun Song y L. Hernández Encinas.*

PROYECTOS RELEVANTES

TIN2011-22668. **Identificación y autenticación segura en comunicaciones electrónicas (IDEASEC-e)**. *Plan Nacional de I+D+i, Ministerio de Ciencia e Innovación. Investigador principal: Luis Hernández Encinas. Fecha de comienzo: 01/01/2012. Fecha de finalización: 31/12/2014.*
Objetivos: mejorar la seguridad para la identificación de las partes y la autenticación de la información en cualquier comunicación. Para ello, 1) se modificarán los protocolos y algoritmos de intercambio de información empleados actualmente, y 2) se diseñarán otros nuevos y mejorar su implementación en dispositivos portátiles (v.gr., tarjetas inteligentes).