MINISTERIO
DE CIENCIA,
INNOVACIÓN
Y UNIVERSIDADES

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

CURRICULUM VITAE

NOMBRE: Luis Hernández Encinas

FECHA: marzo/2025

Número de páginas que contiene: 74

Datos Personales

Apellidos: Hernández Encinas *Nombre:* Luis

Situación profesional actual

Organismo: Consejo Superior de Investigaciones Científicas (CSIC)
Instituto: de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI)
Departamento: Tecnologías de la Información y las Comunicaciones (TIC)
Dirección postal: C/ Serrano 144, 28006, Madrid
Teléfono: 915 618 806 (Ext. 438740), 91 391 69 78 *Correo electrónico:* luis.h.encinas@csic.es

Categoría profesional: Profesor de Investigación *Fecha de inicio:* 12 de septiembre de 2022
Especialidad: Tecnologías Físicas y de la Información
ORCID: 0000-0001-6980-2683, *Web of Science ResearcherID:* K-4649-2014, *Scopus ID:* 57191693382

Situación administrativa: Plantilla *Dedicación:* A tiempo completo

Líneas de Investigación

Especialización (Códigos UNESCO): 1203, 1205, 1206, 3304, 3325.
Líneas de investigación: Criptografía, Criptoanálisis, Protocolos de Firma electrónica y Voto electrónico, Generadores de bits (pseudo)aleatorios, Ciberseguridad, Identificación, Autenticación y Privacidad, Criptobiometría, Autómatas Celulares y Teoría de números.

Formación Académica

Titulación Superior	Centro	Fecha
Licenciado en Ciencias Matemáticas	Universidad de Salamanca	21/10/1980
Grado Licenciado Ciencias Geológicas	Universidad de Salamanca	16/09/1988
Doctor en Ciencias Matemáticas	Universidad de Salamanca	15/06/1992

Actividades anteriores de carácter científico profesional

Puesto	Institución	Fechas
Profesor Agregado de Matemáticas	MEC	10/1980-02/1990
Monitor de Informática (PNTIC)	MEC	1986-1987
Asesor de Matemáticas	MEC	10/1989-02/1990
Profesor Titular de Escuela Universitaria	Universidad de Salamanca	02/1990-08/2000
Científicos Titulares de OPI	CSIC	08/2000-08/2018
Investigadores Científicos de OPI	CSIC	06/08/2018-11/09/2022

Idiomas (R = Regular, B = Bien, C = Correctamente)

Idioma	Habla	Lee	Escribe
Inglés	B	C	B
Francés	R	B	R

Indicadores generales de calidad de la producción científica

Uno de los principales indicadores de la calidad de mi producción científica es que la mayor parte mis artículos científicos de los últimos años han sido publicados en revistas indexadas (Journal Citation Report –JCR– y SCImago Journal & Country Rank –SJR–), 46 de ellos en revistas Q1 y Q2 y todos ellos en las áreas en las que trabajo: Matemáticas (Aplicadas y Aplicaciones interdisciplinares) y Ciencias de la Computación (Sistemas de información, Teoría y métodos). Además, he publicado 14 libros y editado otros 8 (incluyendo actas), he sido editor asociado de la revista Information Sciences (Q1 del JCR), miembro del editorial board de otras revistas y recensor de varias revistas de reconocido prestigio. También son indicadores las numerosas publicaciones en las actas de congresos relevantes tanto internacionales como nacionales. Como resultado, la Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI) me ha evaluado positivamente cinco Tramos de Actividad Investigadora (sexenios: 1993-1998, 1999-2004, 2005-2010, 2011-2016 y 2017-2022), un Tramo de Actividad Investigadora Transferencia de Conocimiento e Innovación (sexenio tecnológico: 2001/2011) y tengo reconocidos los seis Tramos de Méritos Investigadores (quinquenios: (1987-1991), 1992-1996, 1997-2001, 2002-2006, 2007-2011, 2012-2016 y 2017-2021).

Con relación a los índices de impacto en investigación científica, mi índice h en Scopus es 17 y en Google Scholar el índice h es 27, el i10 es 58 y el número de citas es 2.757. He participado en 10 proyectos internacionales y en 24 de plan nacional de I+D+i, de los que he sido el investigador principal en 22 de ellos (7 internacionales). Entre los internacionales destacan SPIRS (H2020) y ORACLE (EIG CONCERT-Japan) y también siguen activos EUROQCI-Spain (Comisión Europea) y GIRLS (Erasmus+). En los nacionales se pueden mencionar EMOCION, firmado con Ilía Sistemas del plan AVANZA. Además, he participado en otros 20 proyectos de planes regionales.

Fui galardonado con el Premio "CCN-2021 a la trayectoria profesional en favor de la Ciberseguridad", del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI); Ministerio de Defensa y condecorado con la "Cruz al Mérito Policial con distintivo blanco", del Ministerio del Interior, 2022.

He sido Profesor de Enseñanza Secundaria (1980-1990) y Profesor Titular de la Universidad de Salamanca (1990-2000). Ya en el CSIC, he sido Científico Titular (2000-2018), Investigador Científico (2018-2022) y actualmente Profesor de Investigación (2022-), además de haber sido el director del Instituto de Tecnologías Físicas y de la Información del CSIC entre 2014 y 2022.

Como indicador en transferencia de tecnología, son destacables las 9 patentes publicadas en colaboración con otros investigadores, 6 de las cuales están licenciadas por Telefónica Investigación y Desarrollo. Otro indicador destacable es el relacionado con mi participación y como responsable de numerosos contratos, tanto con empresas y organismos del sector público, como con empresas privadas. Estos contratos suponen una importante vía tanto de financiación como de devolución a la sociedad del resultado de la investigación realizada. En particular, son de destacar los sucesivos contratos técnicos, desde 2010, en materia de evaluación de la seguridad de productos criptográficos firmados con el Centro Criptológico Nacional (CCN), del Centro Nacional de Inteligencia (CNI); para el análisis de vulnerabilidades en el marco de evaluaciones de seguridad Common Criteria firmado con LGAI, Epoche, Winbond y Lesikar; así como de apoyo tecnológico a otras empresas líderes en seguridad y tecnologías de la Información como EPICOM, Tecnobit, Indra, Ferrovial, Airtel y Visa.

He sido responsable de contratos, en concurrencia competitiva con centros de investigación europeos, en 2014, 2015 y 2016, con la European Union Agency for Cybersecurity (ENISA) relacionados con la seguridad de datos personales, la confiabilidad en herramientas de privacidad para el público en general y la confiabilidad en herramientas de privacidad en línea.

En formación y divulgación, he sido profesor en numerosos cursos de postgrado y en másteres, impartido numerosas conferencias invitadas y dirigido nueve tesis doctorales (actualmente dirijo otras dos). También soy miembro de los Comités de Programa de varios congresos nacionales e internacionales.

Soy Jefe de Seguridad del Servicio de Protección de Información Clasificada nacional del CSIC (JSSP) y Jefe de Seguridad del Servicio Central de Protección de Información Clasificada nacional del CSIC (SCPIC), nombrado por la Presidencia del CSIC (22/12/2019). Soy el representante del CSIC en la Comisión Mixta del Acuerdo Marco CSIC-CNI para la Investigación de vulnerabilidades Criptográficas en el ámbito de la Seguridad de las Tecnologías de la Información (2010-); en la Comisión Mixta del Acuerdo Marco CSIC-INCIBE (Instituto Nacional de Ciberseguridad) para llevar a cabo actividades relacionadas con la investigación científica y el desarrollo tecnológico (2014-); en los Comités Técnicos de UNE CTN320 "Ciberseguridad y protección de datos personales" y CTN71 "Tecnologías Habilitadoras Digitales" (2018-); socio fundador en la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC, http://www.renic.es/es/index.html) (2016-) y patrono de la persona jurídica CSIC en el Patronato de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad (2020-).

Participación en Proyectos de I+D financiados en Convocatorias públicas
(nacionales y/o internacionales)

1. Título: *Seguridad Algebraica y Aplicaciones de la Inteligencia Artificial en la Criptología Actual y Postcuántica (SAIACAP)*. Entidad financiadora: CSIC, 202450E017, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 05/12/2023 hasta: 04/02/2026. Cuantía de la subvención: 199.816,70 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2.

2. Título: *EuroQCI deployment in Spain (EuroQCI-Spain)*. Entidad financiadora: European Comission, Ref: 101109163. Entidades participantes: ICFO (coordinator), UPM, CSIC, Telefónica I+D, Cellnex, Tecnobit, INDRA. Duración, desde: 01/01/2023 hasta: 31/07/2025. Cuantía de la subvención CSIC: 154.905 €. Investigadores participantes: V. Fernández Mármol y L. Hernández Encinas.

3. Título: *Esquemas de Firma Digital para la Criptografía Poscuántica (EFiDiP)*. Entidad financiadora: CSIC, 202250E141, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 01/12/2022 hasta: 30/11/2025. Cuantía de la subvención: 149.668,22 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2.

4. Título: *Generation for Innovation, Resilience, Leadership and Sustainability. The game is on! (GIRLS)*, Programa europeo Erasmus+. Ref: 2022-1-ES01-KA220-HED-000089166. Duración, desde: 01/09/2022 hasta: 31/08/2025. Cuantía de la subvención global: 400.000 €. Cuantía de la subvención CSIC: 41.100 €. Investigador responsable: A. Queiruga Dios. Investigador responsable del CSIC: L. Hernández Encinas. Nº de países participantes: 5 (España, Portugal, Rumanía, Italia y México).

5. Título: *QUantum-based Resistant Architectures and Techniques. Integration QKD+PQC (QURSA)*. Entidad financiadora: MICIIN, Convocatoria 2021 de Proyectos Orientados a la Transición Ecológica y a la Transición Digital, del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023, en el Marco del Plan de Recuperación, Transformación y Resiliencia, Ref: TED2021-130369B-C33. Entidades participantes: CSIC. Duración, desde: 01/12/2022 hasta: 30/11/2024. Cuantía de la subvención: 154.905 €. Investigadores responsables: V. Fernández Mármol y L. Hernández Encinas. Nº de investigadores participantes: 4+6.

6. Título: *Retos de la Seguridad en Entornos Biomédicos*. Entidad financiadora: Universidad de Málaga, Ref: D5-2022_04. Entidades participantes: Universidad de Málaga y CSIC. Duración, desde: 24/05/2022 hasta: 24/05/2024. Cuantía de la subvención: 4.000 €. Investigador responsables A. Peinado Domínguez.

7. Título: *eXplainable AI for disinformation and conspiracy detection during infodemics (XAI-DisInfodemics)*. Entidad financiadora: Agencia Española de Investigación, Prioridad temática: Desinformación, engaños y noticias falsas a través de canales públicos y privados, Ref: PLEC2021-007681. Entidades participantes: Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC, Universidades Politécnica de Valencia, Politécnica de Madrid, de Granada, y de Barcelona, y SYMANTO Spain S.L.U. Duración, desde: 01/12/2021 hasta: 30/11/2024. Cuantía de la subvención: 419.876,50€. Cuantía de la subvención para el ITEFI: 51.578,00 €. Investigador responsable: D. Arroyo Guardeño (ITEFI).

8. Título: *Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS)*. Entidad financiadora: H2020-SU-ICT-2018-2020 (Cybersecurity), Topic: SU-ICT-02-2020, Type of action: RIA, Grant agreement ID: 952622. Entidades participantes: Agencia Estatal Consejo Superior de Investigaciones Científicas (IMSE e ITEFI-CSIC), Tampereen Korkeakoulusaatio SR (TAU), Politecnico di Torino (POLITO), Telefónica Investigación y Desarrollo SA (TID), Commissariat a L'Energie Atomique et aux Energies Alternatives (CEA), Fondazione Links-Leading Innovation & Knowledge for Society (LINKS), NEXT SRL, NEC Laboratories Europe GMBH (NEC), Thales DIS Design Services SAS (THALES). Duración, desde: 01/10/2021 hasta: 30/09/2024. Cuantía de la subvención total: 5.041.091,25 €, cuantía para el CSIC: 930.690,00 €, cuantía para el ITEFI: 261.287 €. Investigadora responsable: P. Brox Jiménez (IMSE).

9. Título: *Protocolos, Mecanismos y Tecnologías Pre y Postcuánticas para la Ciberseguridad y la Privacidad (P2QProMeTe)*. Entidad financiadora: MICIIN, Convocatoria 2020 Proyectos de I+D+i - RTI

Tipo B, Ref: PID2020-112586RB-I00. Entidad financiadora: MCIN/AEI/10.13039/501100011033. Entidades participantes: CSIC, Universidades de Alcalá, Salamanca y Málaga. Duración, desde: 01/09/2021 hasta: 28/02/2025. Cuantía de la subvención CSIC: 101.640 €. Investigadores responsables: A. Martín Muñoz y L. Hernández Encinas. Nº de investigadores participantes: 7+3.

10. Título: *ORACLE: Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to serve Future Connected Societies.* Entidad financiadora: EIG CONCERT-Japan 7th Joint Call ICT for Resilient, Safe and Secure Society. Entidades participantes: Jacobs University Bremen (JUB y coordinador de la parte europea y del proyecto), Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC, The University of ElectroCommunications at Tokyo (UEC y coordinador de la parte japonesa), Scientific and Technological Research Council of Turkey (TÜBITAK), Yokohama National University (YNU), and Tokyo University of Science (TUS). Ref: PCI2020-120691-2. Entidad financiadora: MCIN/AEI/10.13039/501100011033 y Unión Europea NexGenerationEU/PRTR. Duración, desde: 01/04/2021 hasta: 30/03/2024. Cuantía de la subvención CSIC: 120.000 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4.

11. Título: *Técnicas y mecanismos de Ciberseguridad para la Autenticación basados en información Sensorial de Dispositivos Móviles (CASDiM).* Entidad financiadora: CSIC, 202050E304, Programa Intramural Especial. Entidades participantes: CSIC. Duración, desde: 01/02/2021 hasta: 31/01/2024. Cuantía de la subvención: 176.125,73 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2.

12. Título: *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: 01/01/2020 hasta: 31/12/2021. Cuantía de la subvención total: 23.738,00 €. Investigador responsable: P. Brox Jiménez. Nº de investigadores participantes: 18.

13. Título: *Cybersecurity, Network Analysis and Monitoring for the Next Generation Internet (CYNAMON-CM).* Entidad financiadora: Consejería de Educación, Juventud y Deporte, Comunidad de Madrid, P2018/TCS-4566-CM. Entidades participantes: Universidad Carlos III de Madrid, Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC, Universidad Autónoma de Madrid y Universidad Rey Juan Carlos. Duración, desde: 01/01/2019 hasta: 30/04/2023. Cuantía de la subvención total: 885.500,00 €, cuantía para el CSIC: 185.226,00 €. Investigador responsable: D. Arroyo Guardeño. Nº de investigadores participantes: 5.

14. Título: *Criptosistemas Avanzados y Seguros para la Protección de la Privacidad (CASP2).* Entidad financiadora: CSIC, Programa Intramural Especial. 201850E114. Entidades participantes: CSIC. Duración, desde: 01/10/2018 hasta: 31/12/2020. Cuantía de la subvención: 134.000 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2.

15. Título: *Criptografía para Optimizar la Privacidad y la CIberSeguridad (COPCIS).* Entidad financiadora: 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, TIN2017-84844-C2-1-R. Entidades participantes: CSIC, Universidades de Alcalá, Autónoma de Madrid y de Málaga. Duración, desde: 01/01/2018 hasta: 31/12/2020. Cuantía de la subvención: 93.533 €. Investigadores responsables: L. Hernández Encinas y A. Fúster Sabater. Nº de investigadores participantes: 6.

16. Título: *Arctic rank preservers of symmetric matrices and cybersecurity.* Entidad financiadora: National Science Foundation (NSF) of Korea, NRF Joint Research Program, NRF-20170929700. 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. Cuantía de la subvención: ≈20.000 $. Investigadores responsables: Seok-Zun Song y L. Hernández Encinas.

17. Título: *New rules for assessing Mathematical Competencies (Rulεs_M$\alpha\tau$h)*, Programa europeo Erasmus+. Ref: 2017-1-ESO1-KA203-038491. Duración, desde: 01/09/2017 hasta: 31/08/2020. Cuantía de la subvención global: 388.670 €. Cuantía de la subvención CSIC: 36.230 €. Investigador responsable: A. Queiruga Dios. Investigador responsable del CSIC: L. Hernández Encinas. Nº de

países participantes: 8 (España, Bulgaria, Irlanda, Portugal, República Checa, Rumanía, Slovenia y Turquía).

18. Título: *Matemáticas en la Sociedad de la Información*, Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, Acciones de dinamización "Redes de Excelencia" 2015. Duración, desde: 2015 hasta: 2016. Cuantía de la subvención: 30.000 €. Investigador responsable: P. Caballero Gil. Nº de investigadores participantes: 10.

19. Título: *Protocolos criptográficos para la ciberseguridad: identificación, autenticación y protección de la información (ProCriCiS)*. Entidad financiadora: MINECO, 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, TIN2014-55325-C2-1-R. Entidades participantes: CSIC, Universidades de Alcalá y de Málaga. Duración, desde: 01/01/2015 hasta: 31/12/2017. Cuantía de la subvención: 59.500 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 6.

20. Título: *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, 201550E087. Entidades participantes: CSIC. Duración, desde: 23/11/2015 hasta: 28/02/2017. Cuantía de la subvención: 59.200 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2.

21. Título: *Ciberseguridad: Datos, Información y Riesgos (CIBERDINE)*. Entidad financiadora: Consejería de Educación, Juventud y Deporte, Comunidad de Madrid, S2013/ICE-3095-CM. Entidades participantes: Universidad Carlos III de Madrid, Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC y Universidad Autónoma de Madrid. Duración, desde: 01/10/2014 hasta: 31/12/2018. Cuantía de la subvención: 151.742,50 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4.

22. Título: *Diseño y análisis de protocolos para garantizar la confidencialidad, integridad y autenticidad de las imágenes médicas*. Entidad financiadora: Consejería de Sanidad, Junta de Castilla y León. Entidades participantes: Universidad de Salamanca e Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC. Duración, desde: 2014 hasta: 2015. Cuantía de la subvención: 3.182 €. Investigador responsable: A. Martín del Rey.

23. Título: *Sistema universal de promoción turística en destino con bonificaciones progresivas personalizadas a través de dispositivos portátiles sin conexión en la red (SUPPORT)*. Entidad financiadora: Fundación Hergar. Entidades participantes: Universidad de Málaga, Universidad de Alcalá e Instituto de Tecnologías Físicas y de la Información (ITEFI) del CSIC. Duración, desde: 2013 hasta: 2014. Cuantía de la subvención: 4.500 €. Investigador responsable: A. Peinado Domínguez.

24. Título: *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, NRF-2013K2A1A2053670. 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. Cuantía de la subvención: ≈50.000 $. Investigadores responsables: Seok-Zun Song y L. Hernández Encinas.

25. Título: *Identificación y Autenticación Seguras en Comunicaciones electrónicas (IDEASECe)*. Entidad financiadora: Plan Nacional de I+D+i, Ministerio de Ciencia e Innovación, TIN2011-22668. Entidades participantes: CSIC, Universidades de Alcalá, Salamanca y Francisco Vitoria. Duración, desde: 01/01/2012 hasta: 31/12/2014. Cuantía de la subvención: 23.500 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 10.

26. Título: *Identificación electrónica y autenticación en comunicaciones seguras*. Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso". Entidades participantes: Universidad de Salamanca, CSIC, Universidad de Alcalá, Universidad Francisco Vitoria, FS/19-2011. Duración, desde: 01/01/2012 hasta: 31/12/2012. Cuantía de la subvención: 3.500 €. Investigador responsable: A. Queiruga Dios. Nº de investigadores participantes: 10.

27. Título: *Utilización de multifirmas digitales basadas en identidades para la firma de documentos públicos*. Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso". Entidades participantes: Universidad de Salamanca, CSIC, Universidad de Alcalá, FS/7-2010. Duración, desde: 01/01/2011 hasta: 31/12/2011. Cuantía de la subvención: 7.500 €. Investigador responsable: A. Queiruga Dios. Nº de investigadores participantes: 6.

28. Título: *Identificación y autenticación seguras*. Entidad financiadora: Plan Nacional de I+D+i, Ministerio de Ciencia e Innovación, TEC2009-13964-C04-02. Entidades participantes: CSIC. Duración, desde: 01/01/2010 hasta: 31/12/2010. Cuantía de la subvención: 8.470 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 6.

29. Título: *Esquemas de firmas electrónicas para grupos de usuarios*. Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso". Entidades participantes: Universidad de Salamanca, CSIC, Universidad de Alcalá. Duración, desde: 01/01/2010 hasta: 31/12/2010. Cuantía de la subvención: 1.500 €. Investigador responsable: A. Queiruga Dios. Nº de investigadores participantes: 6.

30. Título: *rEconocimiento Mediante Olor Corporal en la Internet del futurO y su securizacióN, EMOCION*. Entidad financiadora: Ministerio de Industria Turismo y Comercio, Subprograma AVANZA I+D (Ingenio 2010), TSI-020100-2009-44. Entidades participantes: CSIC, Universidad Politécnica de Madrid, Universidad Carlos III y empresa Ilía Sistemas SL. Duración, desde: 01/07/2009 hasta: 30/06/2012. Cuantía de la subvención: 112.350 €. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3.

31. Título: *Red temática: Matemáticas en la Sociedad de la Información*. Entidad financiadora: Ministerio de Educación y Ciencia, MTM2008-03268-E/MTM. Entidades participantes: CSIC. y varias universidades españolas. Duración, desde: 01/10/2008 hasta: 30/09/2009. Cuantía de la subvención: 8.000 €. Investigador responsable: J.M. Miret Biosca.

32. Título: *Búsqueda de parámetros que hagan seguro el criptosistema de Chor-Rivest*. Entidad financiadora: Universidad de Salamanca. Entidades participantes: Universidad de Salamanca y CSIC. Duración, desde: 1/07/2008 hasta: 30/07/2009. Cuantía de la subvención: 3.000 €. Investigador responsable: A. Queiruga Dios. Nº de investigadores participantes: 3.

33. Título: *Nuevos protocolos de seguridad y algoritmos criptográficos para la protección de servicios telemáticos*. Entidad financiadora: Plan Nacional de I+D+i, Ministerio de Educación y Ciencia, TSI2007-62657. Entidades participantes: CSIC, Universidades Politécnica de Madrid y de Alcalá. Duración, desde: 01/01/2007 hasta: 31/12/2008. Cuantía de la subvención: 12.100 €. Investigador responsable: F. Montoya Vitini.

34. Título: *Red temática: Matemáticas en la Sociedad de la Información*. Entidad financiadora: Ministerio de Educación y Ciencia, MTM2006-28247-E. Entidades participantes: CSIC. y varias universidades españolas. Duración, desde: 01/10/2007 hasta: 30/09/2008. Cuantía de la subvención: 6.000 €. Investigador responsable: J.M. Miret Biosca.

35. Título: *Preservers of extremes of rank inequalities of matrix sums and products*. Entidad financiadora: Korean Science and Engineering Foundation (KOSEF), F01-2007-000-10047-0, and Consejo Superior de Investigaciones Científicas (CSIC). Entidades participantes: KOSEF, CSIC. Duración, desde: 01/05/2007 hasta: 30/04/2009. Cuantía de la subvención: 18.500 $. Investigadores responsables: Seok-Zun Song y L. Hernández Encinas.

36. Título: *Diseño de protocolos criptográficos basados en autómatas celulares*. Entidad financiadora: Junta de Castilla y León, SA110A06. Entidades participantes: Universidad de Salamanca, CSIC. Universidad de Alcalá. Duración, desde: 2006 hasta: 2009. Cuantía de la subvención: 14.100 €. Investigador responsable: Á. Martín del Rey. Nº de investigadores participantes: 8.

37. Título: *Evaluación de protocolos y algoritmos de seguridad en sistemas de información*. Entidad financiadora: Plan Nacional de I+D+i, SEG2004-02418. Entidades participantes: CSIC, Universidades de Málaga, Politécnica de Madrid y Salamanca. Duración, desde: 2004 hasta: 2007. Cuantía de la subvención: 202.400 €. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 15.

38. Título: *Desarrollo de modelos matemáticos discretos con aplicación a los sistemas de información.* Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso", Universidad de Salamanca, FS/3-2005. Entidades participantes: Universidad de Salamanca, CSIC, Universidad Politécnica de Madrid y Ministerio de Fomento. Duración, desde: 2005 hasta: 2006. Cuantía de la subvención: 4.500 €. Investigador responsable: A. Hernández Encinas. Nº de investigadores participantes: 13.

39. Título: *Diseño de modelos basados en autómatas celulares para el estudio, análisis y control de la propagación de epidemias.* Entidad financiadora: Junta de Castilla y León, SAN/1052/SA29/05. Entidades participantes: Universidad de Salamanca, CSIC, C.S. "Campos Lampreana" (Zamora), Hospital "9 de octubre" (Valencia). Duración, desde: 2005 hasta: 2006. Cuantía de la subvención: 5.989,78 €. Investigador responsable: A. Martín del Rey. Nº de investigadores participantes: 7.

40. Título: *Aplicaciones y simulaciones en Biomedicina de los autómatas celulares.* Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso", Universidad de Salamanca. Entidades participantes: Universidad de Salamanca y CSIC. Duración, desde: 2004 hasta: 2005. Cuantía de la subvención: 1.500 €. Investigador responsable: A. Martín del Rey. Nº de investigadores participantes: 11.

41. Título: *Desarrollo eficiente de un método para el cifrado de imágenes basado en autómatas celulares. Estudio de posibles métodos de criptoanálisis.* Entidad financiadora: Junta de Castilla y León, SA052/03. Entidades participantes: Universidad de Salamanca y CSIC. Duración, desde: 2002 hasta: 2005. Cuantía de la subvención: 18.770 €. Investigador responsable: G. Rodríguez Sánchez. Nº de investigadores participantes: 6.

42. Título: *Modelización y control de problemas medioambientales mediante autómatas celulares.* Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso", Universidad de Salamanca. Entidades participantes: Universidad de Salamanca y CSIC. Duración, desde: 2003 hasta: 2004. Cuantía de la subvención: 7.500 €. Investigador responsable: A. Hernández Encinas. Nº de investigadores participantes: 9.

43. Título: *Gestión de acceso seguro a redes abiertas de recursos distribuidos.* Entidad financiadora: Plan Nacional de I+D, TIC2001-0586. Entidades participantes: CSIC. y Universidad de Málaga. Duración, desde: 2001 hasta: 2004. Cuantía de la subvención: 139.008,09 €. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 8.

44. Título: *Autómatas Celulares: Aplicaciones a la Criptografía.* Entidad financiadora: Fundación "Memoria Samuel Solórzano Barruso", Universidad de Salamanca. Entidades participantes: Universidad de Salamanca y CSIC. Duración, desde: 2001 hasta: 2002. Cuantía de la subvención: 13.612,92 €. Investigador responsable: G. Rodríguez Sánchez. Nº de investigadores participantes: 7.

45. Título: *Estructuras homogéneas Kähler, campos gauge y cálculo de variaciones.* Entidad financiadora: CICYT, P98-0533. Entidades participantes: CSIC, Universidades de Cantabria, Salamanca y Complutense de Madrid. Duración, desde: 1999 hasta: 2002. Cuantía de la subvención: 2.230.000 Pts. Investigador responsable: J. Muñoz Masqué. Nº de investigadores participantes: 5.

46. Título: *Desarrollos hipermedia sobre los procesos de aprendizaje del cálculo aritmético en la enseñanza primaria. Actividades prácticas para los alumnos de Matemáticas y su Didáctica en la titulación de maestro.* Entidad financiadora Junta de Castilla-León, SA04/00. Entidades participantes: Universidad de Salamanca. Duración, desde: 2000 hasta: 2001 Cuantía de la subvención: 713.800 Pts. Investigador responsable: R. López Fernández. Nº de investigadores participantes: 4.

47. Título: *Servicios, redes y sistemas para una Intranet pública regional: aplicación a la teleformación y a la pequeña y mediana empresa.* Entidad financiadora: Plan FEDER, 1FD97-2148-C02-02. Entidades participantes: Universidades de Salamanca y Valladolid. Duración, desde: 1999 hasta: 2001. Cuantía de la subvención: 19.120.000 Pts. Investigador responsable: J. García Carrasco y M. López Coronado.

48. Título: *Construcción de componentes pedagógicos para la enseñanza superior en un espacio virtual.* Entidad financiadora: Junta de Castilla-León. Entidades participantes: Universidad de Salamanca. Duración, desde: 1999 hasta: 2000. Cuantía de la subvención: 650.000 Pts. Investigador responsable: J. García Carrasco.

49. Título: *Infraestructuras de seguridad en Internet e Intranet. Aplicación a redes públicas y corporativas.* Entidad financiadora: Plan Nacional de I+D, TEL98-1020. Entidades participantes: CSIC, Universidades de La Laguna, Málaga, Salamanca y Autónoma de Madrid. Duración, desde: 1998 hasta: 2001. Cuantía de la subvención: 17.457.000 Pts. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 12.

50. Título: *Producción de un CD-ROM para la enseñanza-aprendizaje de las estrategias de resolución de problemas, utilizado como recurso de apoyo hipermedia y dirigido a la formación inicial y permanente de estudiantes y profesorado.* Entidad financiadora: Junta de Castilla y León, SA-19/98. Entidades participantes: Universidad de Salamanca. Duración, desde: 1998 hasta: 1999 Cuantía de la subvención: 1.100.000 Pts. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4.

51. Título: *Estructuras Kahlerianas homogéneas y cálculo de variaciones.* Entidad financiadora: CICYT, PB95-0124. Entidades participantes: CSIC, Universidades de Cantabria y Salamanca. Duración, desde: 1996 hasta: 1999. Cuantía de la subvención: 1.500.000 Pts. Investigador responsable: J. Muñoz Masqué. Nº de investigadores participantes: 5.

52. Título: *Geometría paracompleja y cálculo en variaciones.* Entidad financiadora: Ministerio de Asuntos Exteriores (España) y Ministerio de Enseñanza y Ciencia (Rumanía). Entidades participantes: CSIC, Universidad de Salamanca, Technical University and University of Iasi (Rumanía). Duración, desde: 1996 hasta: 1998. Cuantía de la subvención: No preestablecido. Investigador responsable: J. Muñoz Masqué y Ariel Bejancu. Nº de investigadores participantes: 12.

53. Título: *Sistemas criptográficos de protección de datos para la Red Digital de Servicios Integrados (RDSI).* Entidad financiadora: Plan Nacional de I+D, TIC95-0080. Entidades participantes: CSIC, Universidades de La Laguna y Salamanca, Aeromar Telecomunicaciones. Duración, desde: 1995 hasta: 1998. Cuantía de la subvención: 27.320.000 Pts. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 10.

54. Título: *Estudio sistemático de la distribución de Tierras Raras: Molibdeno, Tántalo, Uranio y Torio, en granitoides y complejos metasedimentarios de Macizo Hespérico.* Entidad financiadora: CICYT. Entidades participantes: Universidad de Salamanca. Duración, desde: 1990 hasta: 1992. Investigador responsable: F. Bea Barredo.

55. Título: *Compilación de una base de datos geoquímicos para el Macizo Ibérico. Aplicaciones al estudio de los granitoides de la cadena.* Entidad financiadora: CICYT. Entidades participantes: Universidad de Salamanca. Duración, desde: 1988 hasta: 1990. Investigador responsable: F. Bea Barredo.

Proyectos Internacionales	10
Proyectos de Planes Nacionales I+D	24
Proyectos de Planes Regionales	21
Subvención ingresada como IP	1.513.074 €

Publicaciones o Documentos Científico-Técnicos[1]

(L = Libro, CL = Capítulo de libro, C = CD, A = Artículo, R = Recensión, E = Editor, S = Doc. científico-técnico)

1. L. Hernández Encinas (S). Guía de Seguridad de las TIC (CCN-STIC-221), "Guía de Mecanismos Criptográficos autorizados por el CCN", para el Centro Criptológico Nacional, noviembre de 2024, 211 pp., https://www.ccn-cert.cni.es/es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6954-ccn-stic-221-guia-de-mecanismos-criptograficos-autorizados-por-el-ccn-1/file?format=html.

2. O. Castillo Campo, V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and R. Álvarez Fernández (A), "Cybersecurity trends in cooperative, connected, and automated mobility", *Logic Journal of the IGPL*, 2024, jzae072, https://doi.org/10.1093/jigpal/jzae072, (Q1, Logic, F.I. 1.0).

3. M. A. González de la Torre, L. Hernández Encinas and J. I. Sánchez García (A), "Structural analysis of Code-based Algorithms of the NIST Post-Quantum Call", *Logic Journal of the IGPL*, 2024, jzae071, https://doi.org/10.1093/jigpal/jzae071 (Q1, Logic, F.I. 1.0).

4. L. Hernández Encinas (S). Píldora CCN-Pytec (CCN-TEC 012) "El estándar de criptografía ligera, ASCON", para el Centro Criptológico Nacional, julio de 2024, 34 pp., https://www.ccn.cni.es/es/docman/documentos-publicos/boletines-pytec/516-ccn-tec-012-el-estandar-de-criptografia-ligera-ascon/file?idU=1.

5. Luis Hernández-Álvarez, Elena Barbierato, Stefano Caputo, José María de Fuentes; Lorena González-Manzano; Luis Hernández Encinas, and Lorenzo Mucchi (A), "Key Encoder: A secure and usable EEG-based cryptographic key generation mechanism", *Pattern Recognition Letters* 173 (2023), 1–9, https://doi.org/10.1016/j.patrec.2023.07.008 (Q2, Computer Science, Artificial Intelligence, F.I. 5.1).

6. L. Hernández Encinas (L), *Manual Básico de Criptología*, Editorial Pinolia, Madrid, 2023, 299 pp. ISBN: 9788418965883, https://almuzaralibros.com/fichalibro.php?libro=6984&edi=9.

7. Luis Hernández-Álvarez, Elena Barbierato, Stefano Caputo, Lorenzo Mucchi, and Luis Hernández Encinas (A), "EEG Authentication System Based on One- and Multi-Class Machine Learning Classifiers", *Sensors* 23(1), 186 (2023), 1–19, Special Issue "Feature Papers in Smart and Intelligent Sensors Systems", https://doi.org/10.3390/s23010186, https://www.mdpi.com/1424-8220/23/1/186 (Q2, Engineering, Electrical & Electronic, F.I. 3.847).

8. L. Hernández Encinas (S). Guía de Seguridad de las TIC (CCN-STIC-221), "Guía de Mecanismos Criptográficos autorizados por el CCN", para el Centro Criptológico Nacional, marzo de 2023, 191 pp., https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6954-ccn-stic-221-guia-de-mecanismos-criptograficos-autorizados-por-el-ccn-1/file.html.

9. L. Hernández Encinas (S). Píldora CCN-Pytec (CCN-TEC 009), "Recomendaciones para una transición postcuántica segura", para el departamento CCN-PYTEC del Centro Criptológico Nacional, diciembre de 2022, 23 pp., https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file.

10. L. Hernández Encinas (S). Guía de Seguridad de las TIC (CCN-STIC-807), "Criptología de empleo en el Esquema Nacional de Seguridad' ', para el Centro Criptológico Nacional, mayo de 2024, 59 pp., https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file?format=html.

11. K. Daimi, G. Francia III and L. Hernández Encinas (E), "Breakthroughs in Digital Biometrics and Forensics", Springer International Publishing, The Netherlands, 2022, 413 pp., ISBN: 978-3-031-10705-4, https://doi.org/10.1007/978-3-031-10706-1, https://link.springer.com/book/10.1007/978-3-031-10706-1

[1] Como es habitual en Matemáticas, los autores se ordenan, en general, alfabéticamente por apellidos: https://www.ams.org/profession/leaders/CultureStatement04.pdf

12. L. Hernández-Álvarez, L. González-Manzano, J.M. Fuentes and L. Hernández Encinas (CL), "Biometrics and Artificial Intelligence: Attacks and Challenges" pp. 213–240 in the book "Breakthroughs in Digital Biometrics and Forensics", Springer, 2022, https://doi.org/10.1007/978-3-031-10706-1_10.

13. M.A. González de la Torre, L. Hernández Encinas, and A. Queiruga-Dios (A), "Analysis of the FO Transformation in the Lattice-Based Post-Quantum Algorithms", *Mathematics* (2022), 10, 16, 2967, https://doi.org/10.3390/math10162967, (Q1, Mathematics, F.I. 2.592).

14. V. Gayoso Martínez, L. Hernández Encinas and A. Martín Muñoz (A), "A modification proposal for the reconciliation mechanism of the key exchange algorithm NewHope", *Logic Journal of the IGPL* (2022), jzac011, https://doi.org/10.1093/jigpal/jzac011, (Q2, Logic, F.I. 0.868).

15. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz and A. Queiruga Dios (A), "Using Free Mathematical Software in Engineering Classes", *Axioms* 10(4), 253 (2021), https://doi.org/10.3390/axioms10040253, http://hdl.handle.net/10261/242692 (Q2, Mathematics Applied, F.I. 1.04).

16. J. Espinosa García, L. Hernández Encinas and A. Peinado Domínguez (A), "A Comprehensive Security Framework Proposal to Contribute to Sustainability", *Sustainability* 13, 6901 (2021), 1–23, https://doi.org/10.3390/su13126901, http://hdl.handle.net/10261/245199 (Q2, Environmental Sciences, Sustainable Science & Technology, F.I. 2.576).

17. L. Hernández Encinas, R. Martínez Martínez, I. Baturone Castillo, V. Fernández Mármol, A. Martín Muñoz, S. Sánchez Solano and L. Terés Terés (CL), "Trust and Security in the Digital Information" pp. 91–109 in the book "Digital & Complex Information", Volume 10 of CSIC Scientific Challenges: Towards 2030, CSIC, Madrid, 2021. http://libros.csic.es/product_info.php?products_id=1523.

18. L. Hernández-Álvarez, J.M. de Fuentes, L. González-Manzano and L. Hernández Encinas (A), "SmartCAMPP - Smartphone-based Continuous Authentication leveraging Motion sensors with Privacy Preservation", *Pattern Recognition Letters* 147 (2021), 189–196, Special Issue "Implicit Biometric Authentication and Monitoring through Internet of Things", https://doi.org/10.1016/j.patrec.2021.04.013, http://hdl.handle.net/10261/241628 (Q2, Computer Science, Artificial Intelligence, F.I. 4.757).

19. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), "Quadratic Maps in Two Variables on Arbitrary Fields", *Carpathian J. Math.* 37, 1 (2021), 91–100, https://doi.org/10.37193/CJM.2021.01.09, http://hdl.handle.net/10261/239454 (Q2, Mathematics, F.I. 1.438).

20. L. Hernández-Álvarez, J.M. de Fuentes, L. González-Manzano and L. Hernández Encinas (A), "Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review", *Sensors*, 21(1), 92 (2021), 23 pp., Special Issue "Cryptography and Information Security in Wireless Sensor Networks", https://doi.org/10.3390/s21010092, http://hdl.handle.net/10261/225771 (Q1, Instruments & Instrumentation, F.I. 3.275).

21. D. Arroyo Guardeño, V. Gayoso Martínez y L. Hernández Encinas (L), *Ciberseguridad*, Colección: ¿Qué sabemos de?, 119, Editorial CSIC-Catarata, Madrid, 2020, 144 pp. ISBN: 978-84-1352-119-0, https://www.catarata.org/libro/ciberseguridad_117356/.

22. V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz (CL) "Limits and apparent paradoxes in economics and engineering", in "Calculus for Engineering Students. Fundamentals, Real Problems, and Computers". J. Martín-Vaquero, M. Carr, A. Queiruga-Dios, and D. Richtáriková (Eds.), Academic Press-Elsevier, Mathematics in Science and Engineering, 1–14 (2020), ISBN: 9780128172100 (paper), 9780128172117 (ebook), https://doi.org/10.1016/B978-0-12-817210-0.00008-4, https://doi.org/10.1016/C2018-0-00422-3

23. I. Querejeta-Azurmendi, D. Arroyo Guardeño, J.L. Hernández-Ardieta, and L. Hernández Encinas (A), "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", https://doi.org/10.3390/math8091618, http://hdl.handle.net/10261/220321 (Q1, Mathematics, F.I. 1.747).

24. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and R. Durán Díaz (A), "Using the Spanish national identity card in social networks", *Logic Journal of the IGPL* 28, 4 (2020), 519–530 (accepted December 2019), https://doi.org/10.1093/jigpal/jzz058, http://hdl.handle.net/10261/237424 (Q1, Logic, F.I. 0.861).

25. L. Hernández Encinas (E), Special Issue "Mathematics Cryptography and Information Security" of the Journal "Mathematics (Basel)" (MDPI, Q1, I.F. 1.747), February 26–December 31, https://www.mdpi.com/journal/mathematics/special_issues/Mathematics_Cryptography_Information_Security.

26. L. Hernández Encinas (E), Special Issue "Cryptography and Information Security in Wireless Sensor Networks" of the Journal "Sensors" (MDPI, Q1, I.F. 3.275), https://www.mdpi.com/journal/sensors/special_issues/Cryptography_Information_Security.

27. R. Durán Díaz, V. Gayoso Martínez, L. Hernández Encinas and J. Muñoz Masqué (A), "Square-Zero Basis of Matrix Lie Algebras", *Mathematics*, 8(6), 1032 (2020), 9 pp., Special Issue "Algebra and Its Applications", https://doi.org/10.3390/math8061032, http://hdl.handle.net/10261/238158 (Q1, Mathematics, F.I. 1.747).

28. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), "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", https://doi.org/10.3390/math8050734, http://hdl.handle.net/10261/212504 (Q1, Mathematics, F.I. 1.747).

29. V. Gayoso Martínez, F. Hernández-Álvarez and L. Hernández Encinas (A), "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", https://doi.org/10.3390/math8040503, http://hdl.handle.net/10261/209461 (Q1, Mathematics, F.I. 1.747).

30. V. Gayoso Martínez, L. Hernández-Álvarez and L. Hernández Encinas (A), "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", https://doi.org/10.3390/math8010131, http://hdl.handle.net/10261/238233 (Q1, Mathematics, F.I. 1.747).

31. H. Rodriguez Cesar, V. Gayoso Martinez, L. Hernandez Encinas, A. Martin Munoz (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, http://hdl.handle.net/10261/239311.

32. Leroy B. Beasley, Luis Hernandez Encinas, and Seok-Zun Song (A), "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, (Q3, Mathematics, Applied, F.I. 0.63).

33. M. Conde Pena, R. Durán Díaz, J.-C. Faugère, L. Hernández Encinas, and L. Perret (A), "Non-quantum Cryptanalysis of the Noisy Version of Aaronson-Christiano's Quantum Money Scheme", *IET Information Security*, 13, 4 (2019), 362–366, https://doi.org/10.1049/iet-ifs.2018.5307, (Q3, Computer Science, Theory & Methods, F.I. 01.068).

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

35. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and O. Martínez-Graullera (A), "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), https://doi.org/10.1093/jigpal/jzy031, (Q1, Logic, F.I. 0.931).

36. V. Gayoso Martínez, L. Hernández Encinas; A. Martín Muñoz; R. Durán Díaz (A), "Secure elliptic curves and their performance" *Logic Journal of the IGPL*, 27, 2 (2019), 277–238 (on-line: 2018 Sep 17), https://doi.org/10.1093/jigpal/jzy035, (Q4, Mathematics, Applied, F.I. 0.449).

37. A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz, and B. Alarcos Alcázar (A), "A Modular and Optimized Toolbox for Side-Channel Analysis", *IEEE Access* 7 (2019), 21889–21903, https://ieeexplore.ieee.org/document/8636501, http://doi.org/10.1109/ACCESS.2019.2897938, (Q1, Computer Science, Information Systems, F.I. 3.745).

38. V. Gayoso Martínez, L. Hernández Encinas y A. Martín Muñoz (L), "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), http://editorial.csic.es/publicaciones/libros/13133/0/criptografia-con-curvas-elipticas.html.

39. L. Hernández Encinas y M. González Hernández (E), "75 años al servicio de las Tecnologías Físicas y de la Información en el Torres Quevedo", Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI), 2018, 261 pp., ISBN: 978-84-09-06956-9, http://www.itefi.csic.es/content/libro-75-aniversario-torres-quevedo.pdf.

40. M. Romera, G. Pastor, M.-F. Danca, A. Martin, A. B. Orue, F. Montoya, L. Hernández Encinas and E. Tundrea (A), "Bifurcation Diagram of a Map with Multiple Critical Points", *International Journal of Bifurcation and Chaos* 28, 05, 1850065 (2018), https://doi.org/10.1142/S0218127418500657, https://www.worldscientific.com/toc/ijbc/28/05, (Q2, Mathematics, Interdisciplinary Applications, F.I. 2.145).

41. L. Hernández Encinas and A. Martín del Rey (A), "Boolean differential operators", *Turkish Journal of Mathematics* **42** 57–68 (2018), http://journals.tubitak.gov.tr/math/issues/mat-18-42-1/mat-42-1-7-1607-22.pdf, https:/doi.org/10.3906/mat-1607-22, (Q3, Mathematics, F.I. 0.597).

42. J.M. de Fuentes, L. Hernández Encinas, and A. Ribagorda (CL), "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, https://doi.org/10.1007/978-3-319-58424-9_8

43. A. Sánchez-Gómez, J. Diaz, L. Hernández Encinas, and D. Arroyo (CL), "Review of the Main Security Threats 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, https://doi.org/10.1007/978-3-319-58424-9_15

44. K. Daimi, G. Francia, L. Ertaul, L. Hernández Encinas, and E. El-SheikhP (E), "Computer and Network Security Essentials", Springer International Publishing, The Netherlands, 2018, 618 pp., ISBN: 978-3-319-58423-2, http://doi.org/10.1007/978-3-319-58424-9, http://www.springer.com/in/book/9783319584232

45. A. B. Orúe, L. Hernández-Encinas, A. Martín and F. Montoya (A), "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, (Q1, Computer Science, Information Systems, F.I. 3.557).

46. R. Durán Díaz, L. Hernández Encinas, A. Martín Muñoz, J. Muñoz Masqué, 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, (Q3, Mathematics, F.I. 0.614).

47. M. Mojica López, J.L. Luis Rodrigo Oliva, V. Gayoso Martínez, L. Hernández Encinas and A. Martín Muñoz (A), "Análisis de la Privacidad de WhatsApp Messenger", *Revista Iberoamericana de Sistemas, Cibernética e Informática*, **14**, 2, 73–78 (2017), http://www.iiisci.org/Journal/riSCI/Contents.asp?var=&next=ISS1402

48. A. Martin del Rey, J.D. Hernández Guillén, Luis Hernández Encinas (A), "Study of the stability of a SEIRS model for computer worm propagation", *Physica A - Statistical Mechanics and its Applications*, **479**, 411–421 (2017), http://doi.org/10.1016/j.physa.2017.03.023, (Q2, Physics, Multidisciplinary, F.I. 2.132).

49. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, M.A. Álvarez Mariño, and D. Arroyo Guardeño (A), "A comparative study of three Spanish eGoverment smart cards", *Logic Journal of the IGPL*, **25**, 1 (2017), 42–53, https://doi.org/10.1093/jigpal/jzw038, (Q3, Logic, F.I. 0.575).

50. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and R. Durán Díaz (A), "A Proposal for Using a Cryptographic National Identity Card in Social Networks", *Advances in Intelligent Systems and Computing*, **649**, 651–660 (2017), https://doi.org/10.1007/978-3-319-67180-2_63

51. J.D. Hernández Guillén, A. Martín del Rey, L. Hernández Encinas (A), "New Approaches of Epidemic Models to Simulate Malware Propagation", *Advances in Intelligent Systems and Computing*, **649**, 631–640 (2017), https://doi.org/10.1007/978-3-319-67180-2_61

52. A. Beatriz Orúe, L. Hernández Encinas, V. Fernández, F. Montoya (A), "A Review of Cryptographically Secure PRNGs in Constrained Devices for the IoT", *Advances in Intelligent Systems and Computing*, **649**, 672–682 (2017), https://doi.org/10.1007/978-3-319-67180-2_65

53. R. Durán Díaz and L. Hernández Encinas (CL), "Special Primes: Properties and Applications", Chapter of the book "Geometry, Algebra and Applications: From Mechanics to Cryptography", Springer International Publishing Switzerland, 2016, 79–90, ISBN: 978-3-319-32084-7, https://doi.org/10.1007/978-3-319-32085-4_7

54. V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz (CL), "Implementation of Cryptographic Algorithms for Elliptic Curves", Chapter of the book "Geometry, Algebra and Applications: From Mechanics to Cryptography", Springer International Publishing Switzerland, 2016, 121–133, ISBN: 978-3-319-32084-7, https://doi.org/10.1007/978-3-319-32085-4_11

55. M. Castrillón López, L. Hernández Encinas, P. Martínez Gadea, and M.E. Rosado María (E), "Geometry, Algebra and Applications: From Mechanics to Cryptography", Springer International Publishing Switzerland, 2016, 181-187, ISBN: 978-3-319-32084-7 (Print) 978-3-319-32085-4 (Online), https://doi.org/10.1007/978-3-319-32085-4

56. L. González-Manzano, José M. de Fuentes, Sergio Pastrana, Pedro Peris-Lopez, and Luis Hernández-Encinas (A), "PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things", *Journal of Network and Computer Applications*, 71 (2016), 59–71, https://doi.org/10.1016/j.jnca.2016.06.001, (Q1, Computer Science, Software Engineering, F.I. 2.229).

57. L. Hernández Encinas (L), *La Criptografía*, Colección: ¿Qué sabemos de?, Editorial CSIC-Catarata, 69, Madrid, 2016, 142 pp. ISBN: 978-84-00-10045-2, https://www.catarata.org/libro/la-criptografia_46013/.

58. G. Pastor, M. Romera, M.-F. Danca, A. Martin, A.B. Orue, F. Montoya, and L. Hernández Encinas (A), "Hidden and non-standard bifurcation diagram of an alternate quadratic system", *International Journal of Bifurcation and Chaos* **26**, 2 (2016) 1550036 (14 pages), https://doi.org/10.1142/S021812741650036X, (Q2, Mathematics, Interdisciplinary Applications, F.I. 1.355).

59. A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz, and B. Alarcos Alcázar (A), "Design and Optimization of the Input Modules of a DPA Toolbox", *Logic Journal of the IGPL* **24**, 1 (2016), 16–28 https://doi.org/10.1093/jigpal/jzv041, (Q3, Logic, F.I. 0.575).

60. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, O. Martínez-Graullera, and J. Villazón-Terrazas (A), "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

61. A. Queiruga-Dios, A. Hernández Encinas, J. Martín-Vaquero, and L. Hernández Encinas (A), "Malware Propagation Models in Wireless Sensor Networks: A Review", *Advances in Intelligent Systems and Computing*, **527**, 648–657 (2016), https://doi.org/10.1007/978-3-319-47364-2_63

62. R. Durán Díaz, V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz (A), "A study on the performance of secure elliptic curves for cryptographic purposes", *Advances in Intelligent Systems and Computing*, **527**, 658–667 (2016), https://doi.org/10.1007/978-3-319-47364-2_64

63. L. Hernández Encinas, A. Martín Muñoz, V. Fernández Mármol, V. Gayoso Martínez, J.I. Sánchez García, C. Castelluccia, and A. Bourka (S), *PETs controls matrix. A systematic approach for assessing online and mobile privacy tools*, ENISA, December, 2016, 62 pp., https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools

64. L. Hernández Encinas y J. Espinosa García (A), "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

65. L. Hernández Encinas y J. Espinosa García (A), "Claves para la gestión de la seguridad integral", *Seguritecnia*, 01/06/2016, 50–52, http://www.seguritecnia.es/revistas/seg/432/index.html?#50

66. L. Hernández Encinas y J. Espinosa García (A), "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/

67. L. Hernández Encinas, A. Martín Muñoz, V. Gayoso Martínez, J. Negrillo Espigares, J.I. Sánchez García, C. Castelluccia, and A. Bourka (S), *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-public

68. L. Hernández Encinas, Young Bae Jun and Seok-Zun Song (A), "Codes generated by R_0-algebra valued functions", *Applied Mathematics Sciences* **9**, 107 (2105), 5343–5352, http://dx.doi.org/10.12988/ams.2015.56443

69. A. Fuentes, L. Hernández, A. Martín and B. Alarcos (A), "Design of a Set of Software Tools for Side-Channel Attacks", *IEEE Latin America Transactions* **13**, 6 (2015), 1966–1978, https://doi.org/10.1109/TLA.2015.7164224, (Q4, Computer Science, Information Systems, F.I. 0.436).

70. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué (A), "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).

71. V. Gayoso Martínez, L. Hernández Encinas, and A. Queiruga Dios (A), "Security and practical considerations when implementing the elliptic curve integrated encryption scheme", *Cryptologia* **39**, 3 (2015), 244–269. https://doi.org/10.1080/01611194.2014.988363, (Q4, Mathematics, Applied, F.I. 0.213).

72. V. Gayoso Martínez and L. Hernández Encinas (A), "ECC programming in Java Card", *Journal of Information Assurance and Security* **10**, 1 (2015), 1–8, https://docplayer.net/44897523-Ecc-programming-in-java-card.html.

73. Varios autores (S), *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.

74. Kyung-Tae Kang, Seok Zun Song, LeRoy B. Beasley, and Luis Hernandez Encinas (A), "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.

75. Kyung-Tae Kang, Seok Zun Song, LeRoy B. Beasley, and Luis Hernandez Encinas (A), "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.

76. A. Queiruga-Dios, A. Hernández Encinas, I. Visus Ruíz, L. Hernández Encinas, V. Gayoso Martínez, and E. Yuste Martínez (A), "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

77. V. Gayoso Martínez, L. Hernández Encinas, J. Martín Vaquero, A. Queiruga Dios, J. Pueyo Candil (A), "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.

78. L. Hernández Encinas (R), B Justus, Benjamin The distribution of quadratic residues and non-residues in the Goldwasser-Micali type of cryptosystem. J. Math. Cryptol. 8 (2014), no. 2, 115–140, MR3213578, 2013.

79. V. Gayoso Martínez, L. Hernández Encinas, A. Hernández Encinas, and A. Queiruga Dios (A), Avoiding Sensitive Information Leakage in Moodle, *Literacy Information and Computer Education* **2**, 2 (2013), 1331–1341, http://www.infonomics-society.org/LICEJ/Publishedpapers.htm.

80. V. Gayoso Martínez and L. Hernández Encinas (A), Implementing ECC with Java Standard Edition 7, *International Journal of Computer Science and Artificial Intelligence* **3**, 4 (2013), 134–142, http://www.jcsai.org/paperInfo.aspx?PaperID=14496.

81. V. Gayoso Martínez, L. Hernández Encinas and A. Martín Muñoz (A), A comparative analysis of hybrid encryption schemes based on elliptic curves, *The Open Mathematics Journal* **6** (2013), 1–8, http://www.benthamscience.com/open/tomatj/openaccess2.htm.

82. A. Hernández Encinas, A. Queiruga Dios, L. Hernández Encinas and V. Gayoso Martínez, Statistical analysis from time series related to climate data (A), *International Journal of Applied Mathematics and Physics* **3**, 3 (2013), 203–207, http://www.ijapm.org/papers/206-D0070.pdf.

83. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué (A), Comments on a cryptosystem proposed by Wang and Hu, *Advances in Intelligent Systems and Computing* **189** (2013), 57–65, http://dx.doi.org/10.1007/978-3-642-33018-6_6.

84. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué (A), Fractal sets attached to homogeneous quadratic maps in two variables, *Physica D-Nonlinear Phenomena* **245**, 1 (2013), 8–18, http://dx.doi.org/10.1016/j.physd.2012.11.002, (Q1, Mathematics, Applied, F.I. 1.829).

85. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), Two proposals for group signature schemes based on number theory problems, *Logic Journal of the IGPL* **21**, 4 (2013), 648–658, http://dx.doi.org/10.1093/jigpal/jzs035, (Q1, Logic, F.I. 0.530).

86. L. Hernández Encinas (R), Bulygin, Stanislav; Walter, Michael; Buchmann, Johannes Many weak keys for PRINTcipher: fast key recovery and countermeasures. Topics in cryptology-CT-RSA 2013, 189–206, Lecture Notes Comput. Sci., 7779, Springer, Heidelberg, 2013, MR3082016, 2013.

87. A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini y J. Muñoz Masqué (L), *Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales*, RA-MA, Madrid, 2012, 364 pp. ISBN: 978-84-9964-136-2, https://www.ra-ma.es/libro/criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para-estudiantes-y-profesionales_48492/.

88. R. Álvarez Mariño, F. Hernández Álvarez and L. Hernández Encinas (A), A crypto-biometric scheme based on iris-templates with fuzzy extractors, *Information Sciences* **195** (2012), 91–102, http://dx.doi.org/10.1016/j.ins.2012.01.042, (Q1, Computer Science, Information Systems, F.I. 3.643).

89. L. Hernández Encinas (R), Hofheinz, Dennis; Kiltz, Eike Programmable hash functions and their applications. J. Cryptology 25 (2012), no. 3, 484–527, MR2900409, 2012.

90. L. Hernández Encinas (R), Boldyreva, Alexandra; Palacio, Adriana; Warinschi, Bogdan Secure proxy signature schemes for delegation of signing rights. J. Cryptology 25 (2012), no. 1, 57–115, MR2875130, 2012.

91. L. Hernández Encinas (R), Seo, Seung-Hyun; Choi, Kyu Young; Hwang, Jung Yeon; Kim, Seungjoo Efficient certificateless proxy signature scheme with provable security. Inform. Sci. 188 (2012), 322–337, MR2873680, 2012.

92. L. Hernández Encinas (R), Hambleton, S.; Scharaschkin, V. Pell conics and quadratic reciprocity. Rocky Mountain J. Math. 42 (2012), no. 1, 91–96, MR2876270,2012.

93. L. Hernández Encinas (R), Goldreich, Oded The GGM construction does not yield correlation intractable function ensembles. Studies in complexity and cryptography, 98–108, Lecture Notes Comput. Sci., 6650, Springer, Heidelberg, 2011, MR2844256, 2012.

94. L. Hernández Encinas (R), Armknecht, Frederik; Furukawa, Jun On the minimum communication effort for secure group key exchange. Selected areas in cryptography, 320–337, Lecture Notes Comput. Sci., 6544, Springer, Heidelberg, 2011, MR2804484, 2012.

95. L. Hernández Encinas (R), Xing, DongSheng; Cao, ZhenFu; Dong, XiaoLei Identity based signature scheme based on cubic residues. Sci. China Inf. Sci. 54 (2011), no. 10, 2001–2012, MR2837336, 2012.

96. L. Hernández Encinas (R), Attrapadung, Nuttapong; Libert, Benoît Functional encryption for public-attribute inner products: achieving constant-size ciphertexts with adaptive security or support for negation. J. Math. Cryptol. 5 (2011), no. 2, 115–158, MR2838372, 2012.

97. L. Hernández Encinas (R), Zhu, Yan; Hu, Hong-Xin; Ahn, Gail-Joon; Wang, Huai-Xi; Wang, Shan-Biao Provably secure role-based encryption with revocation mechanism. J. Comput. Sci. Tech. 26 (2011), no. 4, 697–710, MR2849384, 2012.

98. L. Hernández Encinas (R), Abdalla, Michel; Birkett, James; Catalano, Dario; Dent, Alexander W.; Malone-Lee, John; Neven, Gregory; Schuldt, Jacob C. N.; Smart, Nigel P. Wildcarded identity-based encryption. J. Cryptology 24 (2011), no. 1, 42–82, MR2755162, 2012.

99. L. Hernández Encinas (R), Chatterjee, Sanjit; Hankerson, Darrel; Menezes, Alfred On the efficiency and security of pairing-based protocols in the Type 1 and Type 4 settings. Arithmetic of finite fields, 114–134, Lecture Notes Comput. Sci., 6087, Springer, Berlin, 2010, MR2674219, 2012.

100. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), A multisignature scheme based on the SDLP and on the IFP, *Lecture Notes in Computer Science* **6694** (2011), 135–142.

101. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), A group signature scheme based on the integer factorization and the subgroup discrete logarithm problems, *Lecture Notes in Computer Science* **6694** (2011), 143–150.

102. V. Gayoso Martínez, L. Hernández Encinas and C. Sánchez Ávila (A), Java Card implementation of the Elliptic Curve Integrated Encryption Scheme using prime and binary finite fields, *Lecture Notes in Computer Science* **6694** (2011), 160–167.

103. L. Hernández Encinas (CL), Protocolo de reparto de secretos, Lección 8, Enciclopedia de la Seguridad de la Información (Intypedia), `http://www.intypedia.com/`, Criptored, Junio, 2011.

104. V. Gayoso Martínez, F. Hernández Álvarez, L. Hernández Encinas, and C. Sánchez Ávila (A), Analysis of ECIES and other cryptosystems based on elliptic curves, *Journal of Information Assurance and Security* **6**, 4 (2011), 285–293.

105. L. Hernández Encinas (S). Guía de Seguridad de las TIC (CCN-STIC-807), "Criptología de Empleo en el Esquema Nacional de Seguridad", para el Centro Criptológico Nacional, marzo de 2011, 59 pp, `https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html`.

106. L. Hernández Encinas (R), Katz, Jonathan Digital signatures. Springer, New York, 2010. xiv+192 pp. ISBN: 978-0-387-27711-0, MR2723933, 2011.

107. L. Hernández Encinas (R), Goldreich, Oded A primer on pseudorandom generators. University Lecture Series, 55. American Mathematical Society, Providence, RI, 2010. x+114 pp. ISBN: 978-0-8218-5192-0, MR2677397, 2011

108. L. Hernández Encinas (R), Feng, DengGuo; Chen, WeiDong Security model and modular design of fair authentication key exchange protocols. Sci. China Inf. Sci. 53 (2010), no. 2, 278–287, MR2671662, 2011.

109. L. Hernández Encinas (R), Liu, JingWei; Sun, Rong; Kwak, KyungSup Fair exchange signature schemes. Sci. China Inf. Sci. 53 (2010), no. 5, 945–953, MR2671432, 2011.

110. L. Hernández Encinas (R), Xu, Peng; Cui, GuoHua; Fu, Cai; Tang, XueMing A more efficient accountable authority IBE scheme under the DL assumption. Sci. China Inf. Sci. 53 (2010), no. 3, 581–592, MR2671401, 2011.

111. L. Hernández Encinas (R), Lin, Dai-Rui; Wang, Chih-I; Zhang, Zhi-Kai; Guan, D. J. A digital signature with multiple subliminal channels and its applications. Comput. Math. Appl. 60 (2010), MR2653917, 2011.

112. L. Hernández Encinas (R), Schinzel, Andrzej; Spiez, Stanislaw; Urbanowicz, Jerzy Elementary symmetric polynomials in Shamir's scheme. J. Number Theory 130 (2010), no. 7, 1572–1580, MR2645239, 2011.

113. L. Hernández Encinas (R), Fredricksen, H.; Ionascu, E. J.; Luca, F.; Stanica, P. Remarks on a sequence of minimal Niven numbers. Sequences, subsequences, and consequences, 162–168, Lecture Notes Comput. Sci., 4893, Springer, Berlin, 2007, MR2629557, 2011.

114. L. Hernández Encinas (R), Blackburn, Simon R.; Cid, Carlos; Mullan, Ciaran Cryptanalysis of the MST3 public key cryptosystem. J. Math. Cryptol. 3 (2009), no. 4, 321–338, MR2608599, 2011.

115. L. Hernández Encinas (R), Shin, SeongHan; Kobara, Kazukuni; Imai, Hideki Very-efficient anonymous password-authenticated key exchange and its extensions. Applied algebra, algebraic algorithms, and error-correcting codes, 149–158, Lecture Notes Comput. Sci., 5527, Springer, Berlin, 2009, MR2580863, 2011.

116. A.B. Orue, F. Montoya, and L. Hernández (A), Trifork, a new pseudorandom number generator based on lagged Fibonacci maps, *Journal of Computer Science & Engineering* **2**, 2 (2010), 46–51.

117. V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila (A), A survey of the elliptic curve integrated encryption scheme, *Journal of Computer Science & Engineering* **2**, 2 (2010), 7–13.

118. Seok-Zun Song, Kwon-Ryong Park, and L. Hernández Encinas (A), Extreme preservers of maximal column rank inequalities of matrix multiplications over semirings, *Journal of the Korean Mathematical Society* **47**, 1 (2010), 71–81, (Q4, Mathematics, Applied, F.I. 0.374).

119. J.M. Chamoso Sánchez, L. Hernández Encinas y J. Orrantia Rodríguez (A), Análisis de una experiencia de resolución de problemas de matemáticas en secundaria, *Revista de Educación* **351** (2010), 557–570, (Q3, Education & Educational Research, F.I. 0.622).

120. L. Hernández Encinas (R), Zhang, Shaohua Generalizations of theorem about the binomial coefficient. JP J. Algebra Number Theory Appl. 14 (2009), no. 2, 177–184, MR2583406, 2010.

121. L. Hernández Encinas (R), Fouque, Pierre-Alain; Macario-Rat, Gilles; Perret, Ludovic; Stern, Jacques Total break of the ll-IC signature scheme. Public key cryptography-PKC 2008, 1–17, Lecture Notes Comput. Sci., 4939, Springer, Berlin, 2008, MR2570219, 2010.

122. L. Hernández Encinas (R), Coronado García, Luis Carlos Improvements to the Merkle signature scheme. Tatra Mt. Math. Publ. 37 (2007), 1–21, MR2553403, 2010.

123. L. Hernández Encinas (R), Chamberland, Marc; Dilcher, Karl A binomial sum related to Wolstenholme's theorem. J. Number Theory 129 (2009), no. 11, 2659–2672, MR2549522, 2010.

124. L. Hernández Encinas (R), won, Jeong Ok; Jeong, Ik Rae; Lee, Dong Hoon Light-weight key exchange with different passwords in the standard model. J.UCS 15 (2009), no. 5, 1042–1064, MR2511861, 2010.

125. L. Hernández Encinas (R), Lindell, Yehuda; Pinkas, Benny A proof of security of Yao's protocol for two-party computation. J. Cryptology 22 (2009), no. 2, 161–188, MR2496388, 2010.

126. L. Hernández Encinas (R), Bellare, Mihir; Namprempre, Chanathip; Neven, Gregory Security proofs for identity-based identification and signature schemes. J. Cryptology 22 (2009), no. 1, 1–61, MR2496382, 2010.

127. L. Hernández Encinas (R), Liu, Huaning; Zhan, Tao; Wang, Xiaoyun On the correlation of pseudo-random binary sequences with composite moduli. Publ. Math. Debrecen 74 (2009), no. 1-2, 195–214, MR2490431, 2010.

128. L. Hernández Encinas (R), Susilo, Willy Short fail-stop signature scheme based on factorization and discrete logarithm assumptions. Theoret. Comput. Sci. 410 (2009), no. 8-10, 736–744, MR2492012, 2010.

129. L. Hernández Encinas (R), Chevalier, Yannick; Kourjieh, Mounira Key substitution in the symbolic analysis of cryptographic protocols. FSTTCS 2007: Foundations of software technology and theoretical computer science, 121–132, Lecture Notes Comput. Sci., 4855, Springer, Berlin, 2007, MR2480195, 2010.

130. V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila (A), Elliptic curve cryptography. Java platform implementations, *International Journal of Information Technology & Security* **4** (2009), 65–72.

131. Seok-Zun Song, R. Durán Díaz, L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios (A), Dimension of the intersection of a pair of orthogonal groups, *International Journal of Computer Mathematics* **86**, 10–11 (2009), 1678–1683, (Q4, Mathematics, Applied, F.I. 0.308).

132. L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios (A), Analysis of the efficiency of the Chor-Rivest cryptosystem implementation in a safe-parameter range, *Information Sciences* **179** (2009), 4219–4226, `https://doi.org/10.1016/j.camwa.2008.09.006` (Q1, Computer Science, Information Systems, F.I. 3.095).

133. F. Hernández Álvarez and L. Hernández Encinas (A), Security Efficiency Analysis of a Biometric Fuzzy Extractor for Iris Templates, *Advances in Intelligent Software and Computing* **63** (2009), 163–170.

134. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué (A), Higher-order safe primes with negative signature: An algorithmic approach, *International Journal of Information Technology & Security* 1 (2009), 13–24.

135. L. Hernández Encinas (R), Wang, Jin-Song; Qi, Wen-Feng Four families of binary sequences with low correlation and large linear complexity. Information security and Cryptology, 216–230, Lecture Notes Comput. Sci., 4990, Springer, Berlin, 2008, MR2473377, 2009.

136. L. Hernández Encinas (R), Ding, Ning; Gu, Dawu A discrete-logarithm based non-interactive non-malleable commitment scheme with an online knowledge extractor. Information security and Cryptology, 153–166, Lecture Notes Comput. Sci., 4990, Springer, Berlin, 2008, MR2473372, 2009.

137. L. Hernández Encinas (R), Wang, Weijia; Hu, Lei; Li, Yong Provably secure N-party authenticated key exchange in the multicast DPWA setting. Information security and Cryptology, 93–107, Lecture Notes Comput. Sci., 4990, Springer, Berlin, 2008, MR2473368, 2009.

138. L. Hernández Encinas (R), Chevalier, Yannick; Kourjieh, Mounira Key substitution in the symbolic analysis of cryptographic protocols. FSTTCS 2007: Foundations of software technology and theoretical computer science, 121–132, Lecture Notes Comput. Sci., 4855, Springer, Berlin, 2007, MR2480195, 2009.

139. L. Hernández Encinas (R), Jacobson, M. J., Jr.; Scheidler, R.; Stein, A. Fast arithmetic on hyperelliptic curves via continued fraction expansions. Advances in coding theory and cryptography, 200–243, Ser. Coding Theory Cryptol., 3, World Sci. Publ., Hackensack, NJ, 2007, MR2454114, 2009.

140. L. Hernández Encinas (R), Pietrzak, Krzysztof; Sjödin, Johan Range extension for weak PRFs: the good, the bad, and the ugly. Advances in cryptology—EUROCRYPT 2007, 517–533, Lecture Notes Comput. Sci., 4515, Springer, Berlin, 2007, MR2449229 (2009m:94060), 2009.

141. L. Hernández Encinas (R), Ristenpart, Thomas; Yilek, Scott The power of proofs-of-possession: securing multiparty signatures against rogue-key attacks. Advances in cryptology-EUROCRYPT 2007, 228–245, Lecture Notes Comput. Sci., 4515, Springer, Berlin, 2007, MR2449212 (2009m:94073), 2009.

142. L. Hernández Encinas (R), Maurer, Ueli; Pietrzak, Krzysztof; Renner, Renato Indistinguishability amplification. Advances in cryptology—CRYPTO 2007, 130–149, Lecture Notes Comput. Sci., 4622, Springer, Berlin, 2007, MR2419598, 2009.

143. L. Hernández Encinas (R), Heath-Brown, D. R., Carmichael numbers with three prime factors. Hardy-Ramanujan J. 30 (2007), 6–12, *Mathematical Reviews* MR2440316 (2009g:11123), 2009.

144. L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios (A), Safer Parameters for the Chor-Rivest Cryptosystem, *Computers & Mathematics with Application* **56** (2008), 2883–2886, (Q2, Computer Science, Interdisciplinary Applications, F.I. 0.997).

145. G. Alvarez, L. Hernández Encinas, and A. Martín del Rey (A), A multisecret sharing scheme for color images based on cellular automata, *Information Sciences* **178** (2008), 4382–4395, (Q1, Computer Science, Information Systems, F.I. 3.095).

146. L. Hernández Encinas, A. Martín del Rey and J. Muñoz Masqué (A), A weakness in authenticated encryption schemes based on Tseng et al.'s schemes, *International Journal on Network Security* **7**, 2 (2008), 157–159.

147. A. Queiruga Dios, L. Hernández Encinas, D. Queiruga (A), Cryptography Adapted to the New European Area of Higher Education, *Lecture Notes in Computer Sciences* **5102** (2008), 706–714.

148. G. Alvarez, L. Hernández Encinas, and J. Muñoz Masqué (A), Known-plaintext attack to two cryptosystems based on the BB equation, *IEEE Trans. Circuits Systems II, Express Briefs* **55**, 5 (2008), 423–426, (Q2, Engineering, Electrical & Electronic, F.I. 1.104).

149. A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, and G. Rodríguez Sánchez (A), Simulation of forest fire fronts using cellular automata, *Advances in Engineering & Software* **38** (2007), 372–378, (Q4, Computer Science, Interdisciplinary Applications, F.I. 0.263).

150. L. Hernández Encinas, S. Hoya White, A. Martín del Rey, and G. Rodríguez Sánchez (A), Modelling forest fire spread using hexagonal cellular automata, *Applied Mathematical Modelling* **31** (2007), 1213–1227, (Q2, Mathematics, Interdisciplinary Applications, F.I. 0.433).

151. L. Hernández Encinas, A. Martín del Rey (A), Inverse rules of ECA with rule number 150, *Applied Mathematics & Computation* **189** (2007), 1782–1786, (Q2, Mathematics, Applied, F.I. 0.688).

152. G. Alvarez, S. Li, and L. Hernández (A), Analysis of security problems in a medical image encryption system, *Computers in Biology and Medicine* **37**, 3 (2007), 424–427, (Q2, Computer Science, Interdisciplinary Applications, F.I. 1.358).

153. eSEC (S), *Agenda Estratégica de Investigación*, Plataforma Tecnológica Española de Seguridad y Confianza, AETIC, Madrid, 2006.

154. L. Hernández Encinas (R), Shim, Kyung-Ah; Woo, Sung Sik Cryptanalysis of tripartite and multiparty authenticated key agreement protocols. Inform. Sci. 177 (2007), no. 4, 1143–1151, *Mathematical Reviews* MR2288748 (2007k:94076), 2007.

155. L. Hernández Encinas (R), Malone-Lee, John A general construction for simultaneous signing and encrypting. Cryptography and coding, 116–135, Lecture Notes Comput. Sci., 3796, Springer, Berlin, 2005. 94A62 (94A60), *Mathematical Reviews* MR2235253 (2007c: 94224), 2007.

156. L. Hernández Encinas and A. Peinado Domínguez (A), Comment on 'A technique for image encryption using digital signature', *Optics Communications* **268**, 2 (2006), 261–265, (Q2, Optics, F.I. 0.402).

157. J. Espinosa García, L. Hernández Encinas and J. Muñoz Masqué (A), A review on the isomorphism classes of hyperelliptic curves of genus 2 over finite fields admitting a Weierstrass point, *Acta Applicandae Mathematicae* **93** (2006), 299–318, (Q4, Mathematics, Applied, F.I. 0.456), `https://doi.org/10.1007/s10440-006-9045-2`

158. L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios (A), Maple implementation of the Chor-Rivest cryptosystem, *Lecture Notes in Computer Sciences* **3992** (2006), 438–445, (Q4, Computer Science, Theory & Methods, F.I. 0.402).

159. L. Hernández Encinas (R), Rebollo-Neira, L.; Plastino, A. Statistical distribution, host for encrypted information. Phys. A 359 (2006), 213–221. 94A60 (94A17), *Mathematical Reviews* MR2198982 (2006j:94077), 2006.

160. L. Hernández Encinas (R), Chen, Liqun; Malone-Lee, John Improved identity-based signcryption. Public key cryptography—PKC 2005, 362–379, Lecture Notes Comput. Sci., 3386, Springer, Berlin, 2005. 94A60, *Mathematical Reviews* MR2174053 (2006j:94056), 2006.

161. L. Hernández Encinas (R), Atieg, A.; Watson, G. A. Fitting circular arcs by orthogonal distance regression. Appl. Numer. Anal. Comput. Math. 1 (2004), no. 1-2, 66–76. 65D10 (65K10), *Mathematical Reviews* MR2168317 (2006g:65017), 2006.

162. L. Hernández Encinas (R), Hwang, Shin-Jia Improvement of Tseng et al.'s authenticated encryption scheme. Appl. Math. Comput. 165 (2005), no. 1, 1–4. 94A62 (94A60), *Mathematical Reviews* MR2137020 (2006b:94050), 2006.

163. L. Hernández Encinas (R), Chang, Chin-Chen; Lin, Iuon-Chang Cryptanalysis of the modified remote login authentication scheme based on a geometric approach. Informatica (Vilnius) 16 (2005), no. 1, 37–44. 94A60 (68M12 94A62), *Mathematical Reviews* MR2133298 (2006b:94023), 2006.

164. G. Alvarez, A. Hernández Encinas, L. Hernández Encinas, and A. Martín del Rey (A), A secure scheme to share secret color images, *Computer Physics Communications* **173**, 1 (2005), 9–16, (Q1, Computer Science, Interdisciplinary Applications, F.I. 1.644).

165. G. Alvarez, L. Hernández, J. Muñoz, F. Montoya, and S. Li (A), Security analysis of communication system based on the synchronization of different order chaotic systems, *Physics Letters A* **345**, 4 (2005), 245–250, (Q2, Physics, Multidisciplinary, F.I. 1.550).

166. G. Álvarez Marañón, L. Hernández Encinas, and A. Martín del Rey (A), A new secret sharing scheme for images based on additive 2-dimensional cellular automata, *Lecture Notes in Computer Sciences* **3522** (2005), 411–418, (Q4, Computer Science, Theory & Methods, F.I. 0.402).

167. L. Hernández Encinas, A. Martín del Rey, and J. Muñoz Masqué (A), Faà di Bruno formula, lattices, and partitions, *Discrete Applied Mathematics* **148**, 3 (2005), 246–255, (Q3, Mathematics, Applied, F.I. 0.585).

168. L. Hernández Encinas, A. Martín del Rey, and G. Rodríguez Sánchez (A), Secure storage and integrity protection of images, *IADAT Journal of Advanced Technology on Imaging and Graphics* **1**, 2 (2005), 72–74.

169. L. Hernández Encinas and J. Muñoz Masqué (A), Isomorphism classes of genus-2 hyperelliptic curves over finite fields $\mathbb{F}_{5^m}$, *Information* **8**, 6 (2005), 8 pp.

170. O. García Delgado, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, and G. Rodríguez Sánchez (A), Characterization of the reversibility of Wolfram cellular automata with rule number 150 and periodic boundary conditions, *Information* **8**, 4 (2005), 10 pp.

171. R. Álvarez Mariño, G. Álvarez Marañón, L. Hernández Encinas, A. Martín del Rey y R. Martín del Rey (A), Protección de la confidencialidad, autenticidad e integridad de imágenes médicas mediante protocolos criptográficos, *Informática y Salud* **52** (2005), 81–84.

172. P.M. Alcover Garau, J.M. García Carrasco, y L. Hernández Encinas (A), Diseño de un nuevo generador de secuencias de bits aleatorios por entrada de teclado, *Novática* **174** (2005), 59–65.

173. R. Durán Díaz, L. Hernández Encinas y J. Muñoz Masqué (L), *El criptosistema RSA*, RA-MA, Madrid, 2005, 310 pp. ISBN: 84-7897-651-5, `https://www.ra-ma.es/libro/el-criptosistema-rsa_48854/`.

174. eSEC (S), *Agenda Estratégica de Investigación*, Plataforma Tecnológica Española de Seguridad y Confianza, AETIC, Madrid, 2005.

175. L. Hernández Encinas (R), Chang, Ya-Fen; Chang, Chin-Chen; Huang, Hui-Feng. Digital signature with message recovery using self-certified public keys without trustworthy system authority. *Applied Mathematics & Computation* **161** (2005), no. 1, 211–227. 94A62 (94A60), *Mathematical Reviews* MR2111341 (2005h:94064), 2005.

176. L. Hernández Encinas (R), Buchmann, Johannes. Introduction to cryptography. Second ed. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2004. xvi+335 pp. ISBN 0-387-21156-X; 0-387-20756-2. 94A60 (11T71 94-01 94A62), *Mathematical Reviews* MR2075209 (2005f:94084), 2005.

177. L. Hernández Encinas (R), Lai, Chun-Pong; Ding, Cunsheng. Several generalizations of Shamir's secret sharing scheme. *Internat. J. Found. Comput. Sci.* **15** (2004), no. 2, 445–458. 94A62 (68P25), *Mathematical Reviews* MR2071468 (2005e:94240), 2005.

178. L. Hernández Encinas (R), Bowong, Samuel. Stability analysis for the synchronization of chaotic systems with different order: application to secure communications. *Phys. Lett. A* **326** (2004), no. 1-2, 102–113. 94A60 (34D20 37D45 37N99), *Mathematical Reviews* MR2065892 (2005e:94115), 2005.

179. L. Hernández Encinas (R), Al-Riyami, Sattam S.; Paterson, Kenneth G. Certificateless public key cryptography. *Advances in cryptology—ASIACRYPT 2003*, 452–473, *Lect. Notes Comput. Sci.*, 2894, Springer, Berlin, 2003. 94A60 (94A62), *Mathematical Reviews* MR2093598 (2005f:94076), 2005.

180. L. Hernández Encinas (R), Bresson, Emmanuel; Catalano, Dario; Pointcheval, David. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. *Advances in cryptology—ASIACRYPT 2003*, 37–54, *Lect. Notes Comput. Sci.*, 2894, Springer, Berlin, 2003. 94A60, *Mathematical Reviews* MR2093251 (2005h:94041), 2005.

181. L. Hernández Encinas (R), Niemi, Valtteri. Hiding regular languages. *Grammars and automata for string processing*, 305–315, *Topics in Comput. Math.*, 9, Taylor & Francis, London, 2003. 68P25 (68Q45 94A60), *Mathematical Reviews* MR2036839 (2005b:68084), 2005.

182. G. Álvarez Marañón, L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué (A), Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion, *J. Sound Vibration* **275** (2004), 423–430, (Q1, Engineering, Mechanical, F.I. 0.898).

183. L. Hernández Encinas, A. Martín del Rey and J. Muñoz Masqué (A), Non-degenerate bilinear alternating maps $f\colon V \times V \to V$, $\dim(V) = 3$, over an algebraically closed field, *Linear Algebra and its Applications* **387** (2004), 69–82, (Q2, Mathematics, Applied, F.I. 0.590).

184. L. Hernández Encinas and J. Muñoz Masqué (A), Total curvatures of a closed curve in Euclidean n-space, *Proceedings of the American Mathematical Society* **132** (2004), 2127–2132, (Q3, Mathematics, Applied, F.I. 0.429).

185. C. Fraile Rubio, L. Hernández Encinas, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez (A), The use of linear hybrid cellular automata as pseudorandom bit generators in cryptography, *Neural, Parallel and Scientific Computations* **12** (2004), 175–192.

186. L. Hernández Encinas, A. Hernández Encinas, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez (A), Graphic cryptosystem using memory cellular automata, *Upgrade* **V**, 6 (2004), 22–24.

187. L. Hernández Encinas, A. Hernández Encinas, S. Hoya White, A. Martín del Rey y G. Rodríguez Sánchez (A), Cifrado de imágenes usando autómatas celulares con memoria, *Novática* **172** (2004), 21–23.

188. J. Espinosa García, L. Hernández Encinas y A. Martín del Rey (A), Codificación de información mediante códigos bidimensionales, *SEMA, Boletin de la Sociedad Española de Matemática Aplicada* **29** (2004), 35–55.

189. L. Hernández Encinas y A. Martín del Rey (A), Codificación de información mediante códigos de barras, *SEMA, Boletin de la Sociedad Española de Matemática Aplicada* **27** (2004), 29–48.

190. A. Fúster Sabater, D. de la Guía Martínez, L. Hernández Encinas, F. Montoya Vitini y J. Muñoz Masqué (L), *Técnicas criptográficas de protección de datos*, RA-MA, 3ª edición actualizada, Madrid, 2004, 395 pp. ISBN: 84-7897-594-2.

191. J.M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez (C), *Resolución de problemas en Matemáticas. Aplicación multimedia*, Nivola, Tres Cantos (Madrid), 2004, ISBN: 84-95599-80-5.

192. L. Hernández Encinas (R), Mizuki, Takaaki; Shizuya, Hiroki; Nishizeki, Takao. Characterization of optimal key set protocols. The Second International Colloquium "Journées de l'Informatique Messine" (Metz, 2000). *Discrete Appl. Math.* **131** (2003), no. 1, 213–236. 68P25 (94A99), *Mathematical Reviews* MR2018210 (2004j:68054), 2004.

193. L. Hernández Encinas (R), Beato Sirvent, Jesús. Periods. (Spanish) *Epsilon* **18** (2002), no. 1(52), 115–146. 11A05, *Mathematical Reviews* MR1995270 (2004d:11003), 2004.

194. L. Hernández Encinas (R), Bellare, M.; Namprempre, C.; Pointcheval, D.; Semanko, M. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *J. Cryptology* **16** (2003), no. 3, 185–215. 94A60 (68P25 68Q25), *Mathematical Reviews* MR1985441 (2004g:94043), 2004.

195. L. Hernández Encinas (R), Álvarez, G.; Montoya, F.; Romera, M.; Pastor, G. Cryptanalysis of an ergodic chaotic cipher. *Phys. Lett. A* **311** (2003), no. 2-3, 172–179. 94A60 (37N99), *Mathematical Reviews* MR1982340 (2004e:94029), 2004.

196. L. Hernández Encinas (R), Adi, Kamel; Debbabi, Mourad; Mejri, Mohamed A new logic for electronic commerce protocols. Algebraic methodology and software technology (Iowa City, IA, 2000). *Theoret. Comput. Sci.* **291** (2003), no. 3, 223–283. 94A60 (68P25 68Q60 94A62), *Mathematical Reviews* MR1957432 (2004b:94054), 2004.

197. L. Hernández Encinas (R), Mijajlović, Ž.; Marković, Z. Some recurrence formulas related to the differential operator θD. *Facta Univ. Ser. Math. Inform.* **13** (1998), 7–17. 11B75 (05A10), *Mathematical Reviews* MR2015882 (2004g:11013), 2004.

198. L. Hernández Encinas, J. Muñoz Masqué and A. Queiruga Dios (A), Large decryption exponents in RSA, *Applied Mathematics Letters* **16**, 3 (2003), 293–295, (Q2, Mathematics, Applied, F.I. 0.345).

199. L. Hernández Encinas and J. Muñoz Masqué (A), A short proof of the generalized Faà di Bruno's formula, *Applied Mathematics Letters* **16**, 6 (2003), 975–979, (Q2, Mathematics, Applied, F.I. 0.345).

200. G. Álvarez Marañón, L. Hernández Encinas, A. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez (A), Graphic cryptography with pseudorandom bit generators and cellular automata, *Lecture Notes in Computer Sciences* **2773** (2003), 1207–1214, (Q4, Computer Science, Theory & Methods, F.I. 0.402).

201. R. Díaz Len, A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey, G. Rodríguez Sánchez and I. Visus Ruíz (A), Wolfram cellular automata and their cryptographic use as pseudorandom bit generators, *International Journal of Pure and Applied Mathematics* **4**, 1 (2003), 87–103.

202. L. Hernández Encinas, J. Muñoz Masqué and A. Queiruga Dios (A), An algorithm to obtain an RSA modulus with a large private key, *Cryptology ePrint Archive, Report* 2003/045, 10 pp., `http://eprint.iacr.org/`

203. G. Álvarez Marañón, L. Hernández Encinas, A. Martín del Rey (A), Sharing secret color images using cellular automata with memory, *arXiv.org e-Print archive, Computer Science* 0312034 (2003), 17 pp., `http://arxiv.org/abs/cs.CR/0312034`

204. L. Hernández Encinas (R), Martinelli, Fabio. Analysis of security protocols as open systems. *Theoret. Comput. Sci.* **290** (2003), no. 1, 1057–1106. 94A60 (68Q60), *Mathematical Reviews* MR1935715 (2003i:94048), 2003.

205. L. Hernández Encinas (R), Sandilya, Sathyakama; Kulkarni, Sanjeev R. Principal curves with bounded turn. *IEEE Trans. Inform. Theory* **48** (2002), no. 10, 2789–2793. 62H25 (65D10 68U10 94A08), *Mathematical Reviews* MR1930347 (2003h:62089), 2003.

206. L. Hernández Encinas (R), Li, Baibing; Martin, Elaine B.; Morris, A. Julian. On principal component analysis in L_1. *Comput. Statist. Data Anal.* **40** (2002), no. 3, 471–474. 62H25, *Mathematical Reviews* MR1926612 (2003f:62080), 2003.

207. L. Hernández Encinas (R), Meidl, Wilfried; Niederreiter, Harald. Linear complexity, k-error linear complexity, and the discrete Fourier transform. *J. Complexity* **18** (2002), no. 1, 87–103. 94A60 (11Y16 65T50 68W40 94A55), *Mathematical Reviews* MR1895078 (2003f:94068), 2003.

208. L. Hernández Encinas (R), Shahruz, S. M.; Pradeep, A. K.; Gurumoorthy, R. Design of a novel cryptosystem based on chaotic oscillators and feedback inversion. *J. Sound Vibration* **250** (2002), no. 4, 762–771. 94A60 (34C28 37N99), *Mathematical Reviews* MR1893980 (2003f:94071), 2003.

209. L. Hernández Encinas (R), Masuda, Naoki; Aihara, Kazuyuki. Cryptosystems with discretized chaotic maps. *IEEE Trans. Circuits Systems I Fund. Theory Appl.* **49** (2002), no. 1, 28–40. 94A60 (37E05 37N99), *Mathematical Reviews* MR1874225 (2003a:94038), 2003.

210. L. Hernández Encinas (R), Panario, Daniel; Pittel, Boris; Richmond, Bruce; Viola, Alfredo. Analysis of Rabin's irreducibility test for polynomials over finite fields. Analysis of algorithms (Krynica Morska, 2000). *Random Structures Algorithms* **19** (2001), no. 3-4, 525–551. 68W40 (11T06 12E05), *Mathematical Reviews* MR1871565 (2003e:68152), 2003.

211. L. Hernández Encinas (R), Verheul, Eric R. Certificates of recoverability with scalable recovery agent security. Public key cryptography (Melbourne, 2000), 258–275, *Lect. Notes Comput. Sci.* **1751**, Springer, Berlin, 2000. 94A62 (94A60), *Mathematical Reviews* MR1864783 (2003e:94090), 2003.

212. L. Hernández Encinas, Alfred Menezes and J. Muñoz Masqué (A), Isomorphism classes of genus-2 hyperelliptic curves over finite fields, *Applicable Algebra in Engineering, Communication and Computing* **13**, 1 (2002), 57–65, (Q3, Mathematics, Applied, F.I. 0.389).

213. J. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández and M. Rodríguez López (A), Designing hypermedia tools for solving problems in Mathematics, *Computers & Education* **38, 4** (2002), 303–317, (Q1, Computer Science, Interdisciplinary Applications, F.I. 0.968).

214. L. Hernández Encinas and J. Muñoz Masqué (A), Isomorphism classes of hyperelliptic curves of genus 2 in characteristic 5 *Technical Report*, CORR-2002-07, Centre for Applied Cryptographic Research (CACR), University of Waterloo (Canada), 9 pp.

215. L. Hernández Encinas, A. Martín del Rey y G. Rodríguez Sánchez (A), Aplicaciones de los autómatas celulares a la generación de bits, *SEMA, Boletin de la Sociedad Española de Matemática Aplicada* **21** (2002), 65–87.

216. J.M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez (A), El cálculo mental también se puede desarrollar trabajando con el ordenador de forma interactiva, *Revista de Educación y Pedagogía* **XIV**, 33 (2002), 161–166.

217. N. Callaos, L. Hernández-Encinas and F. Yetim (E, L), *Proceedings of The 6th Multiconference on Systemics, Cybernetics and Informatics. Volumen I: Information Systems Development*, Orlando (USA), 2002, ISBN: 980-07-8150-1.

218. N. Callaos et al. (E, C), *Proceedings of The 6th Multiconference on Systemics, Cybernetics and Informatics*, Orlando (USA), 2002, ISBN: 980-07-8146-3.

219. L. Hernández Encinas (R), Schmitz, Roland. Use of chaotic dynamical systems in cryptography. *J. Franklin Inst.* **338** (2001), no. 4, 429–441. 94A60 (37D45 37N99). *Mathematical Reviews* MR1833969 (2002f:94044), 2002.

220. L. Hernández Encinas (R), Enge, Andreas. The extended Euclidian algorithm on polynomials, and the computational efficiency of hyperelliptic cryptosystems. *Design Codes and Cryptography* **23** (2001), no. 1, 53–74. 94A60 (11T71 14G50 68Q25). *Mathematical Reviews* MR1825028 (2002e:94096), 2002.

221. L. Hernández Encinas (R), Liseikin, V. D. Application of notions and relations of differential geometry to grid generation. *Russian J. Numer. Anal. Math. Modelling* **16** (2001), no. 1, 57–75. 65N50 (53A07 65N55). *Mathematical Reviews* MR1822988 (2002b:65183), 2002.

222. L. Hernández Encinas (L), *Técnicas de Taxonomía Numérica*, La Muralla, Madrid, 2001, 159 pp. ISBN: 84-7133-715-0.

223. N. Callaos, B. Sánchez, L. Hernández and J. Gryzmala (E, L), *Proceedings of The 5th Multiconference on Systemics, Cybernetics and Informatics, Volumen: VII*, Orlando (USA), 2001, 589 pp. ISBN: 980-07-7547-1.

224. N. Callaos et al. (E, C), *Proceedings of The 5th Multiconference on Systemics, Cybernetics and Informatics*Orlando (USA), 2001, ISBN: 980-07-7529-3.

225. L. Hernández Encinas (R), Buchmann, Johannes A. *Introduction to cryptography.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2001. xii+281 pp. ISBN: 0-387-95034-6 94A60 (11T71 94-01). *Mathematical Reviews* MR1802638 (2001k:94048), 2001.

226. L. Hernández Encinas (R), Hertrich-Jeromin, Udo. The surfaces capable of division into infinitesimal squares by their curves of curvature: a nonstandard-analysis approach to classical differential geometry. *Math. Intelligencer* **22** (2000), no. 2, 54–61. 53A05. *Mathematical Reviews* MR1764268 (2001b:53003), 2001.

227. M. Castrillón López, L. Hernández Encinas and J. Muñoz Masqué (A), Gauge invariance on interaction $U(1)$-bundles, *Journal of Physics A. Mathematical and General* **33** (2000), 3253–3267, (Q2, Physics, Mathematical, F.I. 1.680).

228. L. Hernández Encinas, F. Montoya Vitini y J. Muñoz Masqué (A), Esquemas criptográficos visuales, *Seguridad en Informática y Comunicaciones* **38** (2000), VI–X.

229. L. Hernández Encinas (A), Taller de criptomatemáticas para jóvenes (y adultos), *Suma* **33** (2000), 45–58.

230. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué (A), Ataques a DES y módulos factorizados de RSA, *Seguridad en Informática y Comunicaciones* **40** (2000), I–IV.

231. A. Fúster, D. de la Guía, L. Hernández, F. Montoya y J. Muñoz (L), *Técnicas criptográficas de protección de datos*, RA-MA, Madrid, 2ª ed. revisada y actualizada, 2000, 372 pp. ISBN: 84-7897-421-0.

232. L. Hernández Encinas y J. Rubio Álvarez (E, L), *Actas del 5º Seminario Castellano-Leonés de Educación Matemática*, Zamora, 2000, 297 pp. ISBN:84-922919-3-1.

233. L. Hernández Encinas (R), Castrillón-López, M. Gauge invariant variationally trivial U(1)-problems. *Differential geometry and applications* (Brno, 1998), 461–468, Masaryk Univ., Brno, 1999. 58E30 (53C07 70S05). *Mathematical Reviews* MR1708935 (2000f:58034), 2000.

234. L. Hernández Encinas (R), Kotulski, Zbigniew; Szczepański, Janusz; Górski, Karol; Paszkiewicz, Andrzej; Zugaj, Anna. Application of discrete chaotic dynamical systems in cryptography—DCC method. *Internat. J. Bifur. Chaos Appl. Sci. Engrg.* **9** (1999), no. 6, 1121–1135. 94A60 (37E05 37N99). *Mathematical Reviews* MR1712423 (2000i:94054), 2000.

235. L. Hernández Encinas (R), Castrillón López, M.; Muñoz Masqué, J. Gauge forms on SU(2)-bundles. *J. Geom. Phys.* **30** (1999), no. 4, 313–330. 53C07 (22E65). *Mathematical Reviews* MR1700562 (2000d:53039), 2000.

236. L. Hernández Encinas (R), Blackburn, Simon R. Combinatorics and threshold cryptography. *Combinatorial designs and their applications* (Milton Keynes, 1997), 49–70, Chapman & Hall/CRC Res. Notes Math., 403, Chapman & Hall/CRC, Boca Raton, FL, 1999. 94A62 (05B99 94A60). *Mathematical Reviews* MR1678593 (2000d:94026), 2000.

237. L. Hernández Encinas y J. Minguet Melián (A), Criptografía visual, *Novática* **138** (1999), 63–68.

238. L. Hernández Encinas (R), Castrillón López, Marco; Muñoz Masqué, J. Structure symplectique généralisée sur le fibré des connexions. (French). Generalized symplectic structure on the bundle of connections, *C. R. Acad. Sci. Paris Sér. I Math.* **328** (1999), no. 1, 41–44. 58D19 (53C05 58F05). *Mathematical Reviews* MR1674433 (99m:58036), 1999.

239. L. Hernández Encinas (R), Blundo, Carlo; De Santis, Alfredo; Herzberg, Amir; Kutten, Shay; Vaccaro, Ugo; Yung, Moti. Perfectly secure key distribution for dynamic conferences. *Inform. and Comput.* **146** (1998), no. 1, 1–23. 94A60. *Mathematical Reviews* MR1642243 (99j:94039), 1999.

240. A. Bejancu, L. Hernández Encinas and J. Muñoz Masqué (A), Invariant differential forms on the first jet prolongation of the cotangent bundle, *Houston Journal of Mathematics* **24**, 3 (1998), 421–442, (Q4, Mathematics, F.I. 0.353.

241. A. Hernández Encinas y L. Hernández Encinas (L), *Informática. Segundo ciclo de la E.S.O.*, Editex, Madrid, 1998, 471 pp. ISBN: 84-7131-586-6.

242. A. Hernández Encinas y L. Hernández Encinas (L), *Guía didáctica de Informática. Segundo ciclo de la E.S.O.*, Editex, Madrid, 1998, 134 pp. ISBN: 84-7131-587-4.

243. L. Hernández Encinas (R), Damgård, Ivan B.; Pedersen, Torben P.; Pfitzmann, Birgit. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *J. Cryptology* **10** (1997), no. 3, 163–194. 94A60 (68P25). *Mathematical Reviews* MR1456327 (98e:94016), 1998.

244. L. Hernández Encinas (R), Sakai, Manabu. Inflections and singularity on parametric rational cubic curves. *Numer. Math.* **76** (1997), no. 3, 403–417. 65D10 (14H45 65D07). *Mathematical Reviews* MR1452515 (98d:65018), 1998.

245. L. Hernández Encinas (R), Rochowski, Marek. The polar geodesic coordinate system on surfaces in the Euclidean 3-dimensional space. *Demonstratio Math.* **30** (1997), no. 1, 25–42. 53A05. *Mathematical Reviews* MR1446595 (98a:53006), 1998.

246. L. Hernández Encinas (R), Ateniese, Giuseppe; Blundo, Carlo; De Santis, Alfredo; Stinson, Douglas R. Visual cryptography for general access structures. *Inform. and Comput.* **129** (1996), no. 2, 86–106. 94A60 (68P25 94C15). *Mathematical Reviews* MR1418486 (98a:94017), 1998.

247. P.M. Gadea and L. Hernández Encinas (A), Reflector bundles on the 4-dimensional Kaneyuki-Kozai para-Hermitian symmetric spaces, *Balkan Journal of Geometry and Applications.* **2** (1997), 41–49.

248. A. Fúster, D. de la Guía, L. Hernández, F. Montoya y J. Muñoz (L), *Técnicas criptográficas de protección de datos*, RA-MA, Madrid, 1997, 279 pp. ISBN: 84-7897-288-9.

249. L. Hernández Encinas (R), Garg, Hari Krishna. On the factorization of polynomials and direct sum properties in integer polynomial rings. *Circuits Systems Signal Process.* **15** (1996), no. 3, 415–435. 11T30 (11R09 94A12). *Mathematical Reviews* MR1394057 (97e:11155), 1997.

250. L. Hernández Encinas (R), Takeuchi, Yu. Real number representation. (Spanish) VIth National Mathematics Conference (Spanish) (Bucaramanga, 1994). *Rev. Integr. Temas Mat.* **12** (1994), no. 2, 139–147. 11A67 (11A55 11B37). *Mathematical Reviews* MR1386203 (97a:11022), 1997.

251. L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué (A) A report on invariant gauge forms on associated bundles of an Abelian principal bundle, *Analele Stiintifice ale Universitatii Al. I. Cuza* **XLII** (1996), 113–122.

252. L. Hernández Encinas (R), Camarinha, M.; Silva Leite, F.; Crouch, P. Splines of class C^k on non-Euclidean spaces. *IMA J. Math. Control Inform.* **12** (1995), no. 4, 399–410. 41A15 (58E30 65D17). *Mathematical Reviews* MR1363321 (96i:41004), 1996.

253. L. Hernández Encinas (R), De Santis, Alfredo; Di Crescenzo, Giovanni; Persiano, Giuseppe. Zero-knowledge arguments and public-key cryptography. *Inform. and Comput.* **121** (1995), no. 1, 23–40. 94A60 (11Y16). *Mathematical Reviews* MR1347330 (96i:94018), 1996.

254. L. Hernández Encinas (A), Gauge invariant differential forms on Abelian principal bundles, *Analele Stiintifice ale Universitatii "Ovidius" Constanta*, Seria Matematica **3**, 2 (1995), 5–14.

255. L. Hernández Encinas (A), Partitioning large data sets: use of statistical methods applied to a set of russian igneous-rocks chemical analyses, *Computers & Geosciences UK* **20**, 10 (1994), 1405–1414, (Q2, Computer Science, Interdisciplinary Applications, F.I. 0.893).

256. L. Hernández Encinas and J. Muñoz Masqué (A), Gauge invariance on the bundle of conections of a $U(1)$-principal bundle, *Comptes Rendus de l'Académie des Sciences Paris*, Série I-Math **318** (1994), 1133–1138, (Q4, Mathematics, F.I. 0.350).

257. L. Hernández Encinas and J. Muñoz Masqué (A), Symplectic structure and gauge invariance on the cotangent bundle, *Journal of Mathematical Physics* **35** (1994), 426–434, (Q3, Physics, Mathematical, F.I. 1.137).

258. J. del Río Sánchez, L. Hernández Encinas y M. J. Rodríguez Conde (L), *Análisis comparado del curriculum de Matemáticas en Iberoamérica*, Mare Nostrum, Madrid, 1992, 237 pp. ISBN: 84-87049-63-X.

259. L. Hernández Encinas y F. Bea Barredo (A), Técnicas geomatemáticas para la separación de diferentes rocas ígneas a partir de elementos mayores, *Studia Geologica Salmanticensia* **XXVI** (1989), 215–247.

260. J. Cabezas Corchero y L. Hernández Encinas (A), Geometría esférica en LOGO, *Gaceta Matemática* **1** (1) (1988), 13–24.

Artículos en el SCI	67
Libros publicados	14
Otros artículos internacionales (no SCI)	41
Artículos nacionales	15
Recensiones internacionales firmadas	88
Capítulos de libro (con ISBN)	7
Informes y Documentos restringidos	11
Revistas/Libros editados (con ISBN)	11
CD-ROMs	1

Participación en contratos de I+D de especial relevancia con Empresas y/o Administraciones (nacionales y/o internacionales)

1. Contrato: *Common Criteria evaluation project of Beijing Tsingteng Microsystem Co., LTD. THN31 Secure Element version 1.0.1.*. Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 07/01/2025 hasta: 06/01/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 1.815,00 €.

2. Contrato: *Common Criteria evaluation project of EPICOM EPICOM EP430TQ version 2.00 revision 01.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 24/10/2024 hasta: 23/10/2025. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

3. Contrato: *Common Criteria evaluation project of Thales DIS France SAS Multiapp Essential v1.1.*. Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 13/10/2024 hasta: 12/10/2025. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 6.050,00 €.

4. Contrato: *Asistencia técnica para análisis de impacto computacional a criptosistemas post-cuánticos basados en retículos.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 2024/CI01010000/00002850. Entidad participante: CSIC. Duración, desde: 15/01/2025 hasta: 15/12/2025. Investigador responsable: L. Hernández Encinas. Nº de participantes: 5. Importe total del proyecto: 100.000,00 €.

5. Contrato: *Common Criteria Evaluation of LX Semicon Co., Ltd., TOE LX34300 version 1.0.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 13/06/2024 hasta: 12/06/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

6. Contrato: *Common Criteria evaluation project of Datang Microelectronics Technology Co.,Ltd. DMT-CBS-CE3D Secure chip with Crypto library, version 1.1.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 30/05/2024 hasta: 29/05/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

7. Contrato: *Common Criteria evaluation project of Tongxin Microelectronics Co., Ltd. THC80F480C/384C/340C/280C/256C/228C/176C/150C Secure Microcontroller Version 1.0.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 30/05/2024 hasta: 29/05/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 6.050,00 €.

8. Contrato: *Common Criteria evaluation project of GEOP02 on GSE20 Security Chip.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 06/05/2024 hasta: 05/05/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

9. Contrato: *Revision of the AVA report corresponding to the evaluation carried out by LGAI of the Winbond's product SpiFlash® TrustME™ W75F40W[W/R] [I/J/W] [B/C] & W75F40W [BY/Q3] [I/J/W] [C/B]G Secure Serial Flash Memory Version: AA.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 06/03/2024 hasta: 05/03/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 2.000,00 €.

10. Contrato: *Common Criteria Evaluation of Sony Semiconductor Israel Ltd., Sony iSE700 V.1.0.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 29/02/2024 hasta: 28/02/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

11. Contrato: *Common Criteria Evaluation of MK Smart Joint Stock Company's MK Lotus GovID IMDa V4.7.0.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 29/02/2024 hasta: 28/02/2026. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

12. Contrato: *Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010220007100. Entidad participante: CSIC. Duración, desde: 01/01/2024 hasta: 31/12/2024. Investigador responsable: L. Hernández Encinas. Nº de participantes: 6. Importe total del proyecto: 148.830,00 €.

13. Contrato: *CC Evaluation of Tongxing Microelectronics Co., Ltd. THD89 Secure Microcontroller version 1.0 with Crypto Library version 1.01.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 13/12/2023 hasta: 12/12/2025. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 7.562,50 €.

14. Contrato: *Estudio de algoritmo postcuántico.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 2023/CI01010000/00001885-E. Entidad participante: CSIC. Duración, desde: 26/10/2023 hasta: 30/06/2024. Investigador responsable: L. Hernández Encinas. Nº de participantes: 5. Importe total del proyecto: 100.000,00 €.

15. Contrato: *Estudio del estado del arte de la seguridad de librerías de criptografía postcuántica, incluyendo ataques por canal lateral a sus implementaciones y posibles contramedidas.* Empresa financiadora: EPICOM. Entidad participante: CSIC. Duración, desde: 01/06/2023 hasta: 30/12/2023. Investigador responsable: L. Hernández Encinas. Nº de participantes: 5. Importe total del proyecto: 72.600,00 €.

16. Contrato: *Revision of the AVA report corresponding to the evaluation carried out by LGAI of the Winbond's product SpiFlash® TrustME™ W75F40W [W/R] [I/J/W] [B/C] & W75F40W [BY/Q3] [I/J/W] [C/B]G Secure Serial Flash Memory Version: AA.* Empresa financiadora: Winbond Electronics Corporation. Entidad participante: CSIC. Duración, desde: 06/03/2023 hasta: 05/06/2024. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 2.000,00 €.

17. Contrato: *Technical Support Project for CC Evaluation of Tongxing Microelectronics Co., Ltd. THD89 Secure Microcontroller, version 1.0.5, with Crypto Library.* Empresa financiadora: LGAI Technological Center. Entidad participante: CSIC. Duración, desde: 30/01/2023 hasta: 29/01/2025. Investigador responsable: A. Martín Muñoz. Nº de participantes: 2. Importe total del proyecto: 18.150,00 €.

18. Contrato: *Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010220007100. Entidad participante: CSIC. Duración, desde: 01/01/2023 hasta: 31/12/2023. Investigador responsable: L. Hernández Encinas. Nº de participantes: 6. Importe total del proyecto: 148.830,00 €.

19. Contrato: *Revisión de los informes de AVA correspondientes a la evaluación Common Criteria llevada a cabo por LGAI del producto PRESENCE2_SM.* Empresa financiadora: TECNOBIT, S.L.U. Entidad participante: CSIC. Duración, desde: 21/04/2022 hasta: 21/09/2023. Investigador responsable: L. Hernández Encinas. Nº de participantes: 2. Importe total del proyecto: 6.050,00 €.

20. Contrato: *Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010220007100. Entidad participante: CSIC. Duración, desde: 01/01/2022 hasta: 31/12/2022. Investigador responsable: L. Hernández Encinas. Nº de participantes: 7. Importe total del proyecto: 148.830,00 €.

21. Contrato: *Technical Support Project entitled Tongxin Microelectronics Co., Ltd. THD89: "THD89 Secure Microcontroller version 1.0.3 with Crypto Library version 2.10", and the CC renewals of HID Global: "SOMA-c007 Machine Readable Electronic Document Basic Access Control, Version 3", and "SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA, Version 3".* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 13/08/2021 hasta: 12/08/2022. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 19.965 €.

22. Contrato: *SAMSUNG Electronics Co. Ltd 1) S3FW9FG/F6/F5/F2 revision0 - RENEWAL, 2) S3FW9FV/FT/F9/F8 revision2 - RENEWAL, and 3) STRONG_ V2P10_ LN04LPE of S5E9925 with Specific IC Dedicated Software revision 0.0.* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 25/03/2021 hasta: 24/03/2022. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 21.780 €.

23. Contrato: *Technical Support Project "Beijing TsingTeng MicroSystem Co., Ltd THN31: THN31 Secure Element version 1.0 with Crypto Library versión 1.0".* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 19/03/2021 hasta: 18/03/2022. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

24. Contrato: *Estudio de viabilidad para mejorar la obtención de trazas de consumo de potencia o emanaciones electromagnéticas de una PCB.* Empresa financiadora: HOMYHUB S.L. Entidad participante: CSIC. Duración, desde: 22/03/2021 hasta: 30/10/2021. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 1.210 €.

25. Contrato: *KRYPTUS ASI-HSM AHX5 kNET Cryptographic Module: ASI-HSM AHX5 kNET Cryptographic Module v1.1.0 y la evaluación Common Criteria del producto de THALES MultiApp Essential v1.1 : MultiApp Essential v1.1 Platform with Full, Light, XLight_ T1 and XLight_ NB configurations v1.1.* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 22/01/2021 hasta: 17/01/2023. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 7.865 €.

26. Contrato: *Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010220007100. Entidad participante: CSIC. Duración, desde: 01/01/2021 hasta: 31/12/2021. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 148.830,00 €.

27. Contrato: *Evaluación Common Criteria del producto de [Samsung] [Aquarius]: [STRONGV2P0 of S5E9840 with Specific IC Dedicated Software, version 1.0] y la revisión de recertificación de 2 productos de [Samsung] [Arikara3]: [S3FW9FJ/FL/FH/FU Revision 0 with DTRNG Library v2.0], [Samsung] [Arikara4]: [S3M228A/192A/176A/132A Revision 0].* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 30/07/2020 hasta: 30/07/2021. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 15.730 €.

28. Contrato: *Apoyo Tecnológico para la Evaluación y Defensa de los Informes y Algoritmos de Cifra Implementados en Productos de Cifra Nacionales en el Sistema Galileo.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010320025800. Entidad participante: CSIC. Duración, desde: 10/06/2020 hasta: 15/12/2020. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 100.000,00 €.

29. Contrato: *Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010220007100. Entidad participante: CSIC. Duración, desde: 01/01/2020 hasta: 23/12/2020. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 148.830,00 €.

30. Contrato: *Revision of the AVA report corresponding to the evaluation of the mentioned product Winbond W75F40WBYJCG rev A SpiFlash TrustME Secure Flash Memory.* Empresa financiadora: Winbond Electronics Corporation. Entidad participante: CSIC. Duración, desde: 13/12/2019 hasta: 12/06/2020. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 1.500 €.

31. Contrato: *Criptología nacional para el canal secundario Galileo.* Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010219060500. Entidad participante: CSIC. Duración, desde: 30/10/2019 hasta: 30/04/2020. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 242.000,00 €.

32. Contrato: *Supervision and validation of the test plan and attacks corresponding to the vulnerability analysis (AVA) of the LESIKAR product Motion Sensor for Digital (smart) Tachographs Lesikar TACH3, carried out by LGAI.* Empresa financiadora: LESIKAR, a.s. Entidad participante: CSIC. Duración, desde: 23/07/2019 hasta: 22/01/2020. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 5.000 €.

33. Contrato: *Evaluaciones Common Criteria de los productos DNIe versión 4.0, TC-FNMT versión 5.0, Permiso de Residencia versión 4.0 y Pasaporte electrónico versión 4.0, desarrollados por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 07/06/2019 hasta: 30/11/2021. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 24.200 €.

34. Contrato: *Evaluación Common Criteria Samsung Andromeda: SSP01 Secure Element Platform with Specific IC Dedicated Software S3M228A/192A/176A/132A revision0 (recertificación) y del producto TDH Secure Microcontroler version 1.0 Crypto Library version 1.01 (recertificación).* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 10/01/2019 hasta: 10/07/2019. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 21.780 €.

35. Contrato: *Evaluaciones Common Criteria de los productos DNIe-DCCF 3.0, v1.1 Rev 4, CELES-c001 Machine Readable Electronic Document SSCD Application y SOMA-007 Machine Readable Electronic Document SSCD Application Version (recertificación), y soporte para la auditoría SOGIS.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 19/12/2018 hasta: 15/02/2019. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 14.278 €.

36. Contrato: *Revisión del informe AVA correspondiente a la evaluación del producto 'Samsung S3SSE8A revision 0'.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 18/10/2018 hasta: 17/04/2019. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

37. Contrato: *Revision of the AVA report corresponding to the evaluation of the product Winbond W75F32WKDJB - W75F32WKDJC SpiFlash TrustME Secure Serial Flash Memory, version TBD, carried out by LGAI.* Empresa/Administración financiadora: Winbond Electronics Corporation. Entidad participante: CSIC. Duración, desde: 29/08/2018 hasta: 28/03/2019. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 15.000 €.

38. Contrato: *Evaluación Common Criteria EAL 5, AVA VAN 5, MultiApp Essential v1.1.* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 30/08/2018 hasta: 29/08/2019. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

39. Prestación se servicio: *Desarrollo de trabajos relacionados con la evaluación (re-certificación) Common Criteria del producto Samsung S3FW9FJ/FL/FH/FU revision 0.* Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 04/06/2018 hasta: 04/07/2018. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total de la prestación: 2.904 €.

40. Contrato: *Estudio de la fortaleza y posible criptoanálisis de los nuevos algoritmos de cifra implementados en productos de cifra nacionales en el sistema Galileo.* Empresa/Administración financiadora: Ministerio de Defensa, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010318022700. Entidad participante: CSIC. Duración, desde: 09/08/2018 hasta: 15/12/2018. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 59.999,79 €.

41. Contrato: *Asistencia Técnica 2018 para la Evaluación de la Seguridad de Productos Criptográficos.* Empresa/Administración financiadora: Ministerio de la Presidencia, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010318014800. Entidad participante: CSIC. Duración, desde: 01/05/2018 hasta: 15/12/2018. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 148.830 €.

42. Contrato: *Capacitación Security Boxes*. Empresa/Administración financiadora: Epoche and Espri S.L.U. Entidad participante: CSIC. Duración, desde: 07/03/2018 hasta: 06/07/2018. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 12.100 €.

43. Contrato: *Evaluación Common Criteria EAL 4+ BAC y EAC del producto SOMA-c018 Machine Readable Electronic Document*. Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 27/02/2018 hasta: 26/08/2018. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 12.100 €.

44. Contrato: *Common Criteria EAL5+AVA_ AVAN.5+ALC_ DVS.2 de THD89*. Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 03/11/2017 hasta: 03/04/2018. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

45. Contrato: *Estudio de la fortaleza y posible criptoanálisis de algoritmos de cifra implementados en productos de cifra nacionales en el sistema Galileo*. Empresa/Administración financiadora: Ministerio de la Presidencia, Centro Nacional de Inteligencia (CNI). Nº Expediente 3010317032000. Entidad participante: CSIC. Duración, desde: 10/09/2017 hasta: 15/12/2017. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 250.000 €.

46. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a la evaluación Common Criteria EAL5+AVA_ VAN.5, ALC_ DVS.2 Dde KONA2 D2320N ePassport PACE [EAC with PACE configuration] version 02 (CCEKON004)*. Empresa financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 30/03/2017 hasta: 30/06/2018. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

47. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a la evaluación Common Criteria EAL4+AVA_ VAN.4 y ALC_ DVS.2 de S3M228A/192A/176A/132A Rev.0 (CCESAM005)*. Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 30/03/2017 hasta: 30/10/2017. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 2. Importe total del proyecto: 18.150 €.

48. Contrato: *Asistencia técnica 2017 en materia de evaluación de la seguridad de productos criptográficos*. Empresa/Administración financiadora: Ministerio de la Presidencia, Centro Nacional de Inteligencia (CNI). Nº Expediente 3010317001400. Entidad participante: CSIC. Duración, desde: 16/01/2017 hasta: 15/12/2017. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 147.620 €.

49. Contrato: *Análisis de un Sistema de Voto electrónico por internet para Mexicanos Residentes en el Extranjero (VeMRE)*. Empresa/Administración financiadora: Minsait-INDRA. Entidad participante: CSIC. Duración, desde: 25/01/2017 hasta: 31/03/2017. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 49.912,5 €.

50. Contrato: *Métodos de evaluación de los algoritmos SOG-IS*. Empresa/Administración financiadora: Ministerio de la Presidencia, Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010416052199. Entidad participante: CSIC. Duración, desde: 05/08/2016 hasta: 18/12/2016. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 2. Importe total del proyecto: 21.659 €.

51. Contrato: *Asistencia técnica para el análisis de canal lateral sobre circuitos integrados de cifra*. Empresa/Administración financiadora: Ministerio de la Presidencia, Centro Nacional de Inteligencia (CNI). Entidad participante: CSIC. Duración, desde: 29/07/2016 hasta: 28/10/2016. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4. Importe total del proyecto: 42.000 €.

52. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a las evaluaciones Common Criteria EAL 5+ ALC_ DVS.2 y AVA_ VAN.5 para las aplicaciones EAC-SAC y SSCD del producto SOMA-c007 Machine Readable Electronic Document del fabricante ARJO SYSTEMS (CCEARJ002, CCEARJ003)*. Empresa/Administración financiadora:

LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 01/07/2016 hasta: 30/09/2017. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 24.200 €.

53. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a la evaluación Common Criteria EAL4+ AVA_ VAN.4 y ALC_ DVS.2 de S3FW9FJ/FL/FH/FU Rev.0 (CCESAM004) de la funcionalidad RNG y AES.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 27/06/2016 hasta: 15/12/2016. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 3. Importe total del proyecto: 12.100 €.

54. Contrato: *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, D-COD-16-T08.* Empresa/Administración financiadora: European Union Agency for Network and Information Security (ENISA). Entidad participante: CSIC. Duración, desde: 18/03/2016 hasta: 30/09/2016. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 6. Importe total del proyecto: 54.400 €.

55. Contrato: *Revision of the AVA report corresponding to the evaluation of the Secured Element IC product W76S(16/32)R(KD/DN/Q1/Q3/4F) carried out by LGAI.* Empresa/Administración financiadora: Winbond Electronics Corporation. Entidad participante: CSIC. Duración, desde: 13/01/2016 hasta: 12/01/2017. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 18.150 €.

56. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a la evaluación Common Criteria EAL5+AVA_ VAN.5 de KONA2 D2320N ePassport EAC V1.0 (CCEKON002).* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 17/12/2015 hasta: 13/06/2016. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 18.150 €.

57. Contrato: *Métodos de evaluación de las funciones resumen SHA-2.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010415069399. Entidad participante: CSIC. Duración, desde: 27/11/2015 hasta: 15/12/2015. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 21.780 €.

58. Contrato: *Revisión del análisis de vulnerabilidades y de los resultados de los ataques correspondientes a la evaluación Common Criteria EAL5+ de la SCOS Java Card platform V1.0 (CCE-SAM002).* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 17/04/2015 hasta: 18/12/2015. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 18.150 €.

59. Contrato: *Study on the availability of trustworthy online privacy tools for the general public, D-COD-15-T16.* Empresa/Administración financiadora: European Union Agency for Network and Information Security (ENISA). Entidad participante: CSIC. Duración, desde: 16/03/2015 hasta: 15/09/2015. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4. Importe total del proyecto: 24.480 €. `https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-tools-for-the-general-public`.

60. Contrato: *Revision of the AVA report corresponding to the evaluation of the SPI Flash Memory product W75F32W carried out by LGAI.* Empresa/Administración financiadora: Winbond Electronics Corporation. Entidad participante: CSIC. Duración, desde: 19/02/2015 hasta: 19/09/2015. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 18.150 €.

61. Contrato: *Revisión del análisis de vulnerabilidades y de las pruebas de penetración correspondientes a la evaluación Common Criteria de la S3FW9FG Secure 32-bit RISC Microcontroller for Smart Card.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 13/02/2015 hasta: 19/07/2015. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 4. Importe total del proyecto: 6.050 €.

62. Contrato: *Revisión del análisis de vulnerabilidades y de las pruebas de penetración correspondientes a la evaluación Common Criteria del DNI 3.0.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 09/12/2014 hasta: 19/07/2015. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 18.150 €.

63. Contrato: *Asistencia técnica 2014 para la evaluación de la seguridad de productos criptográficos.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010314031800. Entidad participante: CSIC. Duración, desde: 02/12/2014 hasta: 15/12/2014. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 49.973 €.

64. Contrato: *New directions in securing personal data, D-COD-14-T21.* Empresa/Administración financiadora: European Union Agency for Network and Information Security (ENISA). Entidades participantes: everis Aeroespacial y Defensa, CSIC. y Universidad Politécnica de Madrid. Duración, desde: 25/09/2014 hasta: 15/03/2015. Investigador responsable: L. Hernández Encinas. Importe total del proyecto: 5.376 €.

65. Contrato: *Revisión de la ST y del informe de AVA para una evaluación de la tarjeta inteligente TC-FNMT v1.0.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 22/09/2014 hasta: 10/02/2015. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 18.150 €.

66. Contrato: *Revisión del informe de AVA para una evaluación de smartcard de identificación personal.* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 11/12/2013 hasta: 30/05/2014. Investigador responsable: A. Martín Muñoz. Nº de investigadores participantes: 4. Importe total del proyecto: 22.990 €.

67. Contrato: *Evaluación de un criptosistema de tipo caótico desarrollado por la empresa ENIGMEDIA S.L..* Empresa/Administración financiadora: ENIGMEDIA S.L. Entidades participantes: CSIC. Duración, desde: 20/02/2013 hasta: 15/06/2013. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 12.100 €.

68. Contrato: *Revisión del informe de AVA para una evaluación Common Criteria EAL4+ (AVA_ VAN.5 y ALC_ DVS.2).* Empresa/Administración financiadora: LGAI Technological Center S.A. Entidad participante: CSIC. Duración, desde: 17/10/2012 hasta: 31/12/2012. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 12.100 €.

69. Contrato: *Asistencia técnica para el apoyo al Centro Criptológico Nacional en temas cripto 2012.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010312026800. Entidad participante: CSIC. Duración, desde: 04/10/2012 hasta: 20/12/2012. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 70.000 €.

70. Contrato: *Asistencia técnica 2011 en materia de evaluación de la seguridad de productos criptográficos.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010311012300. Entidad participante: CSIC. Duración, desde: 10/05/2011 hasta: 31/12/2011. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 7. Importe total del proyecto: 85.000 €.

71. Contrato: *Análisis de Soluciones Criptográficas.* Empresa/Administración financiadora: Ferrovial Corporación S.L. Entidad participante: CSIC. Duración, desde: 11/10/2011 hasta: 31/12/2011. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 47.200 €.

72. Prestación de servicio: *Servicio de realización de la Guía Técnica de Seguridad del Esquema Nacional de Seguridad (ENS) "Criptología de empleo en el Esquema Nacional de Seguridad".* Empresa/Administración financiadora: Ministerio de la Presidencia, Secretaría de Estado para la Función Pública, Expediente Nº: 460/10. Entidad participante: CSIC. Duración, desde: 20/09/2010 hasta: 20/12/2010. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 14.500 €.

73. Contrato: *Asistencia técnica en materia de evaluación de la seguridad de productos criptográficos.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Expediente: 3010310022100. Entidad participante: CSIC. Duración, desde: 30/06/2010 hasta: 31/12/2010. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 95.000 €.

74. Prestación de servicio: *Políticas y recomendaciones sobre seguridad en algoritmos y parámetros criptológicos, y Métodos formales.* Empresa/Administración financiadora: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Nº Referencia: 0102061000060. Entidad participante: CSIC. Duración, desde: 01/04/2010 hasta: 30/06/2010. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 5. Importe total del proyecto: 10.000 €.

75. Contrato: *SEGUR@: Seguridad y Confianza en la Sociedad de la Información.* Empresa financiadora: Telefónica I+D (Ministerio de Turismo, Industria y Comercio, CENIT-2007 2004). Duración, desde: 2007 hasta: 2010. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 6. Importe total del proyecto: 684.418,56 €.

76. Contrato: *HESPERIA: Homeland security: Tecnologías para la seguridad integral en espacios públicos e infraestructuras.* Empresa/Administración financiadora: Sistemas Avanzados de Control (Ministerio de Turismo, Industria y Comercio). Duración, desde: 2006 hasta: 2009. Investigador responsable: A. Fúster Sabater. Nº de investigadores participantes: 6. Importe total del proyecto: 563.666,91 €.

77. Contrato: *Evaluación de la seguridad de los algoritmos de cifrado e identificación en telefonía GSM y recomendaciones para su mejora.* Empresa/Administración financiadora: AIRTEL móvil, S.A. Entidades participantes: CSIC, Universidades de Málaga y Salamanca. Duración, desde: 1999 hasta: 2000. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 7. Importe total del proyecto: 1.000.000 Pts.

78. Contrato: *Security evaluation of the version 2.1 of the "Common Electronic Purse Specifications", developed by CEPSCO.* Empresa financiadora: VISA INTERNATIONAL, California, (USA). Duración: 01-septiembre-1999 hasta 30-septiembre-1999. Importe total del proyecto: 6.300 $.

79. Contrato: *Security evaluation of the Common Electronic Purse Specification (CEPS).* Empresa financiadora: VISA INTERNATIONAL, California, (USA). Entidades participantes: CSIC, Universidad de Salamanca. Duración, desde: 15-diciembre-1998 hasta: 15-marzo-1999. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 5. Importe total del proyecto: 17.000 $.

80. Contrato: *Security evaluation of the VISA CASH electronic purse, Model TIBC, Designed by SERMEPA.* Empresa: VISA INTERNATIONAL, California, (USA). Entidades participantes: CSIC, Universidad de Salamanca. Duración, desde: 1-julio-1998 hasta: 31-julio-1998. Investigador responsable: F. Montoya Vitini. Nº de investigadores participantes: 5. Importe total del proyecto: 10.000 $.

81. Contrato: *Análisis comparado del curriculum de Matemáticas (nivel medio) en los países iberoamericanos.* Empresa/Administración financiadora: Secretaría de Estado de Educación, CIDE. Entidades participantes: Universidad de Salamanca. Duración, desde: 1992 hasta: 1993. Investigador responsable: L. Hernández Encinas. Nº de investigadores participantes: 3. Importe total del proyecto: 895.000 Pts.

Contratos con empresas/organismos internacionales	13
Contratos con empresas/organismos nacionales	65
Importe ingresado como IP	3.554.692,29 €

Patentes y Modelos de utilidad

1. G. Álvarez Marañón, V. Fernández Mármol, L. Hernández Encinas, F. Montoya Vitini, A. Orúe López, G. Pastor Dégano and M. Romera García, *Method and system for generating unpredictable pseudo-random numbers*. Nº. de patente Europa: 2009852480. Fecha solicitud: 23/10/2012. Fecha publicación: 19/12/2012. Nº. de patente EE.UU: 13643662. Fecha solicitud: 05/02/2013. Fecha publicación: 23/05/2013. Telefónica, S.A. (Licenciada) `https://register.epo.org/application?number=EP09852480`,
`http://www.patentbuddy.com/Patent/20130129088`.

2. F. Montoya Vitini, A. Orúe López, A. Guerra Estévez, L. Hernández Encinas, A. Martín Muñoz, y M. Soto Rodríguez, *Método y sistema para mejorar la sincronización de cifrados de flujo*. Nº de publicación: ES2409458. Clasificación internacional: H04L9/00. País de prioridad: España. Entidad solicitante: Telefónica, S.A. (Licenciada). Fecha de publicación de la concesión: 26/06/2013.

3. L. Hernández Encinas, J. Muñoz Masqué, R. Durán Díaz, F. Montoya Vitini, F. Hernández Álvarez, V. Gayoso Martínez, A. Martín Muñoz, y D. Prieto Marqués, *Método para cifrar y descifrar información*. Nº de solicitud de patente: P201130840. Clasificación internacional: H04L 9/30. País de prioridad: España. Entidad solicitante: Telefónica, S.A. (Licenciada). Fecha de publicación: 02/07/2013. Fecha de concesión: 16/04/2014.

4. L. Hernández Encinas, J. Muñoz Masqué, R. Durán Díaz, V. Gayoso Martínez, A. Martín Muñoz, V. Fernández Mateos, David Prieto Marqués, and F. Hernández Álvarez, *Método para realizar una firma digital de grupo*. Nº de solicitud de patente: P201130779. País de prioridad: España. Clasificación internacional: H04L 9/32. Entidad solicitante: Telefónica, S.A. (Licenciada) . Fecha de publicación: 15/04/2013. Fecha de concesión: 17/03/2014.

5. L. Hernández Encinas, J. Muñoz Masqué, R. Durán Díaz, F. Hernández Álvarez, and V. Gayoso Martínez, *Procedimiento para una firma digital múltiple*. Nº de solicitud de patente: P201130777. Fecha de solicitud: 13/05/2011. País de prioridad: España. Clasificación internacional: H04L 9/32. Entidad solicitante: Telefónica, S.A. (Licenciada). Fecha de publicación: 15/04/2013. Fecha de concesión: 04/03/2014.

6. L. Hernández Encinas, J. Muñoz Masqué y A. Queiruga Dios, *Procedimiento y dispositivo de encriptación mediante un criptosistema tipo RSA*. Nº de publicación: 2 217 959. Clasificación Internacional: H04L 9/30, H04L 9/328. País de prioridad: España. Entidad solicitante: Telefónica, S.A. (Licenciada). Fecha de publicación de la concesión: 01/02/2006.

7. L. Hernández Encinas, G. Álvarez Marañón y A. Martín del Rey, *Procedimiento y dispositivo para dividir de forma secreta, compartir y recuperar imágenes*. Nº de publicación: 2 238 168. Clasificación Internacional: G06T 1/00, H04N 1/44, H04N 7/16, H04L 9/22. País de prioridad: España. Entidad titular: CSIC. y Universidad de Salamanca. Fecha de publicación de la concesión: 01/11/2006.

8. L. Hernández Encinas y G. Álvarez Marañón, *Procedimiento y dispositivo de encriptación de imágenes mediante un criptosistema gráfico simétrico*. Nº de publicación: 2 238 151, Nº de solicitud: 200301902. Clasificación Internacional: H04L 9/22, H04L 9/28, H04L 29/06, G09C 1/00, H04N 1/44, H04N 7/167. País de prioridad: España. Entidad titular: CSIC. Fecha de concesión: 01/11/2006.

9. L. Hernández Encinas y A. Martín del Rey, *Método y aparato para el cifrado de imágenes digitalizadas*. Nº de patente: P200201500. País de prioridad: España. Entidad titular: CSIC. Fecha de publicación de la concesión: 28/06/2002.

Estancias en Centros extranjeros (continuadas superiores a un mes)

(D = doctorado, P = postdoctoral, I = invitado, C = contratado, O = otras)

1. Centro: *Department of Discrete and Statistical Sciences* (I), Auburn University. Localidad: Auburn, Alabama (USA). Fecha: 1997. Duración: 12 semanas. Tema: Criptografía de clave pública. Curvas elípticas e hiperelípticas. Profesor: Alfred Menezes.

2. Centro: *Department of Discrete and Statistical Sciences* (I), Auburn University. Localidad: Auburn, Alabama (USA). Fecha: 1993. Duración: 8 semanas. Tema: Criptografía de clave pública y aplicaciones. Profesor: Alfred Menezes.

Contribuciones a Congresos[2]

1. V. Sarasa Laborda, M.A. González de la Torre, L. Hernández-Álvarez y L. Hernández Encinas, Implementación del algoritmo de Shor para la factorización de $N = 21$, *XVIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2024)*, León, Octubre 23–25, 2024.

2. F. Contreras Alcalá, M.A. González de la Torre, and Hernández Encinas, L.L. Hernández Encinas, Fault Injection Attacks against RSA-CRT Digital Signature, *V International Conference on Mathematics and Its Applications in Science and Engineering (ICMASE 2024)*, Proc. Mathematical Methods for Engineering Applications: ICMASE 2024, 978-3-031-84150-7, Springer Nature, D.M.L.D. Rasteiro, F. Yilmaz, A. Queiruga-Dios, J. Martín Vaquero, and I. Mierlus Mazilu (Eds.), Coimbra (Portugal), September 16–18, 2024.

3. D. García Lleyda, V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and O. Castillo Campo, Performance Analysis of NTT Algorithms, Proc. *International Joint Conference 17th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2024), 15th International Conference on European Transnational Education (ICEUTE 2024)*, H. Quitián et al. (Eds.), Springer, Lecture Notes in Networks and Systems 957, 168–178, ISBN 978-3-031-75016-8, Salamanca, octubre 2024, `https://doi.org/10.1007/978-3-031-75016-8_16`.

4. Diego Rojas Rodríguez and Luis Hernández Encinas, Poster "Analysis of the Crystals-Kyber Implementation", Meetings on Computer Algebra and Applications (EACA 2024), Satellite conference of the 9th European Congress of Mathematics (9ECM), June 26–28, 2024, El Escorial, Madrid (`https://eventos.ucm.es/_files/_event/_104844/_editorFiles/file/Book-of-abstracts.pdf`).

5. E. Iglesias Hernández, L. Hernández-Álvarez L. Hernández Encinas y J. I. Sánchez García, Análisis comparativo de las firmas digitales postcuánticas basadas en retículos, Actas de las *IX Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2024)*, 2024, 404–411, Sevilla 27–39 mayo, 2024, ISBN: 978-84-09-62140-8, `https://idus.us.es/handle/11441/160623`.

6. M.A. González de la Torre, V. Sarasa Laborda, L. Hernández-Álvarez, I. Morales Sandoval y L. Hernández Encinas, Ataques por canal lateral contra AES mediante correlación de consumo de potencia, *IX Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2024)*, 2024, 420–427, Sevilla 27–39 mayo, 2024, ISBN: 978-84-09-62140-8, `https://idus.us.es/handle/11441/160773`.

7. Aida García-Callejo, Ventura Sarasa-Laborda, Luis Hernández-Encinas, and Verónica Fernández, QKD authentication using quantum-safe lightweight cryptography: Analysis and Use Cases, poster at the 10th ETSI/IQC Quantum Safe Cryptography Event, May 14–16, 2024, Singapore.

8. L. Hernández Encinas, Futuros Estándares de la Criptografía Postcuántica, Congreso Bienal de la Real Sociedad Matemática Española (RSME), Sesión especial de Criptografía, pág. 115, Pamplona, 23 de enero 2024, `https://2024.bienalrsme.com/sites/default/files/BienalRSME2024_LIBRO_19enero.pdf`

9. L. Hernández Encinas y V. Sarasa Laborda, Acerca del nuevo estándar de criptografía ligera, ASCON, XVII Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, noviembre 28–30, 2023, `https://jornadas.ccn-cert.cni.es/es/programa/xvii-jornadas-ccn-cert/ponencia/acerca-del-nuevo-estandar-de-criptografia-ligera-ascon`, `https://jornadas.ccn-cert.cni.es/es/programa/xvii-jornadas-ccn-cert`

10. Diego Rojas Rodríguez y Luis Hernández Encinas, Análisis de la implementación de referencia de la propuesta de criptografía postcuántica CRYSTAL-Kyber, Actas *DESEi+d 2023: IX Congreso Nacional de I+D en Defensa y Seguridad*, Cartagena, 14–16 Noviembre, 2023, (aceptado y en prensa).

11. L. Hernández-Álvarez, M.A. González de la Torre, E. Iglesias Hernández, and L. Hernández Encinas. How to attack a galaxy: from Star Wars to Star Trek, Proc. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Security and Management (SAM'23)*, IEEE, 2347–2354. ISBN: 979-8-3503-2759-5, Las Vegas (USA), July 24–27, 2023, `https://doi.org/10.1109/CSCE60160.2023.00381`

[2]Como es habitual en Matemáticas, los autores se ordenan alfabéticamente por apellidos: `https://www.ams.org/profession/leaders/culture/JointResearchandItsPublicationfinal.pdf`

12. O. Castillo Campo, V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz and R. Álvarez Fernández, State of the art of cybersecurity in cooperative, connected and automated mobility, Proc. *International Joint Conference 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) 13th International Conference on EUropean Transnational Education (ICEUTE 2022)*, P. García Bringas et al. (Eds.), Springer, Lecture Notes in Networks and Systems 523, 104–113, ISBN 978-3-031-18408-6, Salamanca, Septiembre 5–7, 2022, https://doi.org/10.1007/978-3-031-18409-3_11, https://link.springer.com/chapter/10.1007/978-3-031-18409-3_11

13. M.A. González de la Torre and L. Hernández Encinas, About the Fujisaki-Okamoto Transformation in the Code-based Algorithms of the NIST Post-Quantum Call, Proc. *International Joint Conference 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) 13th International Conference on EUropean Transnational Education (ICEUTE 2022)*, P. García Bringas et al. (Eds.), Springer, Lecture Notes in Networks and Systems 523, 75–85, ISBN 978-3-031-18408-6, Salamanca, Septiembre 5–7, 2022, https://doi.org/10.1007/978-3-031-18409-3_8, https://link.springer.com/chapter/10.1007/978-3-031-18409-3_8

14. M.A. González de la Torre, L. Hernández Encinas and J.I. Sánchez García, Comparative analysis of lattice-based post-quantum cryptosystems, *XVII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2022)*, Actas 121–126, D. Sadornil Renedo (Ed.), Ediciones Universidad de Cantabria, ISBN: 978-84-19024-14-5, Santander, Octubre 19–21, 2022, https://recsi2022.unican.es/wp-content/uploads/2022/10/LibroActas-978-84-19024-14-5.pdf

15. L. Hernández-Álvarez, S. Caputo, L. Mucchi, and L. Hernández Encinas, EEG Data for User Authentication with Multi-Class and One-Class Classifiers, *VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2022)*, Actas 205–208, J. M. de Fuentes, L. González, J. C. Sancho, A. Ayerbe and M. L. Escalante (Eds.), ISBN: 978-84-88734-13-6, Bilbao, Junio 27–29, 2022, https://2022.jnic.es/Actas_JNIC_2022_v11.pdf.

16. M. A. González de la Torre, L. Hernández Encinas, and A. Queiruga Dios, About the FrodoKEM lattice-based algorithm, *VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'2022)*, Actas 253–256, J. M. de Fuentes, L. González, J. C. Sancho, A. Ayerbe and M. L. Escalante (Eds.), ISBN: 978-84-88734-13-6, Bilbao, Junio 27–29, 2022, https://2022.jnic.es/Actas_JNIC_2022_v11.pdf.

17. A. Queiruga-Dios, J. J. Bullón Pérez and L. Hernández Encinas, Self-Sovereign Identity in University Context, Proc. *31st Conference of Open Innovations Association (FRUCT)*, 2022, 259–264, https://doi.org/10.23919/FRUCT54823.2022.9770913, https://ieeexplore.ieee.org/document/9770913, Helsinki, Finland, April 27–29, 2022.

18. J. Espinosa García, L. Hernández Encinas and A. Peinado Domínguez, Challenges and Competences in Master Degrees from a Comprehensive Security Perspective, *14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational (CISIS 2021 and ICEUTE 2021)*, Advances in Intelligent Systems and Computing 1400, 402–414, J.J. Gude Prego, J. Gaviria de la Puerta, P. García Bringas, H. Quintián, E. Corchado (Eds.), ISBN: 978-3-319-67179-6, https://doi.org/10.1007/978-3-030-87872-6_40, Bilbao (Spain), September 22–24, 2021. Core B.

19. M. Conde Pena, L. Hernández Encinas, R. Durán Díaz, J.-C. Faugère, L. Perret. Criptoanálisis del esquema de dinero cuántico de clave pública de Aaronson y Christiano, *XVI Reunión Española de Criptología y Seguridad de la Información (RECSI 2020)*, Actas 25–30, J.M. Miret y F. Sebé (Eds.), ISBN: 978-84-09-29150-2, Lérida, Abril 14–16, 2021, http://www.recsi2020.udl.cat/proceedings, http://hdl.handle.net/10261/241868.

20. V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz, A Study of the Reconciliation Mechanism of NewHope, Proc. *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS'2020)*, Advances in Intelligent Systems and Computing 1267 (2020), 361–370, A. Herrero, C. Cambra, D. Urda, J.Sedano, H. Quintián, E. Corchado (Eds.), ISBN: 978-3-030-57804-6, https://doi.org/10.1007/978-3-030-57805-3, Burgos (Spain), September 16–18, 2020. Core B.

21. V. Gayoso Martínez, L. Hernández Encinas, A.Martín Muñoz, and A. Queiruga Dios, Using Freeware Mathematical Software in Calculus Classes, Proc. *International Conference on Mathematics and Its Applications in Science and Engineering (ICMASE 2020)*, 243–252, ISBN: 978-84-1311-459-0, `https://doi.org/10.14201/0AQ0302`, `https://doi.org/10.1007/978-3-030-57805-3`, `http://hdl.handle.net/10261/242692`, Ankara (Turkey), July 9–10, 2020.

22. R. Durán Díaz, L. Hernández-Álvarez, L. Hernández Encinas, and A. Queiruga-Dios. Chor-Rivest Knapsack Cryptosystem in a Post-Quantum World, Proc. 2020 International Conference on Security and Management (Worldcomp-SAM'20). In Transactions on Computational Science and Computational Intelligence, *Advances in Security, Networks, and Internet of Things*, 67–83, ISBN: 978-3-030-71016-3, `https://doi.org/10.1007/978-3-030-71017-0_6`, `http://hdl.handle.net/10261/246777`, Las Vegas (USA), July 27–30, 2020.

23. V. Gayoso Martínez, A. Hernández Encinas, L. Hernández Encinas, and A. Martín Muñoz. 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.

24. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, 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.

25. V. Gayoso Martínez y L. Hernández Encinas. 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`

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

27. Hadrián Rodríguez César, Víctor Gayoso Martínez, Luis Hernández Encinas, and Agustín Martín Muñoz. Format-Preserving Encryption: image encryption under FF1 scheme, *Research Fora International Conference*, Proc. 1–4, México City (México), September 28–29, 2019, ISBN: 978-93-87405-198-9.

28. I. Querejeta Azurmendi, L. Hernández Encinas, D. Arroyo and J. Lopez Hernández-Ardieta, An internet voting proposal towards improving usability and coercion resistance, *12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019)*, Proc. 155–164, Sevilla (Spain), May 13–15, Core B.

29. A.B. Orúe López, A. Blanco Blanco, A. Martín Muñoz, V. Gayoso Martínez, O. Martínez Graullera, L. Hernández Encinas and F. Montoya Vitini, 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, Core B.

30. D. Arroyo Guardeño, Á. Rezola Borrego y L. Hernández Encinas. Principales problemas de seguridad en los smart contracts de Ethereum, XII Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, Diciembre 12–13, 2018.

31. A. Blanco Blanco, V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini, y A.B. Orúe López. 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 3–5, 2018, `https://nesg.ugr.es/recsi2018/docs/ActasXVRECSI.pdf`.

32. I. Querejeta Azurmendi, J. López Hernández-Ardieta, y L. Hernández Encinas, Don't shoot the messenger. How a trusted channel may not be a necessary assumption for remote code-voting, *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, `http://2018.jnic.es/assets/Actas_JNIC2018.pdf`.

33. A. Blanco Blanco, J.M. de Fuentes, L. González-Manzano, L. Hernández Encinas, A. Martín Muñoz, J.L. Rodrigo Oliva, and J.I. Sánchez García. A Framework for Acquiring and Analyzing Traces from Cryptographic Devices. *13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2017)*, Niagara Falls (Canada), October 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, **239**, 283–300 (2018), Lin X., Ghorbani A., Ren K., Zhu S., Zhang A. (Eds). ISBN: 978-3-319-78815-9, Springer, Cham, `https://doi.org/10.1007/978-3-319-78816-6_20`. Core B.

34. L. Hernández Encinas, V. Gayoso Martínez y D. Arroyo Guardeño, 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`

35. A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz y B. Alarcos Alcázar, Generación de Valores Intermedios de Forma Paralela en Ataques DPA, *IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2017)*, Actas 67–74, ISBN: 978-950-23-2811-9, A.E. Dams, H.A. Pagola, L.E. Sánchez Crespo y J. Ramió Aguirre (Eds.), Buenos Aires (Argentina), Noviembre 2017.

36. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and M. Mojica López, 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: 978-950-23-2811-9, A.E. Dams, H.A. Pagola, L.E. Sánchez Crespo y J. Ramió Aguirre (Eds.), Buenos Aires (Argentina), Noviembre 2017.

37. M. Mójica López, J. L. Rodrigo Oliva, V. Gayoso Martínez, L. Hernández Encinas y A. Martín Muñoz, Análisis de la privacidad de WhatsApp Messenger, *Décima sexta Conferencia Iberoamericana en Sistemas, Cibernética e Informática (CISCI 2017)*, Actas 109–114, ISBN: 978-1-941763-63-6, Orlando (Florida, USA), July 8–11, 2017.

38. I. Querejeta Azurmendi, J. López Hernández-Ardieta, V. Gayoso Martínez, L. Hernández Encinas, D. Arroyo Guardeño, 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.

39. L. González-Manzano, J.M. de Fuentes, S. Pastrana, P. Peris-Lopez, L. Hernández-Encinas, Resumen de un protocolo de agregación privada en el Internet de las cosas: PAgIoT, *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.

40. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz and J. Zhang, Breaking a Hitag2 Protocol with Low Cost Technology, *3rd International Conference on Information Systems Security and Privacy (ICISSP'2017)*, Proc. 579–584, P. Mori, S. Furnell and O. Camp (Ed.), ISBN: 978-989-758-209-7, Porto (Portugal), February 19–21, 2017.

41. O. Delgado, D. Arroyo, J. Díaz y L. Hernández, Blockchain: Usos y Abusos, X Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, Diciembre 13–14, 2016 (`https://www.youtube.com/watch?v=8OFRb5PJZ_o`)

42. A. Queiruga-Dios, G. Rodríguez Sánchez, A. Hernández Encinas, A. Martín del Rey, J. Martín Vaquero, and L. Hernández Encinas, Case study: Malware propagation models for undergraduate engineering students, *Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'16)*, Proc. 931–936, F.J. García-Peñalvo (Ed.), ISBN: 978-1-4503-4747-1, Salamanca (Spain), November 2–4, 2016.

43. R. Durán Díaz, V. Gayoso Martinez y L. Hernández Encinas, Generación de primos demostrables: implementación y resultados, *XIV Reunión Española de Criptología y Seguridad de la Información (RECSI 2016)*, Actas 58–63, P.L. Ferrer Gomila y M.F. Hinarejos Campos (Eds.), ISBN: 978-84-608-9470-4, Mahón, Octubre 26–28, 2016.

44. A.B. Orúe, A. Fúster, V. Fernández, F. Montoya, L. Hernández y A. Martín, 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.

45. V. Gayoso Martínez, L. Hernández Encinas, A. Martín del Rey and R. Durán Díaz, Análisis de los métodos de generación de curvas elípticas seguras, *Segundas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)*, Actas 87–93, ISBN: 978-84-608-8070-7. Granada, Junio 15–17, 2016.

46. J.D. Hernández Guillén, A. Martín del Rey and L. Hernández Encinas, 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: 978-84-608-8070-7. Granada, Junio 15–17, 2016.

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

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

49. Y. Janati, J. Munilla, A. Peinado, A. Ortiz-García, L. Hernández Encinas, and R. Durán Díaz, 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.

50. V. Gayoso Martínez, L. Hernández Encinas and Seok-Zun Song, 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`

51. D. Arroyo Guardeño, V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz, Using smart cards for authenticating in public services: A comparative study, *International Workshop on Computational Intelligence in Security for Information Systems (CISIS'15)*, Proc. International Join Conference CISIS'15-ICEUTE'15, Advances in Intelligent Systems and Computing 437–446, 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_37`

52. L. Hernández Encinas y A. Martín Muñoz, Exfiltración por canal lateral. ¿Son las certificaciones la solución?, IX Jornadas de Seguridad TIC del CCN-CERT, Centro Criptológico Nacional, Centro Nacional de Inteligencia, Madrid, Diciembre 10–11, 2015 `https://www.youtube.com/watch?v=Wu2nTldXk3Q`

53. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, J.M. de Fuentes, L. González Manzano, 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.

54. V. Gayoso Martínez, L. Hernández Encinas, and A. Martín Muñoz, Securing network communications with TLS and IPsec, *28th International Conference on Information Technologies (InfoTech-2014)*, Proc. 123–131, R. Romansky (Ed.), ISSN: 1314-1023, Varna (Bulgaria), September 2014.

55. V. Gayoso Martínez, F. Hernández Álvarez, and L. Hernández Encinas, La transformada de Walsh-Hadamard 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.

56. V. Gayoso Martínez, F. Hernández Álvarez, and L. Hernández Encinas, 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 1-60132-285-2, Las Vegas (USA), July 2014. Core C.

57. V. Gayoso Martínez, F. Hernández Álvarez, and L. Hernández Encinas, 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 2014. Core C.

58. G. Rodríguez Sánchez, A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey, and A. Queiruga Dios, 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.

59. V. Gayoso Martínez and L. Hernández Encinas, Developing ECC applications in Java Card, *Information Assurance and Security*, Proc. 114–120, ISBN: 978-9962-676-43-0, Tunez (Tunisia), December 2013.

60. V. Gayoso Martínez, L. Hernández Encinas y A. Martín Muñoz, La tarjeta de identidad española como método de autenticación en redes sociales, *VII Congreso Iberoamericano de Seguridad Informática (CIBSI 2013)*, Actas 16–26, ISBN: 978-9962-676-43-0, Ciudad de Panamá (Panamá), Octubre 2013.

61. A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz y B. Alarcos Alcázar, Diseño de un conjunto de herramientas software para ataques por canal lateral, *VII Congreso Iberoamericano de Seguridad Informática (CIBSI 2013)*, Actas 32–44, ISBN: 978-9962-676-43-0, Ciudad de Panamá (Panamá), Octubre 2013.

62. V. Gayoso Martínez and L. Hernández Encinas, Implementing the ECC Brainpool curve generation procedure using open source software, *The 2013 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2013 International Conference on Security and Management (Worldcomp-SAM'13)*, Proc. 162–167, K. Daimi and H.R. Arabnia (Eds.), Las Vegas (USA), July 2013, `http://world-comp.org/proc2013/sam.html`. Core C.

63. V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and J.I. Sánchez García, Identification by means of a national ID card for wireless services, *Global Wireless Summit 2013*, Proc. 5 pp., P. Pruthi and H.V. Poor (Eds.), ISBN: 978-87-92982-52-0, Atlantic City (USA), June 2013.

64. A. Queiruga-Dios, A. Hernández Encinas, I. Visus Ruíz, L. Hernández Encinas, V. Gayoso Martínez, and E. Yuste Martínez, A learning resource to acquire engineering skills through programming languages, *5th World Conference on Educational Sciences (WCES 2013)*, Rome (Italy), February 2013.

65. V. Gayoso Martínez, L. Hernández Encinas, J. Martín Vaquero, A. Queiruga Dios, J. Pueyo Candil, A new approach for obtaining the bachelor's degree by technology professionals, *5th World Conference on Educational Sciences (WCES 2013)*, Rome (Italy), February 2013.

66. A. Fuentes Rodríguez, L. Hernández Encinas, A. Martín Muñoz, and B. Alarcos Alcázar, 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`. Core B.

67. V. Gayoso Martínez, L. Hernández Encinas, A. Hernández Encinas, and A. Queiruga Dios, 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`. Core B.

68. M. Conde Pena, R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué, The isomorphism of polynomials problem applied to multivariate quadratic cryptography, *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13*, Proc. 567–576, 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_58`. Core B.

69. L. Hernández Encinas y A. Peinado Domínguez, Una propuesta para el uso de códigos QR en la autenticación de usuarios, *XII Reunión Española de Criptología y Seguridad de la Información (XII RECSI)*, Actas 387–392, U. Zurutuza, R. Uribeetxeberria e I. Arenaza-Nuño (Eds.), ISBN: 978-84-615-9933-2, San Sebastián (Spain), Septiembre 2012.

70. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué, Comments on a cryptosystem proposed by Wang and Hu, *International Joint Conference CISIS'12-ICEUTE'12-SOC'12 (CISIS'12)*, Proc. 57–65, A. Herrero, V. Snášel, A. Abraham, I. Zelinka, B. Baruque, H. Quintián, J.L. Calvo, J. Sedano, and E. Corchado (Eds.), Springer, ISBN: 978-3-642-33018-6, Ostrava, Czech Republic, September 2012. `http://dx.doi.org/10.1007/978-3-642-33018-6_6`. Core B.

71. L. Hernández Encinas, A. Martín Muñoz and Jaime Muñoz Masqué, Divisors of $\binom{n}{2}$ and prime powers (Extended abstract), *Third Workshop on Mathematical Cryptology (WcM 2012)*, Proc. 62–65, Castro Urdiales, July 2012.

72. A. Queiruga Dios, V. Gayoso Martínez, A. Hernández Encinas, and Luis Hernández Encinas, The computer as a tool to acquire and evaluate skills in Math courses, *2012 International Conference on Computer Research and Development (ICCRD 2012)*, Proc. 65–69, A. Wu (Ed.). ISBN: 978-981-07-2087-2, Chengdu, China, May 2012.

73. F.J. Buenasmañanas Domínguez, A. Hernández Encinas, L. Hernández Encinas, and A. Queiruga Dios, Digital identity-based multisignature scheme implementation, *The First International Conference on Advanced Communications and Computation (INFOCOMP 2011)*, Proc. 42–45. C.-P. Rückemann, W. Christmann, and M. Pankowska (Eds.). ISBN: 978-1-61208-161-8, Barcelona, October 2011.

74. V. Fernández, M.J. García-Martínez, L. Hernández-Encinas, and A. Martín, Formal Verification of the Security of a Free-Space Quantum Key Distribution System, *The 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2011 International Conference on Security and Management (Worldcomp-SAM 2011)*, Proc. vol I, 32–38. H.R. Arabnia, M.R. Grimalia, G. Markowsky, and S. Aissi (Eds.). ISBN: 1-60132-196-1, Las Vegas (USA), July 2011, `http://world-comp.org/proc2011/sam.html`. Core C.

75. V. Gayoso Martínez, L. Hernández Encinas and C. Sánchez Ávila, Java Card implementation of the Elliptic Curve Integrated Encryption Scheme using prime and binary finite fields, *The 4th International Workshop on Computational Intelligence in Security for Information Systems (CISIS'11)*, A. Herrero and E. Corchado (Eds.), LNCS 6499, 160–167, ISBN: 978-3-642-21322-9, Torremolinos, June 2011. Core B.

76. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué, A group signature scheme based on the integer factorization and the subgroup discrete logarithm problems, *The 4th International Workshop on Computational Intelligence in Security for Information Systems (CISIS'11)*, A. Herrero and E. Corchado (Eds.), LNCS 6694, 143–150, ISBN: 978-3-642-21322-9, Torremolinos, June 2011. Core B.

77. R. Durán Díaz, L. Hernández Encinas and J. Muñoz Masqué, A multisignature scheme based on the SDLP and on the IFP, *The 4th International Workshop on Computational Intelligence in Security for Information Systems (CISIS'11)*, A. Herrero and E. Corchado (Eds.), LNCS 6694, 135–142, ISBN: 978-3-642-21322-9, Torremolinos, June 2011. Core B.

78. R. Durán Díaz, L. Hernández Encinas y J. Muñoz Masqué, Generación de primos: una perspectiva computacional, *XI Reunión Española de Criptología y Seguridad de la Información (XI RECSI)*, Actas 59–64, J. Domingo Ferrer et al. (Eds.), ISBN: 978-84-693-3304-4. Tarragona, Septiembre 2010.

79. V. Gayoso Martínez, F. Hernández Álvarez, L. Hernández Encinas, and C. Sánchez Ávila, A comparison of the standardized versions of ECIES, *Sixth International Conference on Information and Security (IAS 2010)*, Proc. 1–4. ISBN: 978-1-4244-7408-0. Atlanta (USA), August 2010, IEEE Catalog number: CFP1061C-CDR. Core C, `https://digital.csic.es/handle/10261/32674`

80. V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, A Java implementation of the Elliptic Curve Integrated Encryption Scheme, *The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2010 International Conference on Security and Management (Worldcomp-SAM 2010)*, Vol II, Proc. 495–501. H.R. Arabnia, K. Daimi, M.R. Grimalia and G. Markowsky (Eds.). ISBN: 1-60132-162-7. Las Vegas (USA), July 2010. Core C.

81. V. Gayoso Martínez, A. Hernández Encinas, L. Hernández Encinas, A. Queiruga Dios, and I. Visus Ruiz, Development of Capstone Projects on Secure Communications for Engineering Students, *The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2010 International Conference on Security and Management (Worldcomp-SAM 2010)*, Vol II, Proc. 516–520. H.R. Arabnia, K. Daimi, M.R. Grimalia and G. Markowsky (Eds.). ISBN: 1-60132-162-7. Las Vegas (USA), July 2010. Core C.

82. R. Durán Díaz, F. Hernández Álvarez, L. Hernández Encinas, and A. Queiruga Dios, A review of multisignatures based on RSA, *Proc. of The 4th International Information Security & Cryptology Conference (ISCTURKEY'10)*, 38–44. M. Alkan, S. Sağiroğlu, and E. Aklyildiz (Eds.). ISBN: 978-9944-0189-2-0. Ankara (Turkey), May 2010.

83. F. Hernández Álvarez and L. Hernández Encinas, Security Efficiency Analysis of a Biometric Fuzzy Extractor for Iris Templates, *The 2nd International Workshop on Computational Intelligence in Security for Information Systems (CISIS'09)*, AISC 63, 163–170. A. Herrero, P. Gastaldo, R. Zunino and E. Corchado (Eds.). ISBN: 978-3-642-04090-0. Burgos, Septiembre 2009. Core B.

84. V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, Elliptic curve cryptography. Java platform implementations, *International Conference on Information Technologies (InfoTech-2009)*, Proceedings of 23^{rd} *International Conference for Automation of Engineering and Research (SAER-2009)* 20–27. R. Romansky (Ed.). ISBN: 978-954-438-771-6. Varna (Bulgaria), September 2009.

85. F. Hernández Álvarez, L. Hernández Encinas, and C. Sánchez Ávila, Biometric fuzzy extractor scheme for iris templates, *The 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2009 International Conference on Security and Management (Worldcomp-SAM 2009)*, Vol II, Proc. 563–569. H.R. Arabnia and K. Daimi (Eds.). ISBN: 1-60132-125-2. Las Vegas (USA), July 2009. Core C.

86. R. Durán Díaz, F. Hernández Álvarez, and L. Hernández Encinas, Graphic multisecret sharing schemes with one-dimensional cellular automata, *The 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2009 International Conference on Security and Management (Worldcomp-SAM 2009)*, Vol II, Proc. 576–582. H.R. Arabnia and K. Daimi (Eds.). ISBN: 1-60132-125-2. Las Vegas (USA), July 2009. Core C.

87. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué, Quadratic discrete dynamics associated to quadratic maps in the plane, *International Conference on Computational and Mathematical Methods on Science and Engineering, (CMMSE-2009)*, vol. II, Proc. 437–448. J. Vigo-Aguiar (Ed.). ISBN: 978-84-612-9727-6. Gijón, Junio-Julio 2009.

88. L. Hernández Encinas y J. Muñoz Masqué, Criptografía con curvas hiperelípticas de género 2, Nuevos Avances en Criptografía y Codificación de la Información, *Congreso de la Real Sociedad Matemática Española (RSME 2009)*, Actas 87–96, ISBN: 978-84-8409-277-3, Oviedo, Febrero 2009.

89. A. Queiruga Dios, L. Hernández Encinas, D. Queiruga, Cryptography Adapted to the New European Area of Higher Education, *International Conference on Computational Science (ICCS 2008)*, M. Bubak, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), LNCS 5102, 706–714, ISBN: 978-3-540-69386-4. Kraków, Poland, June 2008. Core A.

90. F. Hernández Álvarez, L. Hernández Encinas y A. Queiruga Dios, Nuevos parámetros seguros para el criptosistema de Chor-Rivest e Implementación con Magma, *X Reunión Española de Criptología y Seguridad de la Información (X RECSI)*, Actas 101–109, L. Hernández y A. Martín (Eds.), ISBN: 978-84-691-5158-7. Salamanca, Septiembre 2008.

91. R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué, Computational aspects in the generation of higher-order safe primes, *International Conference on Information Technologies (InfoTech-2008)*, Proc. vol 2, 33–40. ISBN: 978-954-9518-56-6. Varna, Bulgaria, Septiembre 2008.

92. L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios, Algorithms to encrypt and decrypt messages with Magma, *International Conference on Computational and Mathematical Methods on Science and Engineering, (CMMSE-2008)*, Proc. 327–330. J. Vigo-Aguiar (Ed.). ISBN: 978-84-612-1982-7. La Manga, Murcia, June 2008.

93. A. Hernández Encinas, L. Hernández Encinas, and A. Queiruga Dios, New Teaching Resources to adapt Mathematics to the new European Area of Higher Education, *International Conference on Computational and Mathematical Methods on Science and Engineering, (CMMSE-2008)*, Proc. 323–326. J. Vigo-Aguiar (Ed.). ISBN: 978-84-612-1982-7. La Manga, Murcia, June 2008.

94. R. Durán Díaz, L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios, Generic intersection of orthogonal groups, *International Conference on Computational and Mathematical Methods on Science and Engineering, (CMMSE-2008)*, Proc. 231–235. J. Vigo-Aguiar (Ed.). ISBN: 978-84-612-1982-7. La Manga, Murcia, June 2008.

95. J. Espinosa García, L. Hernández Encinas, and A. Queiruga Dios, The new Spanish electronic identity card: DNI-e, *International Conference on Information Technologies (InfoTech-2007)*, Proceedings 77–82, vol I: Technological Aspects of the e-Governance and Data Protection, ISBN: 978-954-9518-41-2. Varna (Bulgaria), September 2007.

96. A. Queiruga Dios, L. Hernández Encinas, and J. Espinosa García, e-Learning: A case study of Chor-Rivest cryptosystem in Maple, *International Conference on Information Technologies (InfoTech-2007)*, Proceedings 107–114, vol I: Technological Aspects of the e-Governance and Data Protection, ISBN: 978-954-9518-41-2. Varna (Bulgaria), September 2007.

97. A. Queiruga Dios y L. Hernández Encinas, Proceso de enseñanza-aprendizaje específico: Algoritmos matemáticos y Criptográficos reutilizables, *I Congreso Internacional Escuela y TIC. IV Forum Novadors*, CD 1–10, ISBN: 978-84-690-6871-7. Alicante, Julio 2007.

98. A. Queiruga Dios y L. Hernández Encinas, Aprendizaje Activo de Criptografía: El Criptosistema de Chor-Rivest en MAPLE, *II^{as} Jornadas de Innovación Educativa. Las enseñanzas técnicas ante el reto del Espacio Europeo de Educación Superior*, Actas 426–433, ISBN: 978-84-7800-369-3. Zamora, Julio 2007.

99. A.B. Cabello, A. Hernández Encinas, L. Hernández Encinas y A. Martín del Rey, La diagonalización de matrices aplicada a la Ingeniería e implementada con Mathematica, *II^{as} Jornadas de Innovación Educativa. Las enseñanzas técnicas ante el reto del Espacio Europeo de Educación Superior*, Actas 754–759, ISBN: 978-84-7800-369-3. Zamora, Julio 2007.

100. J. García de Jalón de la Fuente y L. Hernández Encinas, La Criptografía como recurso matemático, *XIII Jornadas de Aprendizaje y Enseñanza de las Matemáticas (XIII JAEM)*, Actas 5 pp. ISBN: 978-84-934488-5-1. Granada, Julio 2007.

101. A. Hernández Encinas, L. Hernández Encinas, R. Álvarez Mariño, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez, Epidemiology through hexagonal cellular automata, *The Fifth International Conference on Engineering Computational Technology (ICECT 2006)*, B.H.V. Topping, G. Montero and R. Montenegro, (Eds.), Civil-Comp Press, Stirlingshire, United Kingdom, paper 34, 15 pp., 2006. ISBN: 1-905088-10-8. Las Palmas de Gran Canaria, Septiembre 2006. Core B.

102. A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez, Modelling the spread of a forest fire by using hexagonal cellular automata, *The Fifth International Conference on Engineering Computational Technology (ICECT 2006)*, Proc. paper 35, 14 pp., B.H.V. Topping, G. Montero and R. Montenegro, (Eds.), Civil-Comp Press. Stirlingshire,

United Kingdom, 2006. ISBN: 1-905088-10-8, Las Palmas de Gran Canaria, September 2006. Core B.

103. A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez, Symmetric block ciphers based on cellular automata, *The Fifth International Conference on Engineering Computational Technology (ICECT 2006)*, B.H.V. Topping, G. Montero and R. Montenegro, (Eds.), Civil-Comp Press, Stirlingshire, United Kingdom, paper 36, 14 pp., 2006. ISBN: 1-905088-10-8. Las Palmas de Gran Canaria, September 2006. Core B.

104. L. Hernández Encinas, J. Muñoz Masqué, and A. Queiruga Dios, Maple implementation of the Chor-Rivest cryptosystem, *International Conference on Computational Science (ICCS 2006)*, LNCS 3992, 438–445, ISBN: 3-540-34381-4. Reading, U.K., May 2006. Core A.

105. L. Hernández Encinas, J. Muñoz Masqué y A. Queiruga Dios, Análisis del criptosistema de Chor-Rivest con parámetros primos, *IX Reunión Española de Criptología y Seguridad de la Información (IX RECSI)*, Actas 548–561, J. Borrell y J. Herrera (Eds.), ISBN: 849-7885-02-3. Barcelona, 2006, Septiembre 2006.

106. J. Crespo Sánchez, J. Espinosa García, L. Hernández Encinas, H. Rifá Pous y M. Torres Hernández, Hacia una nueva identificación electrónica del ciudadano: el DNI-e, *IX Reunión Española de Criptología y Seguridad de la Información (IX RECSI)*, Actas 660–673, J. Borrell y J. Herrera (Eds.), ISBN: 849-7885-02-3. Barcelona, Septiembre 2006.

107. A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey y G. Rodríguez Sánchez, Protocolo para la autenticación de mensajes mediante autómatas celulares, *IX Reunión Española de Criptología y Seguridad de la Información (IX RECSI)*, Actas 63–71, J. Borrell y J. Herrera (Eds.), ISBN: 849-7885-02-3. Barcelona, Septiembre 2006.

108. A.B. Cabello Pardos, A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey y G. Rodríguez Sánchez, Aplicaciones recreativas de los autómatas celulares, *9º Congreso Castellano Leonés de Educación Matemática*. Soria, Septiembre 2006.

109. A.B. Cabello Pardos, A. Hernández Encinas, L. Hernández Encinas y A. Martín del Rey, Aprendizaje activo de Métodos Numéricos con Mathematica, *I^{as} Jornadas de Innovación Educativa. Las enseñanzas técnicas ante el reto del Espacio Europeo de Educación Superior*, Actas 20–32, ISBN: 84-689-9304-2. Zamora, Julio 2006.

110. G. Alvarez, L. Hernández Encinas, A. Martín del Rey y J. Ramió Aguirre, Un nuevo esquema para el reparto de múltiples secretos, 3er *Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, Actas 247–258, R. Monge y J. Ramió (Eds.), ISBN: 956-7051-10-0. Valparaiso (Chile), Noviembre 2005.

111. G. Alvarez, A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez, A New Graphic Cryptosystem Based on One-Dimensional Memory Cellular Automata, *39th Annual 2005 IEEE International Carnahan Conference on Security Technology*, Proc. 200–203, L.D. Sanson (Ed.), ISBN: 0-7803-9245-0. Las Palmas de Gran Canaria, September 2005.

112. J. Espinosa García, L. Hernández Encinas, C. Sánchez Ávila and V. Gayoso Martínez, Elliptic Curve Cryptography: Java implementation issues, *39th Annual 2005 IEEE International Carnahan Conference on Security Technology*, Proc. 238–241. L.D. Sanson (Ed.), ISBN: 0-7803-9245-0. Las Palmas de Gran Canaria, September 2005.

113. L. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez, A CA-based protocol to authenticate images, *17th IMACS World Congress Scientific Computation, Applied Mathematics and Simulation (IMACS 2005)*, Proceedings, T3-R-00-0273, 6 pp. P. Borne, M. Berenjeb, N. Dangoumau and L. Lorimier (Eds.), ISBN: 2-915913-02-1. Paris, Septembre 2005.

114. R. Álvarez Mariño, L. Hernández Encinas, A. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez, Modelling Epidemics using Cellular Automata, *International Conference on Computational and Mathematical Methods on Science and Engineering, (CMMSE-2005)*, Proceedings 353–363. J. Vigo-Aguiar and B.A. Wade (Eds.). ISBN: 84-609-4844-7. Alicante, September 2005.

115. G. Álvarez Marañón, L. Hernández Encinas and A. Martín del Rey, A new secret sharing scheme for images based on additive 2-dimensional cellular automata, *Second Iberian Conference, Pattern Recognition and Image Analysis (IbPRIA 2005)*, LNCS 3522, 411–418, ISBN: 3-540-26153-2. Estoril (Portugal), 2005. Core C.

116. L. Hernández Encinas, A. Martín del Rey, and G. Rodríguez Sánchez, Integrity protection of digital images by means of MCA-based protocols, *IADAT-micv2005 International Conference on Multimedia, Image Processing and Computer Vision*, Proceedings, 250–254, International Association for the Development of Advances in Technology, Madrid, 2005. ISBN: 84-933971-5-6. Madrid, November 2005.

117. J. Espinosa García, V. Gayoso Martínez, L. Hernández Encinas y C. Sánchez Ávila, Sobre la clasificación de curvas hiperelípticas de género 2 definidas en cuerpos finitos, *I Congreso Español de Informática (SSI'2005), Simposio sobre Seguridad Informática (CEDI05)*, Actas 31–36, Thomson, Madrid. A. Peinado y P. Caballero (Eds.). ISBN: 84-9732-447-1. Granada, Septiembre, 2005.

118. V. Gayoso Martínez, C. Sánchez Ávila, J. Espinosa García y L. Hernández Encinas, Estado del arte de las implementaciones Java de criptografía de curva elíptica, *I Congreso Español de Informática (SSI'2005), Simposio sobre Seguridad Informática (CEDI05)*, Actas 127–134, Thomson, Madrid. A. Peinado y P. Caballero (Eds.). ISBN: 84-9732-447-1. Granada, Septiembre, 2005.

119. L. Hernández Encinas, Criptosistemas basados en curvas hiperelípticas, *Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA (MAT.ES 2005)*, Actas de la sesión especial "Tendencias actuales en la Criptología", 115–127, L. Hernández Encinas, A. Martín del Rey y G. Rodríguez Sánchez (Eds.). ISBN: 84-689-0117-2. Valencia, Abril, 2005.

120. L. Hernández Encinas and J. Muñoz Masqué, Isomorphism classes of hyperelliptic curves of genus 2 in characteristic 5, *Third International Conference on Information (Information 2004)*, Proceedings, 97–100, L. Li and K.K. Yen (Eds.). ISBN: 4-901329-02-2. Tokyo (Japón), 2004.

121. O. García Delgado, L. Hernández Encinas, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez, The reversibility problem of 150-Wolfram cellular automaton with periodic boundary conditions, *Third International Conference on Information (Information 2004)*, Proceedings, 101–104, L. Li and K.K. Yen (Eds.). ISBN: 4-901329-02-2. Tokyo (Japón), 2004.

122. A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey and G. Rodríguez Sánchez, A CA-based model for predicting forest fire spreading, *Fourth International Conference on Engineering Computational Technology (ICECT 2004)*, Proceedings, paper 5, 13 pp. B.H.V. Topping and C.A. Mota Soares (Eds.), Civil-Comp Press, Stirling, UK. ISBN: 0-948749-97-0. Lisboa (Portugal), Julio, 2004. Core B.

123. J. Espinosa García y L. Hernández Encinas, Una revisión de los criptosistemas de clave pública sobre curvas elípticas e hiperelípticas, *VIII Reunión Española de Criptología (VIII RECSI)*, Actas, 149–155, B. Ramos Álvarez y A. Ribagorda Garnacho (Eds.), Díaz de Santos, S.A., Madrid. ISBN: 84-7978-650-7. Leganés (Madrid), Septiembre, 2004.

124. G. Álvarez Marañón, L. Hernández Encinas y A. Martín del Rey, Un nuevo esquema umbral para imágenes, *VIII Reunión Española de Criptología (VIII RECSI)*, Actas, 259–267, B. Ramos Álvarez y A. Ribagorda Garnacho (Eds.), Díaz de Santos, S.A., Madrid. ISBN: 84-7978-650-7. Leganés (Madrid), Septiembre, 2004.

125. L. Hernández Encinas, A. Martín del Rey y G. Rodríguez Sánchez, Autómatas celulares reversibles, *IV Jornadas de Matemática Discreta y Algorítmica (IV JMDA)*, Actas, 315–322, Universidad Politécnica de Madrid. ISBN: 84-86189-98-5. Cercedilla (Madrid), 2004.

126. G. Álvarez Marañón, L. Hernández Encinas, A. Hernández Encinas, A. Martín del Rey and G. Rodríguez Sánchez, Graphic cryptography with pseudorandom bit generators and cellular automata, *7th International Conference Knowledge-Based Intelligent Information and Engineering Systems (KES 2003)*, LNAI 2773, 1207–1214, ISBN: 3-540-40803-7. Oxford (UK), 2003. Core B.

127. L. Hernández Encinas, J. Muñoz Masqué y A. Queiruga Dios, Algoritmo para obtener un módulo RSA con clave privada grande, *2º Congreso Iberoamericano de Seguridad Informática (CIBSI 2003)*, Actas, 292–301. R. Menchaca, J. Ramió, L. Hernández, G. Valázquez (Eds.) ISBN: 970-36-010409. México D.F., 2003.

128. S. Petrovic, A. Fúster y L. Hernández, Un ataque sobre texto cifrado para una clase de generadores de secuencias pseudoaleatorias, *2º Congreso Iberoamericano de Seguridad Informática (CIBSI 2003)*, Actas, 448–462, R. Menchaca, J. Ramió, L. Hernández, G. Velázquez (Eds.). ISBN: 970-36-010409. México D.F., 2003.

129. J.M. Chamoso Sánchez, L. Hernández Encinas, J. Martín Lalanda, R. López Fernández, M. Rodríguez Sánchez, M. Rodríguez Prado y J. García Sánchez, Pitágoras desde otro punto de vista, *XI Conferencia Interamericana de Educación Matemática (XI CIAEM)*, Actas, 13–17, U. D'Ambrosio (Ed.). ISBN: 857114141-X. Blumenau, Brasil, 2003.

130. M. Rodríguez Sánchez, J.M. Chamoso Sánchez, J.F. García Sánchez, L. Hernández Encinas y J. Martín Lalanda, Una visión globalizadora de las Matemáticas a partir de herramientas hipermedia, *XI Jornadas sobre el Aprendizaje y Enseñanza de las Matemáticas (XI JAEM)*, Actas 5 pp. ISBN: 84-689-0720-0. Canarias, 2003.

131. A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, G. Rodríguez Sánchez e I. Visus Ruíz, Los autómatas celulares aditivos como generadores de secuencias de bits pseudoaleatorias, *VIII Congreso de Matemática Aplicada (CEDYA 2003)*, Actas, 8 pp. ISBN: 84-930923-2-0. Tarragona, 2003.

132. A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey y G. Rodríguez Sánchez, Diseño de un criptosistema de cifrado en flujo para imágenes basado en sistemas dinámicos discretos, *VIII Congreso de Matemática Aplicada (CEDYA 2003)*, Actas, 8 pp. ISBN: 84-930923-2-0. Tarragona, 2003.

133. L. Hernández Encinas, A. Martín del Rey and A. Hernández Encinas, Encryption of images with 2-dimensional cellular automata, *6th World Multiconference on Systemics, Cybernetics and Informatics (ISAS-SCI 2002)*, Proceedings, Vol. I: Information Systems Development I, 471–476, N. Callaos, L. Hernández Encinas and F. Yetim (Eds.), International Institute of Informatics and Systemics. ISBN: 980-07-8150-1. Orlando (USA), 2002. Core C.

134. L. Hernández Encinas and J. Muñoz Masqué, Classification of genus-2 hyperellyptic curves over $\mathbb{F}_{5m}$, *6th World Multiconference on Systemics, Cybernetics and Informatics (ISAS-SCI 2002)*, Proceedings, Vol. I: Information Systems Development I, 477–482, N. Callaos, L. Hernández Encinas and F. Yetim (Eds.), International Institute of Informatics and Systemics. ISBN: 980-07-8150-1. Orlando (USA), 2002. Core C.

135. A. Martín del Rey, L. Hernández Encinas and J. Muñoz Masqué, A characterization of second-order ODEs reducible to first order, *International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2002)*, Proceedings, Vol. I, 227–236, J. Vigo Aguilar and B. Wade (Eds.). ISBN: 84-607-5365-4. Alicante, 2002.

136. Y. Cortés Gómez, L. Hernández Encinas and A. Martín de Rey, Teaching discrete dynamical systems by using Mathematica and John Conway's Game of Life, *Internacional Conference on Information and Communication Technologies in Education (ICTE 2002)*, Proceedings 901–905, Information Society and Education: Monitoring a Revolution, Vol. II, Government of Extremadura, Badajoz. ISBN: 84-95251-78-7. Badajoz, 2002. Core C.

137. J.M. Chamoso Sánchez, L. Hernández Encinas and M. Rodríguez Sánchez, Teaching and Learning mathematics with multimedia tools, *Internacional Conference on Information and Communication Technologies in Education (ICTE 2002)*, Proceedings 896–900, Information Society and Education: Monitoring a Revolution, Vol. II, Government of Extremadura, Badajoz ISBN: 84-95251-78-7. Badajoz, 2002. Core C.

138. J. Chamoso Sánchez, L. Hernández Encinas y M. Rodríguez Sánchez, Los sistemas hipermedia comparados con otros instrumentos para enseñar Matemáticas, IV Congreso Venezolano de Educación Matemática, Comunicación, Trujillo (Venezuela), 2002.

139. Y. Cortés Gómez, L. Hernández Encinas y A. Martín de Rey, De la divulgación a la investigación: el juego de la vida de Conway, *Congreso Internacional "La Ciencia ante el Público"*, Actas en CD-ROM, Publicaciones de la Universidad de Salamanca. Salamanca, 2002.

140. L. Hernández Encinas, A. Martín de Rey e I. Visus Ruíz, Cifrado de imágenes en tonos de gris mediante autómatas celulares, *VII Reunión Española sobre Criptología y Seguridad de la Información (VII RECSI)*, Actas, Tomo I, 379–389, S. González Jiménez y C. Martínez López (Eds.), Universidad de Oviedo. ISBN: 84-699-8930-8, Oviedo, 2002.

141. L. Hernández Encinas y A. Queiruga Dios, Exponentes de descifrado seguros para los criptoanálisis del tipo Wiener-Boneh al RSA, *VII Reunión Española sobre Criptología y Seguridad de la Información (VII RECSI)*, Actas, Tomo I, 391–400, S. González Jiménez y C. Martínez López (Eds.), Universidad de Oviedo. ISBN: 84-699-8930-8, Oviedo, 2002.

142. L. Hernández Encinas y A. Martín de Rey, Cifrado de imágenes en color con autómatas celulares, *XVII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2002)*, Actas, 457–458, Universidad de Alcalá de Henares. ISBN: 84-8138-517-4. Alcalá de Henares, 2002.

143. R. Díaz Len, L. Hernández Encinas, A. Hernández Encinas, S. Hoya White, A. Martín del Rey, G. Rodríguez Sánchez e I. Visus Ruíz, Uso de los autómatas celulares de Wolfram en los criptosistemas de cifrado en flujo, *III Jornadas de Matemática Discreta y Algorítmica*, Actas, 139–146, Universidad de Sevilla, 2002. ISBN: 84-607-5270-4. Sevilla, 2002.

144. J.M. Chamoso Sánchez, L. Hernández Encinas, J. Martín Lalanda, R. López Fernández y M. Rodríguez Sánchez, La simulación de un ábaco interactivo para la comprensión de la numeración elemental, *V Simposio sobre aportaciones del área de Didáctica de la Matemáticas a diferentes perfiles profesionales*, Actas, 167–174, M.C. Penalva Martínez, G. Torregrosa Gironés y J. Valls González (Eds.), Universidad de Alicante, 2002. ISBN: 84-699-7201-4. Alicante, 2002.

145. J.M. Chamoso Sánchez, J. Martín, J.C. Pereña, L. Hernández Encinas y M. Rodríguez Sánchez, Algunas aportaciones de los sistemas hipermedia a la enseñanza-aprendizaje de las Matemáticas, *7º Seminario Regional de Educación Matemática*, Actas, 265–271, Sociedad Castellano-Leonesa de Profesores de Matemáticas, León, 2002. ISBN: 84-688-0715-X. Ponferrada, 2002.

146. L. Hernández Encinas and J. Muñoz Masqué, The number of hyperelliptic curves over a finite field. Recent results, *5th World Multiconference on Systemics, Cybernetics and Informatics (ISAS-SCI 2001)*, Proceedings, Vol. VII: Computer Science and Engineering, 505–510, N. Callaos, B. Sánchez, L. Hernández Encinas and J. Grzymala Busse (Eds.), International Institute of Informatics and Systemics. ISBN: 980-07-7547-1. Orlando (USA), 2001. Core C.

147. J.M. Chamoso Sánchez, L. Hernández Encinas, J. Martín Lalanda, R. López Fernández y M. Rodríguez Sánchez, Un CD-ROM para la numeración, *X Jornadas sobre el Aprendizaje y Enseñanza de las Matemáticas (X JAEM)*, Actas, 589–592, E. Palacián y J. Sancho (Eds.), Sociedad Aragonesa de Profesores de Matemáticas e ICE de la Universidad de Zaragoza, 2001. ISBN: 84-7791-201-7. Zaragoza, 2001.

148. A. Queiruga Dios y L. Hernández Encinas, Exponentes de cifrado pequeños en RSA y criptoanálisis de Wiener, *XVI Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2001)*, Comunicación, Villaviciosa de Odón (Madrid), 2001.

149. L. Hernández Encinas and J. Muñoz Masqué, Iterated discrete exponentiation and its cryptographic applications, *4th World Multiconference on Systemics, Cybernetics and Informatics (ISAS-SCI 2000)*, Proceedings, Vol. VIII: Computer Science and Engineering, 261–265, J. Kun Lee, M. Juric, A. Bruzzone, D. Klovshy and M. Fujita (Eds.), International Institute of Informatics and Systemics. ISBN: 980-07-6694-4. Orlando (USA), 2000. Core C.

150. L. Hernández Encinas and J. Muñoz Masqué, Invariants of hyperelliptic curves of genus 2 over finite fields, *Third European Congress of Mathematics*, Poster, Barcelona, 2000.

151. L. Hernández Encinas y J. Muñoz Masqué, Una revisión de los generadores pseudoaleatorios del tipo $x^a (\mathrm{mod}\, n)$, *VI Reunión Española de Criptología y Seguridad de la Información (VI RECSI)*, Actas, 297–305, P. Caballero Gil y C. Hernández Goya (Eds.), RA-MA, Madrid, 2000. ISBN: 84-7897-431-8. Puerto de la Cruz (Tenerife), 2000.

152. J.M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez, Pitágoras interactivo, *6º Seminario Castellano-Leonés de Educación Matemática*, Actas, 4 pp., Sociedad de Castilla y León del Profesorado de Matemáticas, Burgos, 2000. ISBN: 84-922919-4-X. Burgos, 2000.

153. J.M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández y M. Rodríguez Sánchez, Los sistemas hipermedia, ¿un posible camino para enseñar Matemáticas?, *IV Simposio sobre propuestas metodológicas y de evaluación en la formación inicial de los profesores del área de Didáctica de las Matemáticas*, Oviedo, 2000.

154. J.M. Chamoso Sánchez, L. Hernández Encinas, R. López Fernández and M. Rodríguez Sánchez, Multimedia resources for Mathematical Education, *Teaching of Information and Communication Sciences. Euroconference'99 (New Technologies for Higher Education)*, Comunicación, Salamanca, 1999.

155. L. Hernández Encinas, Tests estadísticos para el reconocimiento de números pseudoaleatorios en Criptología, *Segundas Jornadas de Estadística Aplicada*, Actas, 22-27, J. López Fidalgo y J.M. Rodríguez Díaz (Eds.), Hespérides, Salamanca, 1999. ISBN: 84-88895-55-0. Salamanca, 1999.

156. M. Rodríguez Sánchez, J.M. Chamoso Sánchez, L. Hernández Encinas y R. López Fernández, Resolución de problemas mediante un CD-ROM, Actas 276–280, *IX Jornadas sobre el Aprendizaje y Enseñanza de las Matemáticas (IX JAEM)*, Lugo, 1999. ISBN: 84-920438-3-0. Lugo, 1999.

157. L. Hernández Encinas, F. Montoya Vitini, J. Muñoz Masqué and A. Peinado Domínguez, Maximal period of orbits of the BBS generator, *1998 International Congress on Information Security and Cryptology (ICISC 98)*, Proceedings, 71-80, Institute of Information Security & Cryptology, Seúl (Corea), 1998. ISBN: 89-85305-14-X. Seúl (Corea), 1998. Core B.

158. L. Hernández Encinas, Alfred Menezes y J. Muñoz Masqué, Algunas propiedades de las curvas hiperelípticas de género 2 sobre un cuerpo finito de característica 2 y su uso criptográfico, *V Reunión Española de Criptología y Seguridad de la Información (V RECSI)*, Actas, 155-166, F. J. López Muñoz, J. Pastor Franco y J.M. Troya Linero (Eds.), Universidad de Málaga, 1998. ISBN: 84-8497-820-6. Málaga, 1998.

159. L. Hernández Encinas, Aplicación de los métodos multivariantes a la clasificación de rocas, *Primeras Jornadas de Estadística Aplicada*, Actas, 19-21, J. López Fidalgo y J.M. Rodríguez Díaz (Eds.), Hespérides, Salamanca, 1999. ISBN: 84-88895-55-0. Salamanca, 1998.

160. L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué, A new proof of Faà di Bruno's formula, *Second International Workshop on Computational Differentiation*, Poster, Santa Fe (USA), 1996.

161. L. Hernández Encinas, F. Montoya Vitini, J. Muñoz Masqué, G. Álvarez Marañón y A. Peinado Domínguez, Algoritmo de cifrado con clave pública mediante una función cuadrática en el grupo de los enteros módulo n, *IV Reunión Española de Criptología (IV REC)*, Actas, 101-108, J. Tena Ayuso y M. F. Blanco Martín (Eds.), Universidad de Valladolid, 1996. ISBN: 84-7762-645-6. Valladolid, 1996.

162. F. Montoya Vitini, J. Muñoz Masqué, G. Pastor Dégano, M. Romera García y L. Hernández Encinas, *Primer Congreso de Usuarios de Internet*, Criptografía en Internet, Madrid, 1996.

163. L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué, Maximal length sequences by iterating the quadratic function on the multiplicative group of integers modulo p, *Fifth IMA Conference on Cryptography and Coding*, Poster, Cirencester (UK), 1995. Core B.

164. L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué, Invariant differential forms on $K(P)\times M_E$, *XXth International Colloquium on Group Theoretical Methods in Physics*, Proceedings, 219-222, A. Arima, T. Eguchi and N. Nakanishi (Eds.), World Scientific, Singapore, 1995. ISBN: 981-02-2087-1. Toyonaka (Japan), 1994.

165. L. Hernández Encinas, F. Montoya Vitini y J. Muñoz Masqué, Generación de sucesiones pseudoaleatorias mediante funciones cuadráticas en $\mathbb{Z}_{p^n}$ y en su límite proyectivo, *III Reunión Española sobre Criptología (III REC)*, Actas, 27-32, Universidad Politécnica de Cataluña, Barcelona, 1994. ISBN: 84-605-1745-4. Barcelona, 1994.

166. L. Hernández Encinas, I. Jiménez Calvo y J. Muñoz Masqué, Un criterio de primalidad basado en las propiedades de autosemejanza de los fractales de Pascal, *IX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 94)*, Las Palmas de Gran Canaria, 1994.

167. A. Arteaga Iriarte, L. Hernández Encinas and J. Muñoz Masqué, Splines on $\mathbb{S}^2$ for small latitudes, *Second International Colloquium on Numerical Analysis*, Proceedings, 3-11, D. Bainov and V. Covachev (Eds.), VSP, Tokyo (Japan), 1994. ISBN: 90-6764-165-8. Plovdiv (Bulgaria), 1993.

168. L. Hernández Encinas, Information meeting about the comparative study of Mathematics and Science curricula in Ibero-American States, *7th International Congress on Mathematical Education (7th ICME)*, Québec (Canada), 1992.

169. L. Hernández Encinas, Estudio de métodos de cluster en muestras grandes y aplicaciones a problemas de clasificación geológica, *Primer Taller Iberolatinoamericano de Informática y Geociencias*, La Habana (Cuba), 1992.

170. L. Hernández Encinas, Testing different geomathematics techniques to identify igneous rocks samples, *I.G.C.P. Project Annual Meeting*, Salamanca, 1990.

171. L. Hernández Encinas, Una aproximación a la Programación Lineal, *Jornadas de Matemáticas Aplicadas*, Salamanca, 1990.

172. L. Hernández Encinas, Algo de Matemática Aplicada, *Jornadas de Matemáticas Aplicadas*, Salamanca, 1990.

173. L. Hernández Encinas, Las nuevas tecnologías de la información en la educación, *Jornadas de Informática*, Cáceres, 1986.

Comunicaciones a congresos internacionales (con ISBN)	92
Posters y comunicaciones a congresos internacionales (sin ISBN)	11
Comunicaciones a congresos nacionales (con ISBN)	53
Posters y comunicaciones a congresos nacionales (sin ISBN)	12
Comunicaciones a congresos internacionales, Core A	2
Comunicaciones a congresos internacionales, Core B	27
Comunicaciones a congresos internacionales, Core C	18

Tesis Doctorales y otros trabajos dirigidos

1. Tesis: *Cryptographic Protocols for Privacy Enhancing Technologies. From Privacy Preserving Human Attestation to Internet Voting.* Doctorando: I. Querejeta Azurmendi. Calificación: Sobresaliente "Cum Laude". Universidad Carlos III de Madrid. Dpto. de Ingeniería Informática, 05/07/2022.

2. Tesis: *Propuesta de un Marco de Referencia para una Seguridad Integral: Más allá de la Seguridad Física y Lógica. Casos de uso en PYME.* Doctorando: J. Espinosa García. Calificación: Sobresaliente "Cum Laude". Universidad de Málaga. Dpto. de Ingeniería de comunicaciones, 20/05/2022.

3. Tesis: *Design and implementation of software tools for side channel attacks to cryptographic devices (Diseño e implementación de herramientas software para ataques por canal lateral a dispositivos criptográficos).* Doctorando: A. Fuentes Rodríguez. Calificación: Sobresaliente "Cum Laude". Universidad de Alcalá de Henares. Dpto. de Automática, 11/12/2020.

4. Tesis: *Modelización Matemática de la propagación de malware: Un nuevo enfoque basado en la seguridad de la información.* Doctorando: J. D. Hernández Guillén. Calificación: Sobresaliente "Cum Laude". Universidad de Salamanca. Dpto. de Matemática Aplicada, 22/10/2020.

5. Tesis: *On the hardness of the hidden subspaces problem with and without noise. Cryptanalysis of Aaronson-Christiano's quantum money scheme.* Doctorando: M. Conde Pena. Calificación: Sobresaliente "Cum laude". Universidad de Salamanca. Dpto. de Matemática Aplicada, 27/09/2018.

6. Tesis: *Autenticación biométrica de usuarios a través del iris mediante la ocultación de claves y funciones resumen que preservan la similitud (Biometric authentication of users through iris by using key binding and similarity preserving hash functions).* Doctorando: F. Hernández Álvarez. Calificación: Sobresaliente "Cum laude". Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Dpto. de Matemática Aplicada a las Tecnologías de la Información, 15/12/2015.

7. Tesis: *Implementación en tarjetas inteligentes Java card de protocolos de cifrado y descifrado basados en curvas elípticas.* Doctorando: V. Gayoso Martínez. Calificación: Sobresaliente "Cum laude". Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Dpto. de Matemática Aplicada a las Tecnologías de la Información, 14/12/2010.

8. Tesis: *Avances recientes en el criptoanálisis del criptosistema de Chor-Rivest. Aplicaciones criptográficas.* Doctorando: A. Queiruga Dios. Calificación: Sobresaliente "Cum laude". Universidad de Salamanca. Facultad de Ciencias, 11/07/2006.

9. Tesis: *Análisis de una experiencia de resolución de problemas para la mejora de la enseñanza-aprendizaje de las Matemáticas.* Doctorando: J. Chamoso Sánchez. Calificación: Sobresaliente "Cum laude" y Premio extraordinario de doctorado. Universidad de Salamanca. Facultad de Educación, 02/11/2000.

10. Proyecto Fin de Máster: *Towards Privacy Preserving Sensor-Based Continuous Authentication.* Alumno: L. Hernández Álvarez. Calificación: Sobresaliente. Departamento de Informática, Universidad Carlos III de Madrid. Master in "Information Health Engineering", 15/09/2020.

Participación en comités y representaciones (nacionales y/o internacionales)

1. Miembro del Comité del Programa Científico en las *VIII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2023)*, Vigo (Spain), 21–23 Junio 2023, (https://2023.jnic.es/comites/).
2. Chair of the *Second International Conference on Innovations in Computing Research (ICR'23)*, Madrid, Spain, 4–6 August 2023, (https://iicser.org/icr23/orgnaization_com.html).
3. Miembro del Program Committee of the *Second International Conference on Innovations in Computing Research (ICR'23)*, Madrid, Spain, 4–6 August 2023, (https://iicser.org/icr23/com_net_sec.html).
4. Miembro del Advisory Committee of the *Second International Conference on Innovations in Computing Research (ICR'23)*, Madrid, Spain, 4–6 August 2023, (https://iicser.org/icr23/advisory_com.html).
5. Co-chair of the Organizational Committee 2023 *International Conference on Security and Management (SAM'23)*, Las Vegas, USA, 24–27 July 2023, (http://http://sam.udmercy.edu/sam23/orgnaization_com.html).
6. Miembro del Program Committee of the 2023 *International Conference on Security and Management (SAM'23)*, Las Vegas, USA, 24–27 July 2023, (http://sam.udmercy.edu/sam23/program_com.html).
7. Miembro del Comité Científico *XVII Reunión Española Sobre Criptología y Seguridad de la Información* (RECSI 2022), Santander 19-21 octubre, https://recsi2022.unican.es/es/comites/
8. Miembro del International Program Committee *36th edition of the International Conference on Information Technologies*, 15-16 September 2022, Bulgaria, http://infotech-bg.com/committees
9. Miembro del Advisory Committee The *2022 International Conference on Innovations in Computing Research* (ICR'22), Athens, Greece, August 29-31, 2022, https://iicser.org/icr22/advisory_com.html
10. Miembro del International Program Committee in *Computer/Network Security The 2022 International Conference on Innovations in Computing Research* (ICR'22), Athens, Greece, August 29-31, 2022, https://iicser.org/icr22/com_net_sec.html
11. Miembro del International Program Committee in Computer Science and Computer Engineering Education The 2022 International Conference on Innovations in Computing Research (ICR'22), Athens, Greece, August 29-31, 2022, https://iicser.org/icr22/CSE_edu.html
12. Co-chair of the Organizational Committee 2022 *International Conference on Security and Management (SAM'22)*, Las Vegas, USA, 25–28 July 2022, (http://sam.udmercy.edu/sam22/Organizational-Committee.html).
13. Miembro del Program Committee for the 2022 *International Conference on Security and Management (SAM'22)*, Las Vegas, USA, 25–28 July 2022, (http://sam.udmercy.edu/sam22/ProgramCommittee.html).
14. Miembro del Advisory Committee del *The 2022 International Conference on Innovations in Computing Research (ICR'22)*, Athens, (Greece), 29–31 August 2022, (https://iicser.org/icr22/advisory_com.html).
15. Miembro del Computer/Network Security Committee del *The 2022 International Conference on Innovations in Computing Research (ICR'22)*, Athens, (Greece), 29–31 August 2022, (https://iicser.org/icr22/com_net_sec.html).
16. Miembro del Computer Science and Computer Engineering Education Committee del *The 2022 International Conference on Innovations in Computing Research (ICR'22)*, Athens, (Greece), 29–31 August 2022, (https://iicser.org/icr22/CSE_edu.html).
17. Miembro del Scientific Committee de las *International Conference on Mathematics and its Applications in Science and Engineering (ICMASE 2022)*, Bucharest (Romania), 4–7 July 2022, (https://icmase.com/committees).

18. Miembro del Comité del Programa de Investigación en las *VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022)*, Bilbao (Spain), 27–29 Junio 2022, (`https://2022.jnic.es/commites`).

19. Participación en la redacción final de los Informes Anuales de Seguridad Nacional, de los años 2018, 2019, 2020 y 2021, del Departamento de Seguridad Nacional, Consejo de Seguridad Nacional, Presidencia del Gobierno.

20. Miembro del Security Advisory Board (SAB) del proyecto "An Interoperable Multidomain CBRN System (NEST)". Call: H2020-SU-SEC-2018-2019-2020 (Security). Topic: SU-DRS04-2019-2020. Type of action: RIA. Proposal number: 101018596. 2021-2024.

21. Participación en la mesa redonda "Sinergias de investigación en ciberseguridad en España", en la XVI Reunión Española sobre Criptología y Seguridad de la Información, Universidad de Lérida, Lérida (Spain), 15 de abril de 2021.

22. Participación en la mesa redonda "Tecnologías Emergentes y Seguridad", en las Jornadas "Mañana empieza hoy", Consejo Superior de Investigaciones Científicas y Universidad Autónoma de Madrid, Madrid (Spain), 13 de junio de 2019.

23. Participación en la mesa redonda "Retos para la seguridad en un futuro cercano. ¿Estamos preparados?", en las Jornadas Técnicas RedIRIS 2019, Red.es, Sevilla (Spain), 29 de mayo de 2019.

24. Associated Editor desde 2010 a 2018 de la revista "Information Sciences", Elsevier, `http://ees.elsevier.com/ins/`, ISSN: 0020-0255. Revista incluida en el JCR del SCI con un Factor de Impacto en 2012 de 3.643 (posición 6 de 132 –Q1–) y un Factor de Impacto medio en los últimos 5 años de 3.676 (Categoría: Computer Science, Information Systems).

25. Miembro del Editorial Board de la revista "The Open Mathematics Journal", Bentham Open, `http://www.bentham.org/open/tomatj`, ISSN: 1874-1177.

26. Miembro del Editorial Board de la revista "International Journal on Information Technologies & Security", `http://ijits-bg.com/`, ISSN: 1313-8251.

27. Recensor del Mathematical Reviews, de la American Mathematical Society desde 1996.

28. Representante del CSIC, desde 2018, en el Comité Técnico de UNE (antes AENOR) CTN320 "Ciberseguridad y protección de datos personales". Dentro de este Comité, actuó como el secretario del subcomité CTN/SC2 "Criptografía y mecanismos de seguridad" y como vocal en el CTN320/SC27 "Seguridad de la información, Ciberseguridad y Protección de la Privacidad".

29. Representante del CSIC, desde 2018, en el Comité Técnico de UNE (antes AENOR) CTN71 "Tecnologías Habilitadoras Digitales". Dentro de este Comité, soy vocal del subcomité CTN31/SC38 "Tecnologías de la Información. Servicios y Plataformas para Aplicaciones distribuidas".

30. Representante del CSIC, como socio fundador desde 2016, de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC, http://www.renic.es/es/index.html). El CSIC ocupa la Vicepresidencia de RENIC desde 2018.

31. Representante del CSIC en la Red de Centros de Excelencia en Ciberseguridad, para el desarrollo de la "Medida 25: Estudio de viabilidad de una red de centros de excelencia en ciberseguridad" del "Eje V: Programa de excelencia en ciberseguridad", dentro del Plan de Confianza en el Ámbito Digital 2013-2015, de la Agenda Digital para España. Puesto en marcha por el Instituto Nacional de Ciberseguridad (INTECO-INCIBE).

32. Representante del CSIC en el Polo Tecnológico Nacional en ciberseguridad, para el desarrollo de la "Acción 3. Observatorio de tendencias y nuevos segmentos en ciberseguridad a nivel internacional", dentro del Plan de confianza en el ámbito digital 2013-2015, de la Agenda digital para España. Puesto en marcha por el Instituto Nacional de Ciberseguridad (INTECO-INCIBE).

33. Representante del CSIC en el Programa de ayudas para grupos de investigación avanzada en ciberseguridad, para el desarrollo de la "Medida 19: Equipo de investigación avanzada" del "Eje V: Programa de excelencia en ciberseguridad", dentro del Plan de confianza en el ámbito digital 2013-2015, de la Agenda digital para España. Puesto en marcha por el Instituto Nacional de Ciberseguridad (INTECO-INCIBE).

34. Representante del CSIC (junto con el coordinador del Área de Tecnologías Físicas) en la Comisión Mixta del *Acuerdo Marco para llevar a cabo actividades relacionadas con la investigación científica y el desarrollo tecnológico*, firmado entre el CSIC y el Instituto Nacional de Ciberseguridad (INTECO-INCIBE) en 2014.

35. Representante del CSIC (junto con el coordinador del Área de Tecnologías Físicas) en la Comisión Mixta del Acuerdo Marco *para la Investigación de vulnerabilidades Criptográficas en el ámbito de la Seguridad de las Tecnologías de la Información*, firmado entre el CSIC y el CNI en 2010.

36. Representante desde 29/04/2013 del CSIC en el Technical Assistance Agreement TA-5299-12 del International Interoperability Control Working Group (IICWG) con el fin de *to promote secure interoperability among various COMSEC products that will be produced by the member nations to protect NATO and national classified information in military and civilian environments* bajo el auspicio del Departamento de Estado del gobierno de EE.UU.

37. Miembro del Programm Committee de *14th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2021)*, Bilbao, 22–24September 2021 (`http://2021.cisisconference.eu/committee/`).

38. Miembro del International Programm Committee de *2021 IEEE International Conference on Information Technologies (InfoTech 2021)*, Varna, Bulgaria, 16–17 September 2021 (`http://infotech-bg.com/committees`).

39. Miembro del Scientific Committee de *International Conference on Mathematics and Its Applications in Science and Engineering (ICMASE 2021)*, Salamanca, Spain, 1–2 July 2021 (`http://icmase2021.com/committees`).

40. Co-chair of the Organizational Committee 2021 *International Conference on Security and Management (SAM'21)*, Las Vegas, USA, 26–29 July 2021, (`http://sam.udmercy.edu/sam21/Organizational-Committee.html`).

41. Miembro del Program Committee for the 2021 *International Conference on Security and Management (SAM'21)*, Las Vegas, USA, 26–29 July 2021, (`http://sam.udmercy.edu/sam21/ProgramCommittee.html`).

42. Miembro del Comité del Programa de Investigación en las *VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC2021)*, Ciudad Real (Spain), 9–10 Junio 2021, (`https://2021.jnic.es/comites`).

43. Miembro del Comité del Programa de la *XVI Reunión Española sobre Criptología y Seguridad de la Información (XVI RECSI)*, Lérida, 14–16 de abril, 2021.

44. Miembro del Programm Committee de *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)*, Burgos, September 2020 (`http://http://2020.cisisconference.eu/`).

45. Miembro del Scientific Committee de *International Conference on Mathematics and Its Applications in Science and Engineering (ICMASE 2020)*, Ankara, Turkey, July 2020 (`http://icmase2020.com/committees`).

46. Miembro del International Programm Committee de *2020 IEEE International Conference on Information Technologies (InfoTech 2020)*, Varna, Bulgaria, September 2020 (`http://infotech-bg.com`).

47. Co-chair of the Organizational Committee 2020 *International Conference on Security and Management (SAM'20)*, Las Vegas, USA, July 2020, (`http://sam.udmercy.edu/sam20/Organizational-Committee.html`).

48. Miembro del Program Committee for the 2020 *International Conference on Security and Management (SAM'20)*, Las Vegas, USA, July 2020, (`http://sam.udmercy.edu/sam20/ProgramCommittee.html`).

49. Miembro del Comité del Programa de las *X Congreso Iberoamericano de Seguridad Informática (CIBSI 2017)*, Bogotá, Colombia, Enero 22–24, 2020 (`http://www.urosario.edu.co/CIBSI/inicio`).

50. Co-chair of the Organizational Committee 2019 *International Conference on Security and Management (SAM'19)*, Las Vegas, USA, July 2019.

51. Miembro del Program Committee for the 2019 *International Conference on Security and Management (SAM'19)*, Las Vegas, USA, July 2019.

52. Miembro del Comité del Programa de Investigación en las *V Jornadas Nacionales de Investigación en Ciberseguridad (JNIC2019)*, Cáceres (Spain), June 2019.

53. Miembro del Program Committee for the *12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019)*, Sevilla (Spain), May 2019.

54. Miembro del Program Committee for the *10th International Conference on EUropean Transnational Education (ICEUTE 2019)*, Sevilla (Spain), May 2019.

55. Co-chair of the Organizational Committee 2018 *International Conference on Security and Management (SAM'18)*, Las Vegas, USA, July 2018.

56. Miembro del Program Committee for the 2018 *International Conference on Security and Management (SAM'18)*, Las Vegas, USA, July 2018.

57. Miembro del Comité del Programa *IV Jornadas Nacionales de Investigación en Ciberseguridad (JNIC'18)*, San Sebastián, Junio 2018.

58. Miembro del Program Committee for the *32nd International Conference on Information Technologies*, St. Constantine and Elena resort, Bulgaria, September 2018.

59. Miembro del Comité del Programa *XV Reunión Española sobre Criptología y Seguridad de la Información (XV RECSI)*, Granada, Octubre 2018.

60. Miembro del Comité del Programa de las *IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2017)*, Buenos Aires, Argentina, Noviembre 1–3, 2017 (`http://cibsi2017.org/`).

61. Miembro del Program Committee for the 31^{st} *International Conference on Information Technologies (InfoTech 2017)*, Sofia, Bulgaria, September 20–21, 2017 (`http://infotech-bg.com/`).

62. Miembro del Program Committee for the 2017 *International Workshop on Computational Intelligence in Security for Information Systems (CISIS'17)*, León (Spain), September 2017.

63. Chair of the Special Session "Identification, Simulation, and Prevention of Security and Privacy Threats in Modern Communication Networks", 2017 *International Workshop on Computational Intelligence in Security for Information Systems (CISIS'17)*, León (Spain), September 2017.

64. Miembro del Program Committee for the 2017 *International Conference on Security and Management (SAM'17)*, Las Vegas, USA, July 2017.

65. Co-chair of the of the Organizational Committee 2017 *International Conference on Security and Management (SAM'17)*, Las Vegas, USA, July 2017.

66. Miembro del Technical Program Committee for the 2016 *8th International Conference on Computational Aspects of Social Networks (CASoN 2016)*, Vellore (India), December 19–21, 2016.

67. Miembro del Technical Program Committee for the 2016 *8th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2016)*, Vellore (India), December 19–21, 2016.

68. Miembro del Comité Científico de la *XIV Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2016)*, Mahón, 26–28 Octubre, 2016.

69. Miembro del Program Committee for the *9th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2016)*, San Sebastián (Spain), October 19–21, 2016.

70. Miembro del Program Committee for the 2016 *International Conference on Security and Management (SAM'16)*, Las Vegas, USA, July 2016.

71. Miembro del Comité del Programa de las *Segundas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)*, Granada, Junio 2016.

72. Miembro del Program Committee for the 2015 *International Conference on Security and Management (SAM'15)*, Las Vegas, USA, July 2015.

73. Miembro del Comité del Programa del *VIII Congreso Iberoamericano de Seguridad Informática (CIBSI 2015)*, Quito, Noviembre 2015.

74. Miembro del Program Committee del 8^{th} *Computational Intelligence in Security for Information Systems (CISIS'15)*, Burgos, June 2015.

75. Miembro del Program Committee del *10th International Conference on Information Assurance and Security (IAS 2014)*, Okinawa, Japan, 27–30 November 2014.

76. Miembro del Program Committee del 7^{th} *Computational Intelligence in Security for Information Systems (CISIS'14)*, Salamanca, September 2014.

77. Miembro del Comité del Programa de la *XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2014)*, Alicante, 2–5 Septiembre 2014.

78. Miembro del Program Committee del 28^{th} *International Conference on Information Technologies (InfoTech-2014)*, Varna, Bulgaria, 18–19 September 2014.

79. Miembro del Program Committee for the *2014 International Conference on Security and Management (SAM'14)*, Las Vegas, USA, 21–24 July 2014.

80. Miembro del Programme Committee del *9th International Conference on Information Assurance and Security (IAS 2013)*, Tunis, Tunisia, December 2013.

81. Miembro del Comité del Programa del *VII Congreso Iberoamericano de Seguridad Informática (CIBSI 2013)*, Panamá, Octubre 2013.

82. Miembro del Program Committee del 5^{th} *Computational Intelligence in Security for Information Systems (CISIS'13)*, Salamanca, September 2013.

83. Miembro del Programme Committee de la *International Conference 'Information Technologies' (InfoTech-2013)*, Varna, Bulgaria, Septiembre 2013.

84. Miembro del Program Committee del *2013 International Conference on Security of Management (SAM 2013)*, Las Vegas, USA, July 2013.

85. Miembro del Comité del Programa del *IX Congreso Iberoamericano de Seguridad Informática (CIBSI 2012)*, Loja, Ecuador, Diciembre 2012.

86. Miembro del Program Committee del *Information Assurance and Security (IAS 2012)*, São Carlos, Brazil, November 2012.

87. Miembro del Program Committee del 5^{th} *Computational Intelligence in Security for Information Systems (CISIS'12)*, Ostrava, Czech Republic, September 2012.

88. Miembro del Programme Committee de la *International Conference 'Information Technologies' (InfoTech-2012)*, Varna, Bulgaria, Septiembre 2012.

89. Miembro del Program Committee del *2012 International Conference on Security of Management (SAM 2012)*, Las Vegas, USA, July 2012.

90. Miembro del Programme Committee del *Integrating Research, Education, and Problem Solving: Summer IREPS 2012*, Orlando, Florida, USA, July 2012.

91. Miembro del Program Committee del *7th International Conference on Hybrid Artificial Intelligence Systems (HAIS12)*, Salamanca, Spain, March 2012.

92. Miembro del Comité Científico de la *XII Reunión Española de Criptología y Seguridad de la Información (XII RECSI)*, San Sebastián, Septiembre 2012.

93. Miembro del Program Committee del *Information Assurance and Security (IAS 2011)*, Malacca, Malaysia, December 2011.

94. Miembro del Comité del Programa del *VIII Congreso Iberoamericano de Seguridad Informática (CIBSI 2011)*, Bucaramanga, Colombia, Noviembre 2011.

95. Miembro del Programme Committee de la *International Conference 'Information Technologies' (InfoTech-2011)*, Varna, Bulgaria, Septiembre 2011.

96. Miembro del Program Committee del 4^{th} *Computational Intelligence in Security for Information Systems (CISIS'11)*, Torremolinos, June 2011.

97. Miembro del Program Committee del 3^{rd} *Computational Intelligence in Security for Information Systems (CISIS'10)*, León, November 2010.

98. Miembro del Program Committee del *Information Assurance and Security (IAS 2010)*, Atlanta, USA, August 2010.

99. Miembro del Comité del Programa de la *Conferencia Ibero-Americana de Ingeniería e Innovación Tecnológica (CIIIT 2010)*, Orlando, Florida, USA, July 2010.

100. Miembro del Program Committee del 3^{rd} *Symposium on Academic Globalization (AG 2010)*, Orlando, USA, July 2010.

101. Miembro del Program Committee del 14^{th} *World Multi-conference on Systemics, Cybernetics and Informatics (WMSCI 2010)*, Orlando, Florida, USA, June-July 2010.

102. Miembro del Program Committee del *The International Symposium on Science 2 and Expansion of Science (S2ES 2010)*, Orlando, Florida, USA, June-July 2010.

103. Miembro del Program Committee del 3^{rd} *International Multi-Conference on Engineering and Technological Innovation (IMETI 2010)*, Orlando, Florida, USA, June-July 2010.

104. Miembro del Program Committee de la *International Conference on Engineering and Meta-Engineering (ICEME 2010)*, Orlando, Florida, USA, April 2010.

105. Miembro del Program Committee del *The International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2010)*, Orlando, Florida, USA, April 2010.

106. Miembro del Comité Científico de la *XI Reunión Española de Criptología y Seguridad de la Información (XI RECSI)*, Tarragona, Septiembre, 2010.

107. Miembro del Comité del Programa del *V Congreso Iberoamericano de Seguridad Informática (CIBSI 2009)*, Montevideo, Uruguay, Noviembre 2009.

108. Miembro del Program Committee del 2^{nd} *International Workshop on Computational Intelligence in Security for Information Systems (CISIS 2009)*, Burgos, September 2009.

109. Miembro del Program Committee de la *International Conference 'Information Technologies' (IT-2009)*, Varna, Bulgaria, Septiembre 2009.

110. Miembro del Program Committee del 2^{nd} *International Symposium on Academic Globalization (AG 2009)*, Orlando, Florida, USA, July 2009.

111. Miembro del Program Committee del 2^{nd} *International Multi-Conference on Engineering and Technological Innovation (IMETI 2009)*, Orlando, Florida, USA, July 2009.

112. Miembro del Program Committee del 13^{th} *World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2009)*, Orlando, Florida, USA, July 2009.

113. Miembro del Program Committee del *Conferencia Ibero-Americana de Ingeniería e Innovación Tecnológica (CIIIT 2009)*, Orlando, Florida, USA, July 2009.

114. Miembro del Program Committee del 2^{nd} *Symposium on Academic Globalization (AG 2009)*, Orlando, USA, Julio 2009.

115. Miembro del Program Committee del *The International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2009)*, Orlando, Florida, USA, April 2009.

116. Miembro del Scientific Committee de *The* 12^{th} *World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2008)*, Orlando, Florida, Septiembre 2008.

117. Miembro del Programme Committee de la *International Conference 'Information Technologies' (IT-2008)*, Varna, Bulgaria, Septiembre 2008.

118. Miembro del Scientific Committee de *The International Multi-Conference on Engineering and Technological Innovation (IMETI 2008)*, Orlando, Florida, USA, Junio-Julio 2008.

119. Vicepresidente del Comité Organizador de la *X Reunión Española de Criptología y Seguridad de la Información (X RECSI)*, Salamanca, Septiembre 2008.

120. Miembro del Comité del Programa de la *X Reunión Española de Criptología y Seguridad de la Información (X RECSI)*, Salamanca, Septiembre 2008.

121. Miembro del Comité del Programa del *IV Congreso Iberoamericano de Seguridad Informática (CIBSI 2007)*, Mar del Plata, Argentina, Noviembre 2007.

122. Miembro del Programme Committee de la *International Conference 'Information Technologies' (IT-2007)*, Varna, Bulgaria, Septiembre 2007.

123. Miembro del Comité Científico del *II Congreso Español en Ingeniería Informática (CEDI 2007)*, Zaragoza, Septiembre 2007.

124. Miembro del Programme Committee del 10^{th} *World Multi-conference on Systemics, Cybernetics and Informatics (WMSCI 2006)*, Orlando, USA, 2006.

125. Miembro del Comité del Programa del *Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, Valparaiso, Chile, 2005.

126. Organizador de Sesión Invitada en el *Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA (MAT.ES 2005)*, Valencia, 2004.

127. Miembro del Programme Committee del 7^{th} *World Multiconference on Systemics, Cybernetics and Informatics (SCI 2003)*, Orlando, USA, 2003.

128. Miembro del Programme Committee del 6^{th} *World Multiconference on Systemics, Cybernetics and Informatics (SCI 2002)*, Orlando, USA, 2002.

129. Organizador de Invited Session en el 6^{th} *World Multiconference on Systemics, Cybernetics and Informatics (SCI 2002)*, Orlando, USA, 2002.

130. Miembro del Comité del Programa de la *VII Reunión Española de Criptología y Seguridad de la Información (VII REC)*, Oviedo, 2002.

131. Organizador de Invited Session en el 5^{th} *World Multiconference on Systemics, Cybernetics and Informatics (SCI 2001)*, Orlando, USA, 2001.

132. Miembro del Programme Committee de la *International Conference/Workshop on Automatic Differentiation (AD 2000)*, Niza, Francia, 2000.

133. Miembro del Comité del Programa de la *VI Reunión Española de Criptología y Seguridad de la Información (VI REC)*, Tenerife, 2000.

134. Miembro de Comisión Organizadora del *V Seminario Castellano-Leonés de Educación Matemática*, Toro (Zamora), 1998.

135. Miembro del Scientific Committee del *Second International Workshop on Differential Geometry and its Applications*, Constanza, Rumanía, 1995.

136. Miembro de Comisión Organizadora de la *III Muestra del ordenador en el aula*, Zamora, 1989.

137. Miembro de Comisión Organizadora de la *II Muestra del ordenador en el aula*, Zamora, 1988.

Conferencias invitadas

1. *A visit to Pre-Quantum, Quantum, and Post-Quantum Cryptography*, The 2024 International Conference on Advances in Computing Research (ACR'24), Madrid, Spain, June 5, 2024.

2. *Transición de la criptografía precuántica a la postcuántica*, Máster Universitario en Modelización Matemática, Universidad de Salamanca, Salamanca, 6 de mayo de 2024.

3. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Programa de Excelencia en Bachillerato, IES La Serna, Fuenlabrada (Madrid), 20 de marzo de 2024.

4. *Situación actual de la Criptografía Postcuántica*, Jornada sobre Criptología Postcuántica: un análisis de la situación, Fundación Círculo de Tecnologías para la Defensa y la Seguridad, Madrid, 28 de febrero de 2024.

5. *Criptografía precuántica, cuántica y postcuántica*, CyberCampUC3M, Universidad Carlos III de Madrid, 1 de junio de 2023.

6. *Pre-Quantum, Quantum and Post-Quantum Cryptography*, IV National CyberLeague, Guardia Civil, Aranjuez, Spain, November 16, 2022.

7. *La ciberseguridad como mecanismo para la protección de la información*, 4º Simposio Internacional de Ingenierías, Universidad Vasco de Quiroga, Morelia (México), octubre de 2022.

8. *Las Matemáticas como herramienta para hacer secreta la información*, Ciclo: Ciencia en Primera Persona, Museo Nacional de Ciencia y Tecnología (MUNCYT). 13 de marzo de 2022.

9. *Acerca de la Criptografía Pre y Post cuántica*, 3er Simposio Internacional de Ingenierías, Universidad Vasco de Quiroga, Morelia (México), noviembre 2021.

10. *Perspectivas de futuro de la Criptografía ante la Computación Cuántica*, Centro Universitario de la Guardia Civil, Aranjuez, noviembre 2020.

11. *Herramientas criptográficas para la autenticación personal con preservación de la privacidad*, Simposio "La importancia de la seguridad de la Información", Universidad Vasco de Quiroga, Morelia (México), octubre 2020.

12. *Seguridad criptográfica de la tecnología Blockchain (y Bitcoin)*, Centro Universitario de la Guardia Civil, Aranjuez, noviembre 2019.

13. *Perspectivas de futuro de la Computación Cuántica*, Centro Universitario de la Guardia Civil, Aranjuez, noviembre 2019.

14. *¿Criptografía cuántica?: ¡Criptografía post-cuántica!*. MasterClass, Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, octubre 2019.

15. *Taller de Criptografía para Docentes*, Universidad Vasco de Quiroga, Morelia (México), octubre 2019.

16. *Taller de Criptografía para Alumnos*, Universidad Vasco de Quiroga, Morelia (México), octubre 2019.

17. *Cripto viene de Criptografía: Criptomonedas (bitcoin) y Criptofundamentos de Blockchain*, ciclo ¿Qué sabemos de?, Delegación del CSIC en Aragón, Zaragoza, septiembre 2019.

18. *Problemas y algoritmos matemáticos para la seguridad de la tecnología Blockchain*, Instituto Universitario de Física Fundamental y Matemáticas, Universidad de Salamanca, Salamanca, septiembre 2019.

19. *Retos para la seguridad en un futuro cercano, ¿está la Criptografía preparada?*, Jornadas Técnicas de RedIRIS 2019, Sevilla, mayo, 2019.

20. *Are difficult Math problems enough to protect sensitive information?*, Applied Algebra and Optimization Research Center (AORC), SungKyunKwan University, Seúl (Corea), May 3, 2019.

21. *Are difficult Math problems enough to protect sensitive information?*, Department of Mathematics, Seoul National University, Seúl (Corea), May 7th, 2019.

22. *Are difficult Math problems enough to protect sensitive information?*, Department of Mathematics, Pusan National University, Pusan (Corea), May 9th, 2019.

23. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Programa de Excelencia en Bachillerato, IES Avenida de los Toreros, Madrid, 11 Abril 2019.

24. *Criptografía y Seguridad: Realidades, Mitos y Leyendas*, Chateando con la Ciencia, Instituto de Ciencia de Materiales de Aragón (CSIC), Zaragoza, 21 Marzo 2019.

25. *La Criptografía.* Ciclo de conferencias: ¿Qué sabemos de...?, CSIC, Madrid, 5 de octubre de 2017.

26. *Investigación en Criptografía: Retos clásicos y Problemas actuales.* Aula Ortega y Gasset, Universidad Internacional Menéndez Pelayo, Santander, 26 de agosto de 2016.

27. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Programa de Excelencia en Bachillerato, IES Los Rosales, Móstoles, Madrid, Abril, 2016.

28. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Instituto de Bachillerato (de Excelencia) IES Francisco Umbral, Ciempozuelos, Madrid, Febrero, 2016.

29. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Instituto de Bachillerato (de Excelencia) IES Arquitecto Ventura Rodríguez, Boadilla del Monte, Madrid, Febrero, 2016.

30. *Cómo hacer secreta la información: Un Problema de las Matemáticas*, Dirección Provincial de Educación, Palencia, Febrero, 2016.

31. *Modelos de colaboración en la industria de la ciberseguridad*, CyberCamp 2015, Instituto Nacional de Ciberseguridad INCIBE, Madrid, Noviembre, 2015.

32. *Matemáticas y Criptografía*, Asociación Castellana y Leonesa de Educación Matemática "Miguel de Guzmán", Salamanca, Abril, 2015.

33. *El DNIe*, IES Vallecas, Marzo, 2015.

34. *Cryptography with mathematical tools and beyond*, Department of Mathematics, Cheju National University, Cheju (Corea), March 2015.

35. *Las Firmas y los Certificados electrónicos (de la Administración Pública del Estado-CSIC)*, Instituto de Tecnologías Físicas "Leonardo Torres Quevedo", CSIC, Noviembre, 2014.

36. *Anonimato y firmas digitales: firma múltiple y firma grupal*, Escuela Politécnica Superior, Universidad Autónoma de Madrid, Madrid, Diciembre 2011.

37. *Una aproximación a las firmas digitales no estándares: la firma múltiple*, VI International Conference on Non Associative Algebra and its Applications, Zaragoza, Noviembre 2011.

38. *Convirtiendo la Información en Secretos*, Escuela Universitaria de Relaciones Laborales, Universidad de Salamanca, Zamora, Diciembre 2010.

39. *La firma electrónica*, Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Madrid, Mayo 2010.

40. *De la escítala griega a la criptografía cuántica, pasando por los números primos*, IV Congreso Académico, Instituto Tecnológico Superior de Misantla, Veracruz, México, 10 Septiembre 2009.

41. *Criptografía con curvas hiperelípticas de género* 2, Congreso de la Real Sociedad Matemática Española (RSME 2009), Oviedo, 9 Febrero 2009.

42. *Fundamentos matemáticos de la Criptografía Asimétrica*, Seminario del Instituto Universitario de Matemáticas y Aplicaciones (IUMA), Universidad de Zaragoza, 23 Enero 2009.

43. *El criptosistema de Chor-Rivest: estado actual y perspectivas de futuro*, Seminario del Grupo de Criptografía y Seguridad de la Información, de la Universidad de Oviedo, 8 Noviembre 2008.

44. *Cryptology from a mathematical point of view*, Department of Mathematics, Sung Kyun Kwan University, Seúl (Corea), 20 Marzo 2008.

45. *Some mathematical problems in Cryptography*, Department of Mathematics, Cheju National University, Cheju (Corea), 18 Marzo 2008.

46. *El DNI-e: Una nueva identificación*, Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Madrid, Diciembre 2006.

47. *Criptografía gráfica: criptografía visual, cifrado de imágenes y reparto de imágenes secretas con autómatas celulares*, Escuela Técnica Superior de Ingeniería de Telecomunicaciones, Universidad de Málaga, Málaga, Febrero 2006.

48. *Introducción a la Criptología y a sus problemas matemáticos*, Escuela Superior de Ingeniería de Telecomunicaciones, Universidad de Cartagena, Cartagena, Enero 2005.

49. *Sobre las claves privadas pequeñas del criptosistema RSA*, Facultad de Ciencias, Universidad de Salamanca, Salamanca, Junio 2004.

50. *Hidden monomial cryptosystems*, Auburn University, Auburn, Alabama (USA), Marzo 1997.

51. *Pseudorandom bit generators*, Auburn University, Auburn, Alabama (USA), Febrero 1997.

52. *Invariant differential forms on the first jet prolongation of the cotangent bundle*, Technical University "Gh. Asachi", Iasi (Rumanía), Septiembre 1996.

53. *Criptografía de Clave Pública y Aplicaciones*. Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Madrid, Junio 1993.

Revisor de Revistas

1. Acta Mathematica Scientia
2. Acta Mathematica Sinica
3. Applied Mathematics Letters
4. Computers & Education
5. Computers and Mathematics with Applications
6. Computers Physics Communications
7. Computing Letters
8. Electronic Letters
9. Finite Fields and their Applications
10. IET Information Security
11. Information
12. Information Processing Letters
13. Information Sciences
14. International Journal for the Foundations of Computer Science
15. International Journal of Applied Metaheuristic Computing
16. International Journal of Computer Mathematics
17. International Journal on Information Technologies and Security
18. International Journal on Network Security
19. Journal of Mathematical Cryptology
20. Journal of Systems and Software
21. Mathematical Reviews
22. Physics Letters A
23. Science in China
24. Security and Communication Networks
25. Signal Processing: Image Communication
26. The Open Mathematics Journal
27. Theoretical Computer Science
28. Wireless Networks

Cursos impartidos de Especialización y Postgrado

1. Curso de Formación: *La firma electrónica: qué es y cómo se usa*, 15 horas. Servicio de Relaciones Laborales, Formación y Acción Social, Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), Madrid, Abril 2024.

2. Curso de Máster: *Criptografía*, 25 horas. Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, Octubre-Diciembre 2023.

3. Curso de Especialización: *XXXII Curso de Especialidades Criptológicas*, 20 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Junio 2023.

4. Curso de Formación: *La firma electrónica: qué es y cómo se usa*, 15 horas. Servicio de Relaciones Laborales, Formación y Acción Social, Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), Madrid, Abril 2023.

5. Curso de Máster: *Criptografía*, 25 horas. Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, Octubre-Diciembre 2022.

6. Curso de Especialización: *XXXI Curso de Especialidades Criptológicas*, 20 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Junio 2022.

7. Curso de Formación: *La firma electrónica: qué es y cómo se usa*, 15 horas. Servicio de Relaciones Laborales, Formación y Acción Social, Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), Madrid, Marzo 2022.

8. Curso de Máster: *Criptografía*, 25 horas. Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, Octubre-Diciembre 2021.

9. Curso de Especialización: *XXX Curso de Especialidades Criptológicas*, 20 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Junio 2021.

10. Curso de Formación: *La firma electrónica: qué es y cómo se usa*, 15 horas. Servicio de Relaciones Laborales, Formación y Acción Social, Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), Madrid, Abril 2021.

11. Curso de Máster: *Criptografía*, 25 horas. Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, Octubre-Diciembre 2020.

12. Curso de Máster: *Criptografía*, 25 horas. Máster en Ciberseguridad, Universidad Pontificia de Comillas, ICAI, Madrid, Octubre-Diciembre 2019.

13. Curso de Especialización: *XXIX Curso de Especialidades Criptológicas*, 20 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Junio 2019.

14. Curso de Especialización: *XXVIII Curso de Especialidades Criptológicas*, 15 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Junio 2017.

15. Curso de Máster: *Criptografía*, 12 horas. Máster INDRA en Ciberseguridad, Centro Universitario de Tecnología y Arte Digital (U-TAD), Madrid, Noviembre-Diciembre 2016.

16. Curso de Especialización: *XXVII Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Mayo-Junio 2016.

17. Curso de Máster: *Criptografía*, 12 horas. Máster INDRA en Ciberseguridad, Centro Universitario de Tecnología y Arte Digital (U-TAD), Madrid, Noviembre-Diciembre 2015.

18. Curso de Especialización: *XXVI Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Octubre 2015.

19. Curso de Máster: *Criptografía*, 15 horas. Máster INDRA en Ciberseguridad, Centro Universitario de Tecnología y Arte Digital (U-TAD), Madrid, Noviembre-Diciembre 2014.

20. Curso de Especialización: *XXV Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Octubre 2014.

21. Curso: *1513 IFCT05TIC Experto en criptografía y seguridad informática (Programa de formación e inserción laboral de demandantes de empleo en tecnologías de la información y de las comunicaciones y de la economía digital)*, 45 horas. Centro Universitario de Tecnología y Arte Digital (U-TAD), Madrid, Diciembre 2013/Enero 2014.

22. Curso de Especialización: *XXIV Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de la Presidencia, Madrid, Octubre 2013.

23. Curso de Máster: *Sistemas Criptográficos. El Estado de la Técnica*, 10 horas. Máster de Ciencia y Tecnología Informática. Universidad Carlos III, Madrid, Enero 2013.

24. Curso de Especialización: *XXIII Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Octubre 2011.

25. Curso de Especialización: *Cifrado Asimétrico, XII Curso INFOSEC*, 4 horas. Departamento de Ciencias y Técnicas Aplicadas (CYTA). Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT). Ministerio de Defensa, Madrid, Abril 2011.

26. Curso de Especialización: *XXII Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Noviembre 2010.

27. Curso de Especialización: *Cifrado Asimétrico, XI Curso INFOSEC*, 4 horas. Departamento de Ciencias y Técnicas Aplicadas (CYTA). Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT). Ministerio de Defensa, Madrid, Abril 2010.

28. Asignatura de Libre Elección: *Criptografía y Seguridad de la Información*, 6 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2009-2010.

29. Curso de Especialización: *XXI Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Noviembre 2009.

30. Curso de especialización: *Criptografía*, Instituto Tecnológico Superior de Misantla, Veracruz, México, Septiembre 2009.

31. Asignatura de Libre Elección: *Criptografía y Seguridad de la Información*, 6 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2008-2009.

32. Curso de Especialización: *Cifrado Asimétrico, X Curso INFOSEC*, 4 horas. Departamento de Ciencias y Técnicas Aplicadas (CYTA). Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT). Ministerio de Defensa, Madrid, Abril 2009.

33. Curso de Especialización: *XX Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Noviembre 2008.

34. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso 2007-2008.

35. Asignatura de Libre Elección: *Criptografía y Seguridad de la Información*, 6 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2007-2008.

36. Curso de Especialización: *Cifrado Asimétrico, IX Curso INFOSEC*, 4 horas. Departamento de Ciencias y Técnicas Aplicadas (CYTA). Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT). Ministerio de Defensa, Madrid, Abril 2008.

37. Curso de Especialización: *XIX Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Noviembre 2007.

38. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso 2006-2007.

39. Asignatura de Libre Elección: *Criptografía y Seguridad de la Información*, 6 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2006-2007.

40. Curso de Especialización: *XVIII Curso de Especialidades Criptológicas*, 10 horas. Centro Criptológico Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Madrid, Noviembre 2006.

41. Curso de Verano de la UNED: *Los retos de las TICs en el siglo XXI*. "La protección de la información". Centro asociado de la UNED, Pontevedra. Julio 2006.

42. Curso de Doctorado: *Introducción a la Algorítmica y Criptografía Cuánticas*. "Estado del arte de la criptografía pre-cuántica", 1 crédito. Dpt. de Matemática Aplicada, Escuela Universitaria de Informática, Universidad Politécnica de Madrid. Curso 2005-2006.

43. Asignatura de Libre Elección: *El criptosistema RSA. Aplicaciones y Protocolos*, 3 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2005-2006.

44. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso 2005-2006.

45. Curso de Especialización (docencia y dirección): *Introducción a la criptografía de clave pública: Aplicación en el aula*, 3 créditos. Consejería de Educación de la Comunidad de Madrid y Consejo Superior de Investigaciones Científicas, Madrid. Curso: 2005-2006.

46. Curso de Verano: *De la Máquina Enigma a la Firma Digital*. "Firmas y certificados digitales". Dpt. Matemática Aplicada, Universidad de Salamanca. Salamanca, Septiembre 2005.

47. Curso de Doctorado: *Introducción a la Algorítmica y Criptografía Cuánticas*. "Criptografía Clásica", 1 crédito. Dpt. de Matemática Aplicada, Escuela Universitaria de Informática, Universidad Politécnica de Madrid. Curso 2004-2005.

48. Curso de Especialización (docencia y dirección): *Criptosistemas de tipo RSA. Aplicaciones*, 3 créditos. Dpt. Postgrado y Especialización, Consejo Superior de Investigaciones Científicas, Madrid. Curso: 2004-2005.

49. Curso de Especialización: *Criptografía: Seguridad en la transmisión de textos e imágenes*. Dpt. Matemática Aplicada, Universidad de Salamanca. Béjar, Curso 2004-2005.

50. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso 2004-2005.

51. Asignatura de Libre Elección: *Criptosistemas de tipo RSA*, 3 créditos. Dpt. Matemática Aplicada a las Tecnologías de la Información, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. Madrid, Curso: 2004-2005.

52. Curso de Doctorado: *Criptografía: Transmisión y almacenamiento seguro de imágenes*, 3 créditos. Programa de Doctorado: Ciencia y Tecnología de la Ingeniería Geodésica y Cartografía, Universidad de Salamanca. Ávila, Curso: 2004-2005.

53. Curso de Especialización: *Criptografía: Seguridad en la transmisión de textos e imágenes*. Dpt. Matemática Aplicada, Universidad de Salamanca. Ávila, Curso 2004-2005.

54. Curso de Especialización: *Diseño de protocolos criptográficos mediante autómatas celulares*. Dpt. Matemática Aplicada, Universidad de Salamanca. Ávila, Curso 2004-2005.

55. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso 2003-2004.

56. Curso de Especialización (docencia y dirección): *El criptosistema RSA*, 3 créditos. Dpt. Postgrado y Especialización, Consejo Superior de Investigaciones Científicas. Madrid, Curso: 2003-2004.

57. Curso de Doctorado: *Técnicas criptográficas para la protección de la información en Internet*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso: 2002-2003.

58. Curso de Doctorado: *Técnicas criptográficas para la protección de la información en Internet*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso: 2001-2002.

59. Curso de Doctorado: *Técnicas de Análisis Multivariante*, 3 créditos. Programa de Doctorado: Estadística, Dpto. de Estadística e Investigación Operativa, Universidad de Salamanca. Salamanca, Curso: 2000-2001.

60. Curso de Doctorado: *Técnicas criptográficas*, 1,5 créditos. Programa de Doctorado: Procesos de formación en espacios virtuales, Instituto Universitario de Ciencias de la Educación, Universidad de Salamanca. Salamanca, Curso: 2000-2001.

61. Curso de Especialización: *La Criptografía como fuente de problemas matemáticos*, Centro de Profesores y Recursos de Salamanca. Salamanca, Curso: 2000-2001.

62. Curso de Especialización: *Taller de Cripto-Matemáticas*, Centro de Profesores y Recursos de Salamanca. Salamanca, Curso: 1999-2000.

63. Curso de Especialización y postgrado: *Didáctica de la Estadística y la Probabilidad*, 3 créditos. Universidad de Salamanca. Salamanca, Curso: 1997-1998.

64. Curso de Especialización y postgrado: *Formación para el proyecto de Aldea Digital*, 3,5 créditos. Centro de Profesores y Recursos de Zamora. Zamora, Curso: 1998-1999.

Miembro de Tribunales de Tesis Doctorales

1. . Doctorando: Petter Solnør, Director: Prof. Thor I. Fossen and Prof. Slobodan Petrovic. Norwegian University of Science and Technology, Trondheim (Noruega), June, 2023. First Opponent (President).

2. *Applications of Cryptographic Methods in Feedback Control.* Doctorando: Petter Solnør, Director: Prof. Thor I. Fossen and Prof. Slobodan Petrovic. Norwegian University of Science and Technology, Trondheim (Noruega), June, 2023. First Opponent (President).

3. *Biopotential Signals and their Applicability to Cybersecurity Problems.* Doctorando: Caterina Fuster Barceló, Directores: Carmen Cámara Núñez y Pedro Peris López. Universidad Carlos III de Madrid, Escuela Politécnica Superior. Departamento de Informática. Diciembre, 2022.

4. *Caracterización y Análisis de la Propagación de Ciberataques Jamming en Redes de Sensores Inalámbricos mediante Modelos Epidemiológicos.* Doctorando: M. López Delgado, Directores: A. Peinado Domínguez y A. Ortiz García. Universidad de Málaga, Escuela Técnica Superior de Ingenieros de Telecomunicación. Julio, 2022.

5. *Constrained Approximate Search and Data Reduction Techniques in Cybersecurity and Digital Forensics.* Doctorando: Ambika Shrestha Chitrakar, Director: Prof. Slobodan Petrovic. Norwegian University of Science and Technology, Faculty of Information Technology and Electrical Engineering, Department of Information Security and Communication Technology, Gjøvik (Noruega), Noviembre, 2019. First Opponent (President).

6. *Contribuciones a la cardinalidad de curvas elípticas y a los volcanes de isogenias.* Doctorando: J. Valera Martín, Directores: Mirelle Fouquet y Josep M. Miret. Universidad de Lérida, Departamento de Matemáticas, Septiembre, 2017.

7. *Identidad digital evolutiva.* Doctorando: J.L. Tornos Martínez, Director: J.L. Salazar Riaño. Universidad de Zaragoza, Departamento de Ingeniería Electrónica y Comunicaciones, Febrero, 2016. Presidente del Tribunal.

8. *Sistema de ayuda a la selección de soluciones de protección de datos personales, para los productos y servicios en "internet de las cosas".* Doctorando: J.A. Sánchez Alcón, Directores: L. López Sanchidrián y J. Fernán Martínez Ortega. Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicaciones, Febrero, 2016.

9. *Vector Boolean functions: Applications in Symmetric Cryptography.* Doctorando: J.A. Álvarez Cubero, Director: P.J. Zufiria. Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Departamento de Matemática Aplicada a las Tecnologías de la Información, Diciembre, 2015.

10. *Study of stochastic and machine learning techniques for anomaly based web attack detection.* Doctorando: C. Torrano Giménez, Directores: G. Álvarez Marañón y J. Carbó Rubiera. Universidad Carlos III de Madrid, Escuela politécnica Superior, Ingeniería Informática, Departamento de Informática, Septiembre, 2015. Presidente del Tribunal y Tesis con mención internacional.

11. *Design and implementation of secure protocols for practical authentication and fair anonymity systems.* Doctorando: J. Díaz Vico, Directores: F. de Borja Rodríguez Ortiz y D. Arroyo Guardeño. Universidad Autónoma de Madrid, Escuela Politécnica Superior, Departamento de Ingeniería Informática, Mayo, 2015. Presidente del Tribunal y Tesis con mención internacional.

12. *Desarrollo de un sistema exportable de confianza corporativa. Aplicación a entornos de trazabilidad de productos.* Doctorando: G. Azuara Guillén, Director: J.L. Salazar Riaño. Universidad de Zaragoza, Departamento de Ingeniería Electrónica y Comunicaciones, Junio, 2013.

13. *Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable.* Doctorando: E. Pérez Belleboni, Directores: A. Gómez Oliva y J. Carracedo Gallardo. Universidad Politécnica de Madrid, Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Departamento de Ingeniería y Arquitecturas Telemáticas, Marzo, 2013.

14. *Evaluation methodologies for security testing of biometric systems beyond technological evaluation.* Doctorando: M.B. Fernández Saavedra, Director: R. Sánchez Reíllo. Mención Internacional, Universidad Carlos III de Madrid, Departamento de Tecnología Electrónica, Marzo, 2013.

15. *Contribución al estudio del criptoanálisis y diseño de los criptosistemas caóticos.* Doctorando: A.B. Orúe López, Directores: C. Sánchez Ávila y G. Álvarez Marañón. Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Departamento de Matemática Aplicada a las Tecnologías de la Información, Enero, 2013.

16. *Seguridad y confianza en la e-Cognocracia.* Doctorando: D. Joan Josep Piles Contreras, Director: J.L. Salazar Riaño. Universidad de Zaragoza, Departamento de Ingeniería Electrónica y Comunicaciones, Mayo, 2012.

17. *Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model.* Doctorando: D. Jorge López Hernández-Ardieta, Directora: A.I. González-Tablas Ferreres. Universidad Carlos III de Madrid, Departamento de Ingeniería y Ciencias de la Computación, 2011.

18. *Automatización de procedimientos en esteganografía y estegoanálisis lingüístico utilizando la lengua española.* Doctorando: D. Alfonso Muñoz Muñoz, Director: J. Carracedo Gallardo. Universidad Politécnica de Madrid, Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Departamento de Ingeniería y Arquitecturas Telemáticas, 2010.

19. *Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems.* Doctorando: D. David Arroyo Guardeño, Directores: G. Álvarez Marañón y G. Pastor Dégano. Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros Agrónomos, Departamento de Física y Mecánica Fundamentales Aplicadas a la Ingeniería Forestal, 2009.

20. *Rational exchange protocols.* Doctorando: Dª A. Alcaide Raya, Directores: J.M. Estévez Tapiador y A. Ribagorda Garnacho. Universidad Carlos III de Madrid, Departamento de Ciencias de la Computación, 2009.

21. *Problemas de clasificación de curvas en variedades riemannianas.* Doctorando: D. Víctor Fernández Mateos, Directores: J. Muñoz Masqué y M. Castrillón López. Universidad Complutense de Madrid, Facultad de Matemáticas, Departamento de Geometría y Topología, 2008.

22. *Números primos especiales y sus aplicaciones criptográficas.* Doctorando: D. Raúl Durán Díaz, Directores: F. Montoya Vitini y J. Muñoz Masqué. Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Departamento de Física Aplicada a las Tecnologías de la Información, 2003.

23. *Aplicación de Internet como nuevo espacio de formación y comunicación para los centros de primaria y secundaria.* Doctorando: Dª Mª Jesús Verdú Pérez, Directores: R. Mompó y J. García Carrasco. Universidad de Valladolid, Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática, 1999.

24. *La teleeducación como base de la enseñanza universitaria y de la formación continua en Castilla y León.* Doctorando: Dª María A. Pérez Juárez, Directores: R. Mompó y J. García Carrasco. Universidad de Valladolid, Escuela Técnica Superior de Ingenieros de Telecomunicaciones, Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática, 1999.

25. *Desarrollos curriculares de la ciencia de los computadores en la enseñanza elemental.* Doctorando: D. Ricardo López Fernández, Directores: J. García Carrasco. Universidad de Salamanca, Facultad de Educación, Departamento de Teoría e Historia de la Educación, 1999.

26. *Curvas elípticas módulo N y Aplicaciones Criptográficas.* Doctorando: D. Sebastiá Martín Molleví, Directores: P. Morillo Bosh. Universitat Politècnica de Catalunya, Departamento de Matemàtica Aplicada i Telemàtica, 1998.

27. *Órbitas de las funciones cuadráticas sobre cuerpos finitos. Aplicaciones a la generación de números pseudoaleatorios y al diseño de criptosistemas.* Doctorando: D. Alberto Peinado Domínguez, Directores: F. Montoya Vitini y J. Muñoz Masqué. Universidad Politécnica de Madrid, Facultad/Escuela: Facultad de Informática, Departamento de Lenguajes y Sistemas Informáticos e Ingeniería del Software, 1997.

Premios y Distinciones

1. Condecorado con la "Cruz al Mérito Policial con Distintivo Blanco", del Ministerio del Interior, 3 de octubre de 2022.

2. Galardonado con el Premio Nacional "CCN-2021 A la trayectoria profesional en favor de la Ciberseguridad", del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), Ministerio de Defensa, 30 de noviembre de 2021.

3. Tutor del trabajo Fin de Máster *Towards Privacy Preserving Sensor-Based Continuous Authentication*, presentado por L. Hernández Álvarez, galardonado con una Mención Especial en la III Edición (2020) de los Premios "Tengo un Proyecto" en el Área de Criptología y Seguridad de la Información, patrocinado por el Centro Criptológico Nacional.

4. Tutor del trabajo Fin de Máster *Towards Privacy Preserving Sensor-Based Continuous Authentication*, presentado por L. Hernández Álvarez, galardonado con el Primer premio al Mejor Trabajo Fin de Máster, organizado por la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC) en su edición de 2020.

5. Premio al mejor trabajo de investigación: I. Querejeta Azurmendi, J. López Hernández-Ardieta, V. Gayoso Martínez, L. Hernández Encinas, D. Arroyo Guardeño, "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.

6. Finalista del "V Premio Möbius Barcelona Multimedia" (1999), con el CD-ROM "Resolución de problemas en Matemáticas".

Tutoría de alumnos y profesores con estancias de investigación

1. Tutor de un becario JAE Intro-ICU (Diego Rojas Rodríguez) dentro del programa de becas JAE Intro, convocado por el CSIC, desde el 16/08/2024 hasta el 15/06/2025.

2. Tutor de un becario (Fernando Contreras Alcalá) dentro del Programa de Cooperación Educativa entre la Fundación Max Mazin y el CSIC. Título del Proyecto: *Ataques por canal lateral a dispositivos criptográficos,*. Duración: desde el 28/06/2024 hasta el 30/07/2024.

3. Tutor de un becario (Diego Rojas Rodríguez) dentro del Programa de Cooperación Educativa entre la Fundación Max Mazin y el CSIC. Título del Proyecto: *Análisis de la implementación en C de la librería LIBOQS de algoritmos postcuánticos.* Duración: desde el 29/05/2023 hasta el 07/07/2023.

4. Tutor de Alberto Sánchez del Monte, alumno de doctorado dentro del Acuerdo de Cooperación para la Realización de Tesis Doctorales y/o Actividades Prácticas de Programas de Doctorado entre la Universidad de Salamanca y el CSIC. Título del Proyecto: *Inteligencia artificial aplicada a la predicción de ciberataques.* Duración: desde el 17/04/2023 hasta el 17/07/2023.

5. Tutor de Hadrián Rodríguez César, alumno del Master 2 Mathématiques de l'Information, Cryptographie, dentro del Programa de Cooperación Internacional para prácticas de máster entre la Universidad de Rennes (Francia) y el CSIC. Título del Proyecto: *Study the state of the art for the format-preserving cryptosystems based on the NIST SP 800-38G, focusing on multimedia supports (namely image support) and a possible software implementation.* Duración: desde el 11/03/2019 al 13/09/2019.

6. Tutor de José Diamantino Hernández Guillén, alumno de doctorado de la Universidad de Salamanca, durante una estancia de investigación en el CSIC. Título del Proyecto: *Modelización matemática para la simulación de la propagación de malware en redes de ordenadores.* Duración: desde el 01/01/2018 hasta el 31/07/2018.

7. Tutor de Marta Mójica López, Promoción de Empleo y Garantía Juvenil. Ministerio de Educación y el CSIC. Duración: desde el 03/05/20 hasta el 30/04/2018.

8. Tutor de Jingyi Zhang, estudiante del Master of Science in Information Technology de la Hong Kong University of Science and Technology (HKUST), dentro del Programa de Cooperación entre la HKUST y el CSIC. Título del Proyecto: *Analysis and implementation of cryptographic algorithms related to cryptocoins (crptocurrencies) by means of CUDA architecture.* Duración: desde el 20/06/2016 hasta el 20/12/2016.

9. Tutor de Marta Conde Pena, beneficiaria de una Ayuda de Formación de Personal Investigador (FPI), con referencia BES-2012-056689, asociada al Proyecto *Identificación y Autenticación Seguras en Comunicaciones electrónicas (IDEASECe)* del Plan Nacional de I+D+i, Ministerio de Ciencia e Innovación, TIN2011-22668.

10. Tutor de Jesús García de Jalón de la Fuente, profesor de Enseñanza Secundaria, durante su Licencia por Estudios (Modalidad A3) del Ministerio de Educación y Ciencia. Título del Proyecto: *Desarrollo de materiales de aula para la enseñanza de la Criptología.* Duración: Septiembre de 2006 a Agosto de 2007.

11. Tutor de un becario CSIC predoctoral (Ref: I3P-BPD2002-1). Título: *Factorización de polinomios sobre cuerpos finitos y sus aplicaciones a la Criptología.* Diciembre de 2002.

Otros méritos o aclaraciones que se desee hacer constar

1. Evaluación positiva de cinco Tramos de Actividad Investigadora (Sexenios), 1993/1998, 1999/2004, 2005/2010, 2011/2016 y 2017-2022.

2. Evaluación positiva de un Tramo de Actividad Investigadora Transferencia de Conocimiento e Innovación (Sexenio Tecnológico), 2001/2011.

3. Evaluación positiva de seis Tramos de Méritos Investigadores (Quinquenios), (1987/1991) 1992/1996, 1997/2001, 2002/2006, 2007/2011, 2012/2016, 2017/2021.

4. Asesor en temas de Criptografía y Seguridad del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), Ministerio de la Presidencia.

5. Especialista "Técnico Superior en Seguridad de las Tecnologías de la Información y Telecomunicaciones" para el Organismo de Certificación del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), Ministerio de la Presidencia, desde el 12/07/2010.

6. Jefe de Seguridad del Servicio de Protección de Información Clasificada nacional del CSIC (JSSP) y Jefe de Seguridad del Servicio Central de Protección de Información Clasificada nacional del CSIC (SCPIC). Presidencia del CSIC, 22/12/2019.

7. Representante del patrono persona jurídica CSIC en el Patronato de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad, Vicepresidenta de Organización y Relaciones Institucionales, 09/10/2020.

8. Director del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" del Consejo Superior de Investigaciones Científicas, desde el 25/07/2014 al 3/08/2022.

9. Realización de "Curso de Formación Directiva y Gerencial del CSIC" organizado por el Instituto Nacional de Administración Pública, del Ministerio de Hacienda y Administraciones Públicas, 60 horas, Octubre-Noviembre 2014.

10. Director (en funciones) del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" del Consejo Superior de Investigaciones Científicas, 01/07/2013-24/07-2014.

11. Director (en funciones) del Instituto de Seguridad de la Información del Consejo Superior de Investigaciones Científicas, 02/11/2012-20/06/2013.

12. Vocal, desde 2011 al 2018, del Subcomité CTN71/SC27 de la Asociación Española de Normalización (UNE, antes AENOR) "Tecnologías de la Información. Técnicas de Seguridad".

13. Vocal, desde 2011, del Subcomité CTN71/SC38 de la Asociación Española de Normalización (UNE, antes AENOR) "Tecnologías de la Información. Servicios y Plataformas para Aplicaciones distribuidas".

14. Miembro del "Grupo de Trabajo para la Seguridad y Confianza" de la Dirección General para el Desarrollo de la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio.

15. Miembro del Comité Editorial de la revista *Confirma*, dedicada a seguridad documental.

16. Miembro del Jurado de los Premios de Investigación Fundación Policía Nacional en las convocatorias de 2018, 2019, 2020, 2021, 2022.

17. Chairman invitado en numerosos congresos nacionales e internacionales.

18. Miembro de la International Association for Cryptologic Research (IACR, `https://www.iacr.org`).

19. Miembro de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC, `http://www.renic.es/es/index.html`).

20. Miembro de la Real Sociedad Matemática Española (RSME, `http://www.rsme.es/`).

21. Miembro de la Sociedad Española de Matemática Aplicada (SEMA, `http://www.sema.org.es/es`).

22. Consultor de la empresa SIGNE S.A., Impresores de Seguridad (http://www.signe.com/)

23. Organizador y responsable del *Taller de Criptografía 2021*, Semana de la Ciencia y la Tecnología en el CSIC-2021, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2021.

24. Organizador y responsable del *Taller de Criptografía 2019*, Semana de la Ciencia y la Tecnología en el CSIC-2019, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2019.

25. Organizador y responsable del *Taller de Criptografía 2017*, XVII Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2017.

26. Organizador y responsable del *Taller de Criptografía 2016*, XVI Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2016.

27. Organizador y responsable del *Taller de Criptografía 2015*, XV Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2015.

28. Organizador y responsable del *Taller de Criptografía 2014*, XIIII Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2014.

29. Organizador y responsable del *Taller de Criptografía 2013*, XIII Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid, Noviembre, 2013.

30. Organizador y responsable del *Taller de Criptografía 2012-Alan Turing*, XII Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Seguridad de la Información, CSIC, Madrid, Noviembre, 2012.

31. Organizador y responsable del *Taller de Criptografía y Seguridad*, XI Semana de la Ciencia y la Tecnología en el CSIC, Instituto de de Seguridad de la Información, CSIC, Madrid, Noviembre, 2011.

32. Organizador y responsable del *Taller de Criptología*, X Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Física Aplicada, CSIC, Madrid, Noviembre, 2010.

33. Organizador y responsable del *Taller de Criptografía*, IX Semana de la Ciencia y la Tecnología en el CSIC, Instituto de Física Aplicada, CSIC, Madrid, Noviembre, 2009.