María Isabel González Vasco

Currículum Vitae

Junio 2024

APARTADOS EN ESTE DOCUMENTO

PRESENTACIÓN

DATOS PERSONALES

Apellidos: González Vasco
Nombre: María Isabel

Código ORCID: https://orcid.org/0000-0002-7452-9121
Web personal: https://sites.google.com/site/maribelurjc/

SITUACIÓN PROFESIONAL ACTUAL

Categoría profesional: Prof. Catedrático de Universidad
Organismo: Universidad Carlos III de Madrid
Centro: Escuela Politécnica Superior
Departamento: Matemática Aplicada

LÍNEAS DE INVESTIGACIÓN

Criptografía Matemática. Seguridad demostrable. Análisis formal de esquemas y protocolos criptográficos, destacando:

- criptoanálisis de esquemas de cifrado e intercambio de clave construidos a partir de teoría de grupos;
- diseño y análisis de protocolos de intercambio de claves para n participantes, en especial con autenticación por contraseñas y seguros en diferentes modelos de criptografía resistente a adversarios cuánticos;
- diseño de protocolos multiusuario para operaciones conjuntistas con garantías de privacidad.

Especialización (Códigos UNESCO): 120308, 1201

FORMACIÓN

LICENCIATURA

Julio 1999 - **Licenciada en Matemáticas** por la Universidad de Oviedo
Especialidad en Estadística. Nota media del expediente: 3.376
Julio 2000 - Obtención del **grado de Licenciada**, mediante tesina, con la calificación de SOBRESALIENTE
Enero 2001 - **Premio Extraordinario de Licenciatura** (Matemática Aplicada). Curso 1998- 1999, Universidad de Oviedo

DOCTORADO

Julio de 2003 - **Doctora por la Universidad de Oviedo**
Programa de doctorado: Matemáticas y Estadística
Título de Tesis: Criptosistemas basados en Teoría de Grupos
Dirigida por: Prof. Consuelo Martínez López
Calificación: Sobresaliente Cum Laude por unanimidad
Enero de 2006 - **Premio Extraordinario de Doctorado.** Universidad de Oviedo

AYUDAS Y BECAS DE FORMACIÓN

1. **Beca de Colaboración** del Ministerio de Educación y Cultura, con aplicación en el Departamento de Matemáticas, Universidad de Oviedo, curso 1998-1999.
2. Beca del **Programa Europeo para la Formación Leonardo da Vinci,** de cooperación Universidad-Empresa, con aplicación en Philips Crypto B.V., Eindhoven, Holanda. Periodo de disfrute: 1 de agosto al 31 de octubre de 1999.
3. Beca **F.P.U**. del Ministerio de Educación y Cultura, con efecto desde 1 de enero de 2000 hasta el 31 de diciembre de 2003 (evaluada positivamente y renovada con periodicidad anual). En el subprograma de estancias de investigación para becarios F.P.U., se obtuvo financiación para dos estancias de investigación en el Instituto IAKS/EISS de la U. de Karlsruhe

PREMIOS RECIBIDOS

Premio de **Honor del Jurado** en la categoría de **Talento STEM** de los We Leadership Awards Madrid 2023

IDIOMAS

1. INGLÉS: **C2**. Proficiency in English (Cambridge), 1994. Certificado de Aptitud del Ciclo Superior (5 Cursos) de la Escuela Oficial de Idiomas, modalidad libre, 1996.
2. ALEMÁN: **B1**. Certificado de Aptitud del Ciclo Superior (3 Cursos) de la Escuela Oficial de Idiomas, modalidad libre, 1995.

TRAYECTORIA PROFESIONAL

- 1/09/1999 - 31/10/1999. **Investigadora en Formación** Philips Crypto B.V., Eindhoven, Holanda.
- 1/01/2000 - 16/03/2003. Becaria del programa **F.P.U.** del M.E.C. Universidad de Oviedo.
- 17/03/2003 - 11/07/2003. **Profesora Ayudante (T.C.)** Universidad de Oviedo.
- 12/07/2003 - 30/09/2003. **Becaria del programa F.P.U. del M.E.C** Universidad de Oviedo.
- 01/10/2003 - 31/05/2004. **Profesora Ayudante (T.C.),** Universidad Rey Juan Carlos
- 01/06/2004 - 06/02/2007. **Profesora Ayudante Doctor (T.C.),** Universidad Rey Juan Carlos
- 07/02/2007 - 16/03/2009. **Profesora Contratado Doctor (T.C.)** Universidad Rey Juan Carlos.
- 05/2015 - 03/2020. **Affiliated Research Professor,** Florida Atlantic University, E.E.U.U.
- 17/03/2009 - 5/04/2021. **Profesora Titular de Universidad.** Universidad Rey Juan Carlos
- 6/04/2021 – 30/12/2022. **Catedrática de Universidad.** Universidad Rey Juan Carlos
- 31.12.2022 - **Catedrática de Universidad.** Universidad Carlos III de Madrid (en comisión de servicios, ocupando una **Cátedra de Excelencia**)

EVALUACIONES

Evaluaciones **positivas de la ANECA** para las figuras de PROFESOR AYUDANTE DOCTOR, PROFESOR CONTRATADO DOCTOR, PROFESOR COLABORADOR, PROFESOR DE UNIVERSIDAD PRIVADA, PROFESORA TITULAR DE UNIVERSIDAD y CATEDRÁTICO DE UNIVERSIDAD (RAMA CIENCIAS)

4 Tramos de Investigación concedidos por la CNEAI (2000-2005, 2006-2011, 2012-2017, 2018-2023).

1 Tramo de Transferencia concedido por la CNEAI (2013-2018).

1. PARTICIPACIÓN EN PROYECTOS DE I+D

A) PROYECTOS EN LOS QUE LA CANDIDATA FUE/ES INVESTIGADOR PRINCIPAL FINANCIADOS EN CONVOCATORIAS PÚBLICAS (nacionales y/o internacionales):

1. Título del proyecto: Cifrado de mensajes: seguridad y eficiencia de los métodos basados en Teoría de Grupos
Entidad financiadora: Fundación Banco Herrero
Duración, desde: 1/05/2004 hasta:1/05/2005
Cuantía de la subvención: 3.000 €
Número de investigadores participantes: 1

2. Título del proyecto: Análisis y desarrollo de herramientas criptográficas basadas en álgebra y matemática discreta. (PPR 2004 - 47)
Entidad financiadora: Universidad Rey Juan Carlos
Duración, desde: 1/01/2005 hasta:31/12/2005
Cuantía de la subvención: 6.000 €
Investigador responsable: María Isabel González Vasco
Número de investigadores participantes: 5

3. Título del proyecto: BASE COAT – Basing Security in Combinatoric and Algebraic Techniques (HA 2004 -0063)
Entidad financiadora: M.E.C – Acciones Integradas Hispano alemanas
Duración, desde: 1/01/2005 hasta:31/12/2006
Cuantía de la subvención: 10.800 €
Investigador responsable: María Isabel González Vasco
Número de investigadores participantes: 6

4. Título del proyecto: SEGURIDAD DEMOSTRABLE: VALIDACION DE HERRAMIENTAS CRIPTOGRAFICAS A TRAVES DEL ALGEBRA Y LA MATEMATICA DISCRETA (MTM2010-15167)
Entidad financiadora: Ministerio de Ciencia e Innovación
Duración, desde: 1/01/2011 hasta:31/12/2013
Cuantía de la subvención: 40.777 €
Investigador responsable: María Isabel González Vasco
Número de investigadores participantes: 5

5. Título del proyecto: SECURE COMMUNICATION IN THE QUANTUM ERA (SPS G5448)
Entidad financiadora: OTAN – SPS Programme
Duración, desde: 30/09/2018 hasta:30/09/2021
Cuantía de la subvención: 264,200€
Investigador responsable: Otokar Grosek (Co-Director España) María Isabel González Vasco
Número de investigadores participantes: 4 (equipo español)

6. Título del proyect: CRIPTOGRAFIA PARA RETOS DIGITALES EMERGENTES: ESCENARIOS MULTIUSUARIO Y SEGURIDAD POST-CUÁNTICA (CREEME) PID2019-109379RB-I00
Entidad Financiadora: Ministerio de Ciencia e Innovación
Duración desde: 1/01/2020 hasta 31/10/2022 [prorrogado hasta 29/02/2024]
Cuantía de la subvención: 37.147€
Investigador Responsable: Javier Herránz Sotocá (IP1) y María Isabel González Vasco (IP2)
Número de investigadores participantes: 9.

7. Título del proyecto: SECURE COMMUNICATION VIA CLASSICAL AND QUANTUM TECHNOLOGIES (SPS G5985)
Entidad financiadora: OTAN – SPS Programme
Duración, desde: 30/03/2023 hasta:30/03/2026
Cuantía de la subvención: 350,000€
Investigador responsable: Rainer Steinwandt (Co-Director España: María Isabel González Vasco

B) PROYECTOS FINANCIADOS EN CONVOCATORIAS PÚBLICAS EN LOS QUE LA CANDIDATA FUE/ES PARTICIPANTE

1. Título del proyecto: Estructura de Grupos y álgebras. Aplicaciones a la Codificación y Criptografía (PB – EXP 01- 33)
Entidad financiadora: FICYT
Entidades participantes: Universidad de Oviedo
Duración, desde: 15/09/2001 hasta: 31/03/2002
Cuantía de la subvención: 20.000 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 10

2. Título del proyecto: Estructura de Grupos y Álgebras. Aplicaciones a la Codificación y Criptografía (PR – 01 – GE -15)
Entidad financiadora: FICYT (Grupos de Excelencia))
Duración, desde: 01/04/2002 hasta: 31/12/2004
Cuantía de la subvención: 47.422 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 8

3. Título del proyecto: Estructura de Grupos y Álgebras. Aplicaciones a Geometría, Codificación y Criptografía (BMF2001-3239-C03-01)
Entidad financiadora: MCYT
Duración, desde: 01/01/2001 hasta: 31/12/2004
Cuantía de la subvención: 52.113,58 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 10

4. Título del proyecto: Estructura de grupos y álgebras. Aplicaciones a Geometría, Codificación y Criptografía (MTM 2004 - 08115 - C 04- 01)
Entidad financiadora: M.E.C
Duración, desde: 10/12/2004 hasta:9/12/2007
Cuantía de la subvención: 95.800 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 11

5. Título del proyecto: Estructuras Algebraicas y Aplicaciones a Teoría de la Información (IB05-186)
Entidad financiadora: FICYT
Duración, desde: 1/12/2005 hasta: 31/12/2007
Cuantía de la subvención: 53.532,64 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 12

6. Título del proyecto: Estructuras Algebraicas No Asociativas, Codificación y Criptografía (MTM2007-67884-C04-01)
Entidad financiadora: M.E.C
Duración, desde:01/10/2007 hasta: 30/09/2010
Cuantía de la subvención: 121.363 €
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 11

7. Título del proyecto: Matemáticas e Información Cuántica CCG07-UCM/ESP-2797
Entidad financiadora: UCM/CAM
Duración, desde: 01/01/2008 hasta: 31/12/2008
Cuantía de la subvención: 5.000 €
Investigador responsable: David Pérez García
Número de investigadores participantes: 5

8.Título del proyecto: Estructuras Algebraicas y aplicaciones a la seguridad de la información (IB08-147)
Entidad financiadora: FICYT
Duración, desde 1/12/2008 a 31/12/2010
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes:12

9. Título del proyecto: 70C0ABC GATES FOR EUROPE (ABC4EU) (Referencia URJC: M1097)
Entidad financiadora: Comisión Europea. VII Programa Marco
Entidades participantes: Universidad Rey Juan Carlos, INDRA, Price Waterhouse Coopers, Vision Box, Universidad de Laurea, Eticas Research and Consulting, Centre for Irish and European Security Limited, Dermalog Identification Systems GMBH, Universita degli Studi di Milano, Safe Id Solutions GMBH, Ministerio del Interior Español, Ministerio da Administracao Interna de Portugal, Politsei- ja P. de Estonia, Ministerul

Afacerilor Interne de Rumanía.
Duración, desde: 01/01/2014 hasta:30/06/2017
Cuantía de la subvención: 666522,88 € (URJC), 20012.015.246,04 (Total proyecto)
Investigador responsable: Enrique Cabello Pardos (URJC)
Número de investigadores participantes: 70

10. Título del proyecto: Hacia una sociedad digital segura: avances matemáticos en criptografía y su impacto en las tecnologías (MTM2013-41426-R)
Entidad financiadora: MINECO (convocatoria RETOS)
Duración, desde: 01/1/2014 hasta: 31/12/2016
Cuantía de la subvención: 42.350 €
Investigador responsable: Jorge Luis Villar Santos
Número de investigadores participantes: 5

11. Título del proyecto: Criptografía avanzada para afrontar nuevos retos de la sociedad digital (MTM2016-77213-R)
Entidad financiadora: MINECO (RETOS)
Duración: enero 2017- diciembre 2019
Cuantía de la subvención: 69.700€
Investigador responsable: Javier Herranz Sotocá
Número de investigadores participantes: 11

12. Título del proyecto: Grupo de Análisis de Redes Complejas en las Ciencias, la Sociedad y la Tecnología (GARECOM)
Entidad financiadora: URJC- Banco Santander (Grupos de excelencia)
Duración: enero 2015- julio 2018
Cuantía de la subvención 30.261,18€
Investigador responsable: Regino Criado Herrero
Número de investigadores participantes: 19

2. PUBLICACIONES (especializadas)

A1) LIBROS

1. (con R. Steinwandt) Group Theoretic Cryptography. En la Serie "Cryptographic and Network Security Series" Taylor and Francis, CRC Press, 2015. ISBN 9781584888369.

A2) CAPÍTULOS DE LIBROS

1. (con T. Beth, S. González, C. Martínez y R. Steinwandt) *Cryptographic Shelter for the Information Society: Modelling and Fighting Novel Attacks on Cryptographic Primitives*. Capítulo del libro: Techno-Legal Aspects of Information Society and New Economy: an Overview. Ed. Formatex. Vol. 1, 'Information Society' Series, ISBN: 84-607-8104-6, pp. 163-170, 2003.

2. (con S. González, C. Martínez y A. Suarez-Corona). *The Roll of Dices in Cryptology.* The Mathematics of the Uncertain: A Tribute to Pedro Gil. Studies in Systems, Decision and Control, Vol 142, Springer International Publishing. ISBN 978-3-319-73848-2, pp 493--504, febrero 2018.

A3) DOCUMENTOS ACADÉMICOS PUBLICADOS COMO LIBROS

1. *Criptosistemas Basados en Teoría de Grupos. Tesis doctoral.* Servicio de Publicaciones de la Universidad de Oviedo, ISBN: 84-8317-373-5, pp.1-136, 2003.

B) ARTÍCULOS LISTADOS EN JCR

Nota: a continuación de cada artículo se incluye el índice de impacto, que, salvo reseña explícita, es del año de publicación. Además, se incluye el área JCR en la que aparece, y su lugar relativo/número total de revistas.

1. M.I. González Vasco, R. Steinwandt. *Clouds over a public key cryptosystem based on Lyndon words.* Information Processing Letters, Vol. 80, pp. 239--242, Elsevier Science, 2001.
Doi: 10.1016/S0020-0190(01)00170-3
JCR 2001: 0.288, Computer Science, Information Systems; 55/73, Q4.

2. M.I. González Vasco, I. E. Shparlinski. *Security of the Most Significant Bits of the Shamir Message Passing Scheme*. Mathematics of Computation, Vol. 71, Num. 237, pp. 333-342, AMS, 2002.
Doi: 10.1090/S0025-5718-01-01358-8
JCR 2002: 1.015, Mathematics, Applied; 29/156. **Q1**.

3. M.I. González Vasco, M. Näsnuld e I. E. Shparlinski. *The Hidden Number Problem in Extension Fields in Its Applications*. Proceedings of LATIN 2002. Lecture Notes in Computer Science, Vol. 2286, pp. 105-117, Springer, 2002.
Doi: 10.1007/3-540-45995-2_14
JCR 2002: 0.515, Computer Science, Theory and Methods; 39/69. Q3

4. M.I. González Vasco, M. Rötteler y R. Steinwandt. *On Minimal Length Factorizations of Finite Groups*. Experimental Mathematics, Vol 12, Num 1. 1-12, 2003.
Doi: 10.1080/10586458.2003.10504708
JCR 2003: 0.480, Mathematics, 74/174. Q2

5. M.I. González Vasco, M. Näsnuld e I.E. Shparlinski. *New results on the Hardness of Diffie-Hellman Bits.* Proceedings of IACR – Public Key Cryptography 2004, Lecture Notes in Computer Science, Vol. 2947, pp. 159-172, Springer, 2004.
Doi: 10.1007/978-3-540-24632-9_12
JCR 2004: 0.513, Computer Science, Theory and Methods; 53/70. Q4

6. M.I. González Vasco, R. Steinwandt. *A Reaction Attack on a Public Key Cryptosystem Based on the Word Problem*. Applicable Algebra in Engineering, Communication and Computing, Vol. 14, Num. 5, pp. 335-340, Springer, 2004.
Doi: 10.1007/s00200-003-0135-3
JCR 2004: 0.531, Matemática Aplicada, 93/162. Q3

7. M.I. González Vasco, C. Martínez y R. Steinwandt. *Towards a Uniform Description of Several Group Based Cryptographic Primitives*. Designs, Codes and Cryptography, Vol. 33, pp. 215-226, Kluwer, 2004
Doi: 10.1023/B:DESI.0000036247.38461.c9
JCR 2004: 0.690, Matemática Aplicada, 62/162. Q2

8. M.I. González Vasco, D. Hoffheinz, C. Martínez y R. Steinwandt. *On the Security of Two Public Key Cryptosystems using non-abelian groups*. Designs, Codes and Cryptography, Vol. 32, pp. 207-216 (Special Issue: Proceedings of the Third Pythagorean Conference), Kluwer, 2004.
Doi: 10.1023/B:DESI.0000029223.76665.7e
JCR 2004: 0.690, Matemática Aplicada, 62/162. Q2

9. J-M. Bohli, M.I. González Vasco, C. Martínez, y R. Steinwandt. *Weak Keys in MST_1*. Designs, Codes and Cryptography, Vol. 37, Num. 3, pp. 509-524, Kluwer, 2005.
Doi: 10.1007/s10623-004-4040-y
JCR 2005: 0.661, Matemática Aplicada, 70/151. Q2

10. M.I. González Vasco, C. Martínez, R. Steinwandt, y J. Villar) *A new Cramer-Shoup like methodology for group based provably secure encryption schemes.* Proceedings of 2nd IACR Theory of Cryptography Conference 2005, Lecture Notes in Computer Science, Vol. 3378, pp. 495- 509, Springer, 2005.
Doi: 10.1007/978-3-540-30576-7_27
JCR 2005: 0.402, Computer Science, Theory and Methods; 62/71. Q4

11. M.I. González Vasco, R. Steinwandt. *Pitfalls in public key cryptosystems based on free partially commutative monoids and groups*. Applied Mathematics Letters, Vol. 19, Num. 10, pp. 1037-1041, Elsevier, 2006.
Doi: 10.1016/j.aml.2005.11.014
JCR 2006: 0.546, Matemática Aplicada, 103/150. Q3.

12. M.I. González Vasco, D. Pérez. *Attacking a Public Key Cryptosystem Based on Tree Replacement*. Discrete Applied Mathematics, Vol. 155, pp. 61-67, Elsevier, 2007.
Doi: 10.1016/j.dam.2006.05.009
JCR 2007: 0.625, Matemática Aplicada, 95/165. Q3

13. R. Criado, J. Flores, M.I. González Vasco y J. Pello. *Choosing a leader on a complex network: a trade-off between robustness and efficiency*. Journal of Computational and Applied Mathematics, Vol. 204, pp. 10-17, Elsevier, 2007.
Doi: 10.1016/j.cam.2006.04.024
JCR 2007: 0.943, Matemática Aplicada, 51/165. Q2

14[1]. J.M. Bohli, M.I. González Vasco y R. Steinwandt. *Secure Group Key Establishment Revisited*. International Journal of Information Security, Vol. 6, Num. 4, pp. 243-254, Springer, 2007.
Doi: 10.1007/s10207-007-0018-x
JCR 2010 (año en que la revista entra en lista del JCR): 1.094 Computer Science, Theory and Methods; 43/97, Q2.

15. M.I. González Vasco, J. Villar. *In search of mathematical primitives for deriving universal projective hash families*. Applicable Algebra in Engineering, Communication and Computing, Vol. 19, Num. 2, pp. 161-173, 2008.
Doi: 10.1007/s00200-008-0068-y
JCR 2008: 0.5 Matemática Aplicada, 143/175, Q4.

16. M.I. González Vasco, A.L. Pérez del Pozo y P. Taborda Duarte. *A note on the security of MST3*. Designs Codes and Cryptography, Vol. 55, p.189--200, 2010.
Doi: 10.1007/s10623-010-9373-0
JCR 2010: 0.771, Matemática Aplicada, 121/236. Q3

17. M.I. González Vasco, A.L. Pérez del Pozo, P. Taborda Duarte y J.L. Villar. *Cryptanalysis of a key exchange scheme based on block matrices*. Information Sciences, Vol. 276, pp. 319-331, 2014.
Doi: 10.1016/j.ins.2013.11.009
JCR 2014: 4.038, Computer science, information systems; 6/139 **Q1**

18. M.I. González Vasco, F. Hess y R. Steinwandt. *Combined schemes for* signature and encryption: the public key and the identity-based setting. Information and Computation, 246, 00, 1-10, 2016.
Doi: 10.1016/j.ic.2015.11.001

[1] Esta revista no entra en JCR hasta 2010, ocupando hasta la fecha posiciones relevantes en distintas listas del JCR.

JCR 2016: 1,05, Mathematics, Applied; 103/255, Q2

19. M.I. González Vasco, A.L. Pérez del Pozo y A. Suárez Corona. *Pitfalls in a Server-Aided Authenticated Group Key Establishment*. Information Sciences, Vol. 363, pp. 1-7, 2016.
Doi: 10.1016/j.ins.2016.05.004
JCR 2016: 4,832, Computer Science, Information Systems; 7/146 **Q1**

20. P. D'Arco, M.I. González Vasco, A.L. Pérez del Pozo, C. Soriente y R. Steinwandt. *Private Set Intersection: New Generic Constructions and Feasability Results.* Advances in Mathematics of Communications, Vol 11, num 3, pp. 481-502, 2017.
Doi:10.3934/amc.2017040
JCR 2017: 0,564, Mathematics, Applied; 217/252, Q4.

21. D. Fiore, M.I. González Vasco y C. Soriente. *Partitioned Group Password-Based Authenticated Key Exchange*. The Computer Journal, Vol 60, No. 12, pp.1912-1922, 2017
Doi: 10.1093/comjnl/bxx078
JCR 2017: 3,378 Computer science, Theory and Methods; 75/103. Q3.

22. M.I. González Vasco, A.L. Pérez del Pozo y A. Suárez Corona. *Group key Exchange protocols withstanding ephemeral key reveals*. IET Information Security, Vol 12, Num. 1, pp. 79-86, 2018.
Doi: 10.1049/iet-ifs.2017.0131
JCR 2018: 0,949 Computer Science, Theory and Methods; 71/105, Q3.

23. M.I. González Vasco, E.P. Fernández-Manzano. *Analytic Surveillance: Big Data Business Models in the Time of Privacy Awareness.* Vigilancia analítica: modelos comerciales de datos masivos y concienciación sobre la privacidad, El Profesional de la Información (EPI), Vol 27, núm 2, 2018.
Doi: 10.3145/epi.2018.mar.19
JCR 2018: 1.505, Information Science & Library Science, 40/89. Q2

24. M.I. González Vasco, J. I. Escribano Pablos, M.E. Marriaga and A. L. Pérez del Pozo. *The Cracking of WalnutDSA: A Survey*, Symmetry 11(9), 1072, 2019.
Doi: 10.3390/sym11091072
JCR 2019: 2.645, Multidisciplinary Sciences, 29/71. Q2

25. J.M. Bohli, M.I. González Vasco y R. Steinwandt. *Password Authenticated Group Key Establishment from Smooth Projective Hash Functions.* International Journal of Applied Mathematics and Computer Science (AMCS), Vol. 29, No. 4, 797–815, 2019.
DOI: 10.2478/amcs-2019-0059
JCR 2019: Mathematics, Applied, 165/260**, T2, Q3**

26. M.I. González Vasco, A.L. Pérez del Pozo y C. Soriente. *A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols*.
IEEE Transactions on Dependable and Secure Computing, vol, 18 (3), 1336-1353, 2021
Doi: 10.1109/TDSC.2019.2919013
JCR 2021: 6.791, Computer Science, Information Systems; 25/164, **Q1.**

27. J.M. Bohli, M.I. González Vasco y R. Steinwandt. *Building Group Key Establishment on Group Theory: A Modular Approach.*
Symmetry, 12(2), 197, 2020.
JCR 2019: 2.645, Multidisciplinary Sciences; 29/71. Q2

28. J.I. Escribano Pablos, M.I. González Vasco, M.E. Marriaga y A. L. Pérez del Pozo. *Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber*. Mathematics, 8, 1853, 2020.
JCR 2019: 1.741, Mathematics; 28/325, **Q1.**

29. M.I. González Vasco, A. Pérez del Pozo y R. Steinwandt. *Group Key Establishment in a Quantum-Future Scenario*. Informatica, 31 (4), pp. 751-768, 2020.
Doi: 10.15388/20-INFOR427
JCR 2020: 2.688, Mathematics, Applied; 35/265, **Q1.**

30. C. González, M.I. González Vasco, F. Johnson, y A.L. Pérez del Pozo. *Concerning Quantum Identification Without Entanglemen*t. Entropy, 23(4), 38, 2021
Doi: https://doi.org/10.3390/e23040389
JCR 2020: 2.524 Physics, Multidisciplinary 38/86 **Q2**

31. J.I. Escribano Pablos, M.I. González Vasco. *Secure post-quantum group key exchange: Implementing a solution based on Kyber*, IET Communications, 1--16, 2023.
JCR 2021: 1.345 ENGINEERING, ELECTRICAL & ELECTRONIC 225/276, **Q4**

C) OTRAS PUBLICACIONES EN REVISTAS Y CONGRESOS INTERNACIONALES, CON PROCESO DE REVISIÓN ANÓNIMO POR PARES E INDICADORES OBJETIVOS DE ALTA CALIDAD

1. M.I. González Vasco, M. Näslund. *A survey of Hard Core Functions*. Cryptography and Computational Number Theory, de la serie: Progress in Computer Science and Applied Logic, Vol. 20, pp. 227-255, Birkhäuser Verlag, 2001.

2. M.I. González Vasco, I.E. Shparlinski. *On the Security of Diffie-Hellman Bits*. Cryptography and Computational Number Theory (Proceedings of CCNT'99), de la serie: Progress in Computer Science and Applied Logic, Vol. 20, pp. 258-268, Birkhäuser Verlag, 2001.

3. M.I. González Vasco, R. Steinwandt. *Obstacles in two public key cryptosystems based on group factorizations*. Cryptology, Vol 25, pp. 23-37, Tatra Mt. Mathemathical Publications, 2002.

4. M.I. González Vasco, R. Steinwandt. *Chosen ciphertext attacks as common vulnerability of some group- and polynomial-based encryption schemes.* Tatra Mountains Mathematical Publications, Vol 33, pp. 149-158, 2006.

5. M.I. González Vasco, R. Steinwandt. *On ideal and subalgebra coefficients in a class of k-algebras*, Note di Matematica, Vol. 27, Num. 1, pp. 77-83, 2007.

6. M.I. González Vasco, R. Steinwandt y J.L. Villar) *Towards Provable Security for Cryptographic Constructions Arising from Combinatorial Group Theory*. Algebraic methods in cryptography, L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger, and V. Shpilrain, eds., Contemporary Mathematics, Vol. 418, pp. 89-101, American Mathematical Society, 2006.

7. W. Geiselmann , M.I. González Vasco, R. Steinwandt. *Entwurf asymmetrischer Kryptographischer Verfahren unter Berücksichtigung von Quantenalgorithmen*. IT-Information Technology, número especial, "Cryptography and Quantum Informatics—dedicado a la memoria del Prof. Thomas Beth), Vol. 48, Num. 6, pp. 327-331, 2006.

8. J.M. Bohli, M.I. González Vasco y R. Steinwandt. *A Subliminal-Free Variant of ECDSA*, Proceedings of 6th Information Hiding, Lecture Notes in Computer Science, Vol. 4437, pp. 375-387, Springer, 2007.

9. M. Abdalla, J.M. Bohli, M.I. González Vasco, y Rainer Steinwandt. *(Password)-Authenticated Key Establishment: from 2-Party to Group,* Proceedings of 3rd IACR Theory of Cryptography Conference, Lecture Notes in Computer Science, Vol. 4392, pp. 499-514, Springer, 2007.

10. M.I. González Vasco, J.Villar y S. Heidervand. *Anonymous subscription schemes (a flexible construction for on-line sevices.* Proc. of the International Conference on Security and Cryptography (SECRYPT 2010), pp. 120-13, 2010.

11. P. D'Arco, M.I. González Vasco, A. L. Pérez del Pozo y C. Soriente. *Size Hiding in Private Set Intersection: Existential Results and Constructions.* Proc of the 5th International Conference on Cryptology (Africacrypt 2012). Lecture Notes in Computer Science, Vol. 7374, pp. 378—394, Springer Verlag, 2012.

12. M.I. González Vasco, S. Heidarvand y J. Villar. *Flexible anonymous subscription schemes*. In CCIS, Vol 222, pp. 203--219, Springer Verlag, 2012

13. M.I. González Vasco, A. Robinson y R. Steinwandt. *Cryptanalysis of a proposal based on the discrete logarithm problem inside Sn*. Cryptography 2, 16, 2018.

14. C. Colombo, M.I. González Vasco, R. Steinwandt y P. Zajac. *Secure Communication in the Quantum Era: (Group) Key Establishment*. In: Palestini C. (eds) Advanced Technologies for Security Applications. NATO Science for Peace and Security Series B: Physics and Biophysics. Springer, Dordrecht, 2020.

15. A. Russo, A. Fernández Anta, M.I. González Vasco y Simon Pietro Romano. *Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures,* In: Proceedings of IEEE Blockchain, Worshop on Security, Application, and Performance (BSAP-2021), IEEE, pp. 417—424, 2021

16. A. Faonio, M.I. González Vasco, C. Soriente and H. T. T. Truong. *Auditable Asymmetric Password Authenticated Public Key Establishment*, In Proceedings of CANS 2022, Lecture Notes in Computer Science, Vol. 13641, pp. 122—142, Springer, 2022.

17. D. Balbás, D. Fiore, M.I. González Vasco, D. Robissout and C. Soriente. *Modular Sumcheck Proofs With Applications to Machine Learning and Image Processing*, CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, November 2023, pp. 1437-1451, 2023.

18. M.I. González Vasco, A. Moreno, A.L. Pérez del Pozo, M. Portela, J. Portilla, J. Señor. *Group Key Exchange: Living on the Edge with a Quantum Adversary* .NATO Science for Peace and Security Series - D: Information and Communication Security. Volume 64, Toward a Quantum-Safe Communication Infraestructure, pp. 106—116, 2024.

19. M.I. González Vasco, D. Kahrobaei, E. McKemmie. *Applications of Finite non-Abelian Simple Groups to Cryptography in the Quantum Era.* La Matematica, Volume 3, pages 588–603, 2024

20. . M.I. González Vasco, R. Steinwandt. *Group Key Establishment in the Post-Quantum Setting: Constructions and Research Avenues* https://www.springer.com/series/13764/books. Springer volume "Proceedings of 2022 AWM Research Symposium" which will be published in the Springer "Association for Women in Mathematics Series."

D) OTRAS PUBLICACIONES: ARTÍCULOS EN ACTAS DE CONGRESOS NACIONALES, O INTERNACIONALES SIN REVISIÓN POR PARES

1. M.I. González Vasco, C. Martínez y R. Steinwandt. *Un Marco Común para Varios Esquemas de Clave Pública Basados en Grupos.* Actas de la VII Reunión Española sobre Criptología y Seguridad de la Información, pp. 351-362, Servicio de Publicaciones de la Universidad de Oviedo, 2002.

2. M.I. González Vasco, R. Steinwandt. *On ideal and subalgebra coefficients in a class of k-algebras*. Abstract en las Actas del First Joint Meeting RSME-AMS, Sevilla, España, 2003.

3. M.I. González Vasco, D. Pérez y R. Steinwandt. *On the Security of Certain Public Key Cryptosystems Based on Rewritting Problems*. Actas de la VIII Reunión Española sobre Criptología y Seguridad de la Información, pp.175-184, Díaz de Santos, 2004.

4. M.I. González Vasco, C. Martínez, R. Steinwandt y J. Villar. *On Provably Secure Encryption Schemes Based on Non-Abelian Groups*. Actas de la VIII Reunión Española sobre Criptología y Seguridad de la Información, pp.101-112, Díaz de Santos, 2004.

5. M.I. González Vasco, *On the security of a group based public key cryptosystem.* Actas del Workshop on Mathematical Problems and Techniques in Cryptology, CRM Quaderns, Num. 31, pp. 91-98, 2005.

6. R. Criado, J. Flores, M.I. González Vasco, y J. Pello) *Locating a leader node on a complex network: a trade-off between robustness and efficiency*. Ac as del congreso Internacional Conference on Computational and Mathematical Methods in Science and Engineering CMMSE-2005, Alicante, España, 2005.

7. M.I. González Vasco, C. Martínez y S. González. *Esquemas de cifrado basados en grupos: pasado y futuro*. Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA, *MAT.ES* . Sesión especial: Tendencias actuales en criptología. Valencia, 2005.

8. M.I. González Vasco, Pedro Taborda. *New steps towards secure word-problems based encryption schemes: analysis of a recent proposal*, IX Reunión Española sobre Criptología y Seguridad de la Información, Barcelona, pp. 276-286, 2006.

9. M.I. González Vasco, A.L. Pérez del Pozo. *Related message attacks: a formal treatment*. X Reunión Española sobre Criptología y Seguridad de la Información, pp. 111-118, Ed. f

10. M.I. González Vasco, A. Pérez del Pozo y A. Suarez Corona. *Modelling ephemeral leakage in group key exchange protocols*, Actas de las I Jornadas Nacionales de Investigación en Ciberseguridad. ISBN: 978-84-9773-742-5. pp. 90-91., 2015.

11. M.I. González Vasco, A. Pérez del Pozo y A. Suarez Corona. *Thwarting randomness reveals in group key agreement,* In Proceedings of the Internacional Conference on Computational and Mathematical Methods in Science and Engineering CMMSE-2016, Cádiz, Spain, 2016.

12. Linares, R., Fernández Manzano, E., & González Vasco, M. I. (2023). Oportunidades de la tecnología blockchain: La industria cinematográfica: Criptomonedas, tokens y NFTs. InMediaciones De La Comunicación, 19(1), 137–159, 2023. https://doi.org/10.18861/ic.2024.19.1.

E. ACTIVIDAD EDITORIAL

- Miembro del **Comité Editorial** de:
    - **Journal of Mathematical Cryptology** (Walter de Gruyter)-(2007-2019).
    - **Mathematical Cryptology** (desde 2020).
    - **International Journal of Computer Mathematics: Computer Systems Theory** (Taylor & Francis) (desde 2020).

- **Co-editora** (junto a R. Steinwandt) del Special Issue: *Applications of Algebra to Cryptography*, Discrete Applied Mathematics, Vol. 156, Num. 16, 2008.
  JCR 2007: 0.625, Matemática Aplicada, 95/165

- **Editora** del Special Issue *Interactions between Group Theory, Symmetry and Cryptography*, de la revista Symmetry, septiembre 2020.

- **Co- editora** del Special Issue *Mathematics of Cryptography and Coding in the Quantum Era*. International Journal of Computer Mathematics Computer Systems Theory, diciembre 2020.

- **Co-editora** (junto a Gretchen Matthews) del Special Issue: MathCrypt 2023, Mathematical Cryptology, Vol 3, Num 2, octubre 2023.

- **Revisora habitual** de las revistas:
    - Applicable Algebra in Engineering, Communication and Computing
    - Applied Mathematics Letters
    - Experimental Mathematics
    - Designs Codes and Cryptography
    - Finite Fields and Applications
    - IEICE Transactions, (special section on Cryptography and Information Security.)
    - IET Transactions on Information Sciences
    - Information Sciences
    - Journal of Cryptology
    - Journal of Pure and Applied Algebra
    - The Computer Journal

- Recensora de **Mathematical Reviews**.
- **Co-chair** del 5th Workshop on Mathematical Cryptology (MathCrypt23), California, EEUU, 2023.
- Miembro del **Comité de Programa** de las conferencias internacionales: WOSIS 2005, STM 2006, WISA 2007, CEDI 2007, IACR- PKC 2008, MMICS, CDGF, ACISP09, IACR-PKC 2010, SCC 2010, ACNS2011, ACISP2011, HMAMS, Africacrypt 2011, ICITS 2011, LatinCrypt 2012 , Latincrypt 2014, ACNS 2019, PQCrypt 2019, IACR-Asiacrypt 2021, LatinCrypt 2022.

- Miembro del **Comité de Programa** de las conferencias nacionales: RECSI (2004,2006, 2008, 2010, 2012, 2014, 2016, 2018,2020), JNIC2015, JNIC2020.

- **Revisora externa** de las conferencias internacionales: IACR- EUROCRYPT 2005, IACR-EUROCRYPT 2006, ESORICS 2006, TATRACRYPT 2007, PAIRING 2008, IACR- PKC 2009, IACR-EGaceUROCRYPT 2016, IACR-CRYPTO 2018.

III. ESTANCIAS EN CENTROS DE INVESTIGACIÓN

1. Estancia PREDOCTORAL. Instituto IAKS/EISS, Universität Karlsruhe, Karlsruhe, Alemania, abril-julio 2001 (14 semanas).

2. Estancia PREDOCTORAL. Instituto IAKS/EISS, Universität Karlsruhe, Karlsruhe, Alemania, octubre-diciembre 2002 (10 semanas).

3. Estancia POSTDOCTORAL, Instituto IAKS – Universität Karlsruhe, Karlsruhe, Alemania, octubre 2004 (4 semanas).

4. Estancia POSTDOCTORAL, Instituto IAKS – Universität Karlsruhe, Karlsruhe, Alemania, mayo 2005 (2 semanas).

5. Estancia POSTDOCTORAL, Instituto IAKS – Universität Karlsruhe, Karlsruhe, Alemania, junio 2006 (2 semanas).

6. Estancia POSTDOCTORAL, CRM, Barcelona, España, noviembre 2007 (2 semanas).

7. Estancia POSTDOCTORAL, Florida Atlantic University, Boca Ratón, Florida, EE.UU., diciembre 2007 (4 semanas).

8. Estancia POSTDOCTORAL, tiempo parcial IMDEA SOFTWARE (Madrid), España. Del 19.02 al 31.12 de 2015 (10 meses y medio)

9. Estancia POSTDOCTORAL, tiempo parcial IMDEA SOFTWARE (Madrid), España. Del 23.02 al 31.12 de 2017 (10 meses y medio)

10. Estancia POSTDOCTORAL, tiempo parcial IMDEA SOFTWARE (Madrid), España. Del 28.04 al 31.12 de 2018 (8 meses y medio)

11. Estancia POSTDOCTORAL, tiempo parcial, IMDEA SOFTWARE (Madrid), España. Del 01.01 al 31.12 de 2019 (12 meses)

IV. CONTRIBUCIONES A CONGRESOS

A) CONFERENCIAS INVITADAS EN CONGRESOS INTERNACIONALES
1. AUTORES: M.I. González Vasco,
TÍTULO: Constructing group based provable secure encryption schemes: a methodology'
CONGRESO – Workshop on Provable Security
LUGAR DE CELEBRACIÓN: INRIA, Versalles, Francia, AÑO: 2004

2. AUTORES: Mª Isabel González Vasco
TITULO: Group action systems: a mathematical tool for developing provable secure cryptographic schemes
CONGRESO: Workshop of Algebraic Methods in Cryptography
PUBLICACIÓN: Post proceedings, VER PUBLICACIONES
LUGAR DE CELEBRACIÓN: Bochum, Alemania, AÑO: 2005

3. AUTORES: J.M. Bohli, M.I. González Vasco, R. Steinwandt.
TITULO: An application of verifiable randomness: subliminal free EC-DSA
CONGRESO: Workshop of Mathematical Cryptology
LUGAR DE CELEBRACIÓN: Santander, España, AÑO: 2006

4. AUTORES: M.I. González Vasco
TITULO: Secure Group Key Establishment: Group Theoretic Constructions
CONGRESO: Conference on Associative and Non-associative Algebraic Structures
LUGAR DE CELEBRACIÓN: Oviedo, España, AÑO: 2006

5. AUTORES: Jens M. Bohli, M. I. González Vasco, R. Steinwandt,
TITULO: Secure group key establishment: constructions in the standard model
CONGRESO: Geometric and Asymptotic Group Theory with Applications (GAGTA)
PUBLICACIÓN: abstract en libro de abstracts del congreso
LUGAR DE CELEBRACIÓN: Manresa, España, Año: 2006

6. AUTORES: M.I. González Vasco
TITULO: When group theory helps keeping secrets: cryptographic constructions based on groups
CONGRESO: Seminario internacional sobre matemática aplicada y su repercusión en la sociedad actual, INTERNACIONAL
LUGAR DE CELEBRACION: U. Rey Juan Carlos, Madrid, España, Año: 2008

7. AUTORES: M.I. González Vasco
TÍTULO: Group Key Establishment a la carte (a tool for every occasion)
CONGRESO: Central European Conference on Cryptology 2018
LUGAR DE CELEBRACIÓN: Smolenice, Eslovaquia, AÑO: 2018

8. AUTORES: M.I. González Vasco, Àngel L. Pérez del Pozo, Rainer Steinwandt
TITULO: Group Key Establishment in a Quantum-Future Scenario
CONGRESO: 2022 AWM Research Symposium
PUBLICACIÓN: No
LUGAR DE CELEBRACIÓN: Minneappolis, Minessota, EEUU, Año: 2022

9. AUTORES: M.I. González Vasco [Keynote speaker]
TITULO: Secure Key Exchange Withstanding Quantum Attacks
CONGRESO: ICR 23
PUBLICACIÓN: No
LUGAR DE CELEBRACIÓN: Madrid, España, Año: 2023.

10. AUTORES: M.I. González Vasco [Keynote speaker]
TITULO: Secure Key Exchange Withstanding Quantum Attacks
CONGRESO: 2024 International Conference on Advances in Computing Research (ACR'24)
PUBLICACIÓN: No
LUGAR DE CELEBRACIÓN: Madrid, España, Año: 2024.

B) CONFERENCIAS INVITADAS EN CONGRESOS NACIONALES

1. AUTORES: J.M. Bohli, M. I. González Vasco, R. Steinwandt
TITULO: The Enemy at home: Malicious insiders in Key Exchange protocols
CONGRESO: Workshop on Practical Aspects of Cryptography
LUGAR DE CELEBRACIÓN: Oviedo, España, Año: 2007

2. AUTORES: M.I. González Vasco
TITULO: Provable Security for Key Stablishment Protocols
CONGRESO: Workshop Interconsolider ARES-I-Math
LUGAR DE CELEBRACION: Castro Urdiales, España, Año: 2008

3. AUTORES: M.I. González Vasco
TITULO: Braid based cryptography; constructions, attacks and new research directions
TIPO DE PARTICIPACIÓN: Ponencia Invitada
CONGRESO: Jornada Temática Interdiscipinal de la Red Española de Topología:
LUGAR DE CELEBRACIÓN: Barcelona, Año: 2010.

4. AUTORES: M.I. González Vasco
TITULO: Provable security: why should mathematicians care
TIPO DE PARTICIPACIÓN: Ponencia (invitada)
CONGRESO: 4th Iberian Mathematical Meeting, session Computer Algebra and Applications
LUGAR DE CELEBRACIÓN: Valladolid, Año: 2012

5. AUTORES: M.I. González Vasco
TITULO: *Private Set Intersection: The Problem, Some Solutions and What to do if Size Matters*
TIPO DE PARTICIPACIÓN: Ponencia (invitada)
CONGRESO: XIII Encuentro de Álgebra Computacional y Aplicaciones (EACA),
LUGAR DE CELEBRACIÓN: Alcalá de Henares, Año: 2012

6. AUTORES: M.I. González Vasco
TITULO: *GAKE for a priori unknown partners*
TIPO DE PARTICIPACIÓN: Ponencia (invitada)
CONGRESO: BIENAL RSME, Sesión Matemáticas de la Teoría de Información
LUGAR DE CELEBRACIÓN: Ciudad Real,
Año: 2022.

7. AUTORES: M.I. González Vasco
TITULO: *Group Key Exchange in the Quantum Era*
TIPO DE PARTICIPACIÓN: Ponencia (invitada)
CONGRESO: 8th Iberian Mathematical Meeting, session Mathematics of Information
LUGAR DE CELEBRACIÓN: Sevilla,
Año: 2022.

8. AUTORES: M.I. González Vasco
TITULO: *Q-Alice and C-Bob tienen que hablar*
TIPO DE PARTICIPACIÓN: Ponencia (invitada)
CONGRESO: BIENAL RSME, Sesión Matemáticas de la Teoría de Información
LUGAR DE CELEBRACIÓN: Pamplona
Año: 2024.

C) PONENCIAS EN CONGRESOS INTERNACIONALES (NO POR INVITACIÓN)

1. AUTORES: M.I. González Vasco, R. Steinwandt
TÍTULO: Obstacles in Two Public Key Cryptosystems Based on Group Factorizations
CONGRESO: 1st Central European Conference on Cryptology - Tatracrypt.
PUBLICACIÓN: Artículo en actas, publicadas tras recensión por Tatra Mountain Math. Publications (ver apartado PUBLICACIONES).
LUGAR DE CELEBRACIÓN: Liptovský Ján, Eslovaquia AÑO: 2001

2. AUTORES: M.I. González Vasco, M. Näslund, I. E. Shparlinski
TÍTULO: Trace Interpolation Problems for Polynomials over Finite Fields (presentada por I.E. Shparlinski, coautor)
CONGRESO: Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC 14)
PUBLICACIÓN: Abstract en libro de abstracts del congreso
LUGAR DE CELEBRACIÓN: Melbourne, Australia
AÑO: 2001

3. AUTORES: M.I. González Vasco, M. Näslund, I. E. Shparlinski
TÍTULO: The Hidden Number Problem in Extension Fields and its Applications (presentada por I.E. Shparlinski, coautor)
CONGRESO: 3rd Latin American Theoretical Informatics Conference - LATIN 2002 -
PUBLICACIÓN: Artículo en actas, publicado tras recensión por Springer Verlag (ver publicaciones)
LUGAR DE CELEBRACIÓN: Cancún, México
AÑO: 2002

4. AUTORES: M.I. González Vasco, C. Martínez, R. Steinwandt.
TÍTULO: On Several Group based Cryptographic Primitives (presentada por R. Steinwandt, coautor)
CONGRESO: Third Pythagorean Conference
PUBLICACIÓN: Artículo aceptado en Special Issue (ver publicaciones)
LUGAR DE CELEBRACIÓN: Rhodas, Grecia
AÑO: 2003

5. AUTORES: M.I. González Vasco, R. Steinwandt
TÍTULO: On ideal and subalgebra coefficients in certain k-algebras (presentada por R.Steinwandt, coautor)
CONGRESO: First Joint Meeting RSME-AMS
PUBLICACIÓN: Abstract en libro de abstracts del congreso

LUGAR DE CELEBRACIÓN: Sevilla, España
AÑO: 2003

6. AUTORES: S. González, M.I. González, C. Martínez
TÍTULO: Group based Public Key Cryptography
CONGRESO: 12th International Conference on Logic, Methodology and Philosophy of Science
PUBLICACIÓN: Abstract en libro de abstracts del congreso
LUGAR DE CELEBRACIÓN: Oviedo, España
AÑO: 2003

7. AUTORES: M.I. González Vasco
TÍTULO: On Hard Bits of the Diffie-Hellman function
CONGRESO: Curso: Advanced Course on Contemporary Cryptology
LUGAR DE CELEBRACIÓN: Barcelona, España
AÑO: 2004
8. AUTORES: M.I. González Vasco, M. Näslund, I.E. Shparlinski
TÍTULO: New results on the Hardness of Diffie-Hellman Bits
CONGRESO – Public Key Cryptography, PKC 2004
PUBLICACIÓN: Artículo en actas, publicado tras recensión por Springer
LUGAR DE CELEBRACIÓN: Sentosa, Singapur
AÑO: 2004
9. AUTORES: M.I. González Vasco, C. Martínez, J. L. Villar, R. Steinwandt
TÍTULO: A new Cramer-Shoup like methodology for group based provably secure encryption schemes (presentada por coautor)
CONGRESO – 2nd Theory of Cryptography Conference TCC 2005
PUBLICACIÓN: Artículo en actas, publicado tras recensión por Springer Verlag (ver publicaciones)
LUGAR DE CELEBRACIÓN: MIT, Cambridge, EE.UU.
AÑO: 2005

10. AUTORES: M.I. González Vasco
TITULO: On the security of a group based public key cryptosystem
CONGRESO: Workshop on Mathematical Problems and Techniques in Cryptology
PUBLICACIÓN: Artículo en actas, Proceedings publicados por el CRM (ver publicaciones)
LUGAR DE CELEBRACIÓN: Centre de Recerca Matematica. Bellaterra, España
AÑO: 2005

11. AUTORES: R. Criado, J. Flores, M.I. González Vasco, J. Pello
TITULO: Locating a leader node on a complex network: a trade-off between robustness and efficiency (presentada por J. Pello, coautor)
CONGRESO: Internacional Conference on Computational and Mathematical Methods in Science and Engineering CMMSE-2005
PUBLICACIÓN: Artículo en actas locales, tras recensión
LUGAR DE CELEBRACIÓN: Alicante, España,
AÑO: 2005

12. AUTORES: J-M. Bohli, M.I. González Vasco, R. Steinwnadt
TITULO: A subliminal free variant of EC-DSA (impartida por coautor, J-M. Bohli)
CONGRESO: Information Hiding, INTERNACIONAL
PUBLICACIÓN: Si. VER PUBLICACIONES
LUGAR DE CELEBRACIÓN: Virginia, EE.UU.
AÑO: 2006

13. AUTORES: M. Abdalla, J. M. Bohli, M. I. González Vasco, R. Steinwandt
TITULO: (Password) Authenticated Key Establishment: From 2-Party to Group
(impartida por J. Bohli, coautor)
CONGRESO: Theory of Cryptology Conference
PUBLICACIÓN: si (ver publicaciones)
LUGAR DE CELEBRACIÓN: Ámsterdam, Holanda, Año: 2007

14. AUTORES: M.I. González Vasco, A.L. Perez del Pozo, P. Taborda
TITULO: A Note on the Security of MST3
TIPO DE PARTICIPACIÓN: Ponencia (impartida por coautor)
CONGRESO: Cryptology, Designs and Finite Groups 2009
PUBLICACIÓN: No
LUGAR DE CELEBRACIÓN: Deerfield Beach, Florida, EEUU.
Año: 2009.

15. AUTORES: P.D'Arco, M.I. González Vasco, A.L. Perez del Pozo, C. Soriente
TITULO: *Size Hiding in Private Set Intersection: Existential Results and Constructions*
TIPO DE PARTICIPACIÓN: Ponencia (impartida por coautor)
CONGRESO: 5th International Conference on Cryptology (Africacrypt 2012)
PUBLICACIÓN: Si (ver publicaciones)
LUGAR DE CELEBRACIÓN: Marruecos
Año: 2012

16. AUTORES: M.I. González Vasco, A.L. Pérez del Pozo, A. Suarez Corona
TITULO: Thwarting randomness reveals in group key agreement
TIPO DE PARTICIPACIÓN: Ponencia (impartida por coautor)
CONGRESO: CMMSE 2016
PUBLICACIÓN:Si (artículo en Actas, ISBN: 978-84-608-6082-2, pp. 606—614)
LUGAR DE CELEBRACIÓN: Cádiz
Año: 2016

17. AUTORES: Christian Colombo, María Isabel González Vasco, Mark Vella and Pavol Zajac
TITULO: Applying runtime verification to group key agreement
TIPO DE PARTICIPACIÓN: Ponencia (impartida por coautor)
CONGRESO: CSAW18
PUBLICACIÓN:No
LUGAR DE CELEBRACIÓN: Malta
Año: 2018

18. AUTORES: C. Colombo, M.I. González Vasco, R. Steinwandt, P. Zajac.
TITULO: Secure Communication in the Quantum Era: (Group) Key Establishment
TIPO DE PARTICIPACIÓN: Ponencia (impartida por coautor)
CONGRESO: Cluster Workshop on Advanced Technologies (NATO)
PUBLICACIÓN: Si (ver apartado PUBLICACIONES)
LUGAR DE CELEBRACIÓN: Lovaina, Bélgica
Año: 2019

D) PONENCIAS EN CONGRESOS NACIONALES (NO POR INVITACIÓN)

1. AUTORES: M.I. González Vasco, C. Martínez, R. Steinwandt
TÍTULO: Un Marco Común Para Varios Esquemas de Clave Pública Basados en Grupos
CONGRESO: VII Reunión Española de Criptología y Seguridad de la Información
PUBLICACIÓN: Artículo en actas, publicado tras recensión por el Servicio de Publicaciones de la Universidad de Oviedo (ver apartado PUBLICACIONES)
LUGAR DE CELEBRACIÓN: Oviedo, España
AÑO: 2002
2. AUTORES: M.I. González Vasco, D. Perez García, R. Steinwandt
TITULO: On the security of certain public key cryptosystems based on rewritting problems
TIPO DE PARTICIPACIÓN: Ponencia
CONGRESO: IX Reunión Española de Criptología y Seguridad de la Información
PUBLICACIÓN: Artículo en actas, (ver apartado publicaciones)
LUGAR DE CELEBRACIÓN: Leganés, España
AÑO: 2004

3. AUTORES: M.I. González Vasco, C. Martínez, R. Steinwand y J. Villar
TITULO: On provable secure encryption schemes based on non abelian groups
CONGRESO: IX Reunión Española de Criptología y Seguridad de la Información
PUBLICACIÓN: Sí, (ver apartado publicaciones)
LUGAR DE CELEBRACIÓN: Leganés, España
AÑO: 2004

4. AUTORES: M.I. González Vasco, Consuelo Martínez, S. González
TÍTULO: Esquemas de cifrado basados en grupos: pasado y futuro
CONGRESO – Mat.es
PUBLICACIÓN: Artículo CD de la sesión especial de Criptología
LUGAR DE CELEBRACIÓN: Valencia, España
AÑO: 2005

5. AUTORES: M. I. González Vasco, P. Grijó
TITULO: New steps towards secure word-problem based encryption schemes: analysis of a recent proposal (impartida P. Grijó, por coautor)
CONGRESO: IX Reunión Española de Criptología y Seguridad de la Información
PUBLICACIÓN: si (ver publicaciones)
LUGAR DE CELEBRACIÓN: Barcelona, España
Año: 2006

6. AUTORES: M.I. González Vasco, Angel L. Pérez del Pozo
TITULO: Related Mesage Attacks: A formal treatment
TIPO DE PARTICIPACIÓN: Ponencia (impartida por A. Pérez, coautor)
CONGRESO: X Reunión Española sobre Criptología y Seguridad de la Información
PUBLICACION: Artículo en libro de actas (ver publicaciones)
LUGAR DE CELEBRACION: Salamanca, España
Año: 2008

7. AUTORES: F. García, R. Criado, M.I. González Vasco, A.L. Perez del Pozo, M. Romance
TITULO: Tokenización: Una revisión al cifrado preservando el formato para el caso de datos bancarios
TIPO DE PARTICIPACIÓN: Ponencia
CONGRESO: RECSI 2012
PUBLICACIÓN: Si (ver publicaciones)
LUGAR DE CELEBRACIÓN: San Sebastián.
Año: 2012

8. AUTORES: M.I. González Vasco, A.L. Perez del Pozo, A. Suarez Corona
TITULO: Modelling ephemeral leakage in group key exchange protocols
TIPO DE PARTICIPACIÓN: Ponencia
CONGRESO: Jornadas Nacionales de Investigación en Ciberseguridad
PUBLICACIÓN: Si (Actas de las I Jornadas Nacioinales de Investigación en Ciberseguridad. ISBN: 978-84-9773-742-5. pp. 90-91)
LUGAR DE CELEBRACIÓN: León
Año: 2015

9. A.I. González-Tablas, M.I. González Vasco
TITULO: CryptoGo: criptografía simétrica en tapete verde
TIPO DE PARTICIPACIÓN: Ponencia
CONGRESO: Jornadas Nacionales de Investigación en Ciberseguridad
PUBLICACIÓN: Si (Actas de las IV Jornadas Nacionales de Investigación en Ciberseguridad
ISBN: 978-84-09-02697-5
LUGAR DE CELEBRACIÓN: San Sebastián
Año: 2018

E) POSTERS

1. AUTORES: M. I. González Vasco, R. Steinwandt, J.L. Villar
TITULO: Using non-abelian groups in cryptography: new approaches towards provable security

TIPO DE PARTICIPACIÓN: Poster
CONGRESO: International Congress of Mathematicians
PUBLICACIÓN: abstract en libro de abstracts del congreso
LUGAR DE CELEBRACIÓN: Madrid, España
Año: 2006

V. ORGANIZACIÓN DE ACTIVIDADES CIENTÍFICAS

1. **Miembro del comité organizador** de los congresos: ESTYLF99, RECSI 2002, CMMSE 06, JNIC 2017.

2. **Local Co-Chair del congreso**: International Conference on Information Theoretic Security ICITS 07, que tuvo lugar en la U. Carlos III de Madrid, julio de 2007.

3. **Organización de actividades en la línea de investigación** "Criptografía Matemática" del Instituto **IMDEA Matemáticas** (septiembre de 2007 a diciembre de 2008).

4. Miembro del Comité Coordinador de los **Itinerant Cryptography Seminars.** Organizadora local del Crypto Seminars day@URJC. 2015-2016.

5. Miembro del **Comité Coordinador (**de noviembre de 2006 hasta noviembre de 2010) de la **Red Española de Matemáticas para la Seguridad de la Información**. Como tal, miembro del comité organizador de las escuelas:

    - International School on Mathematical Cryptology 2008: Mathematical Foundations of Cryptology, Barcelona, del 22 al 26 de septiembre de 2008
    - (en colaboración con la Red Europea de Excelencia ECrypt II) International School on Mathematical Cryptology 2009. Provable Security. Barcelona, septiembre de 2009.

VI. OTROS MÉRITOS

A) INVITACIONES A SEMINARIOS DE PRESTIGIO

Asistencia por invitación al seminario Quantum Cryptanalysis en el **Schloss Dagstuhl**, **Leibniz-Zentrum für Informatik GmbH (LZI)**, 17401, del 1 al 6 de octubre de 2017.

Asistencia por invitación al seminario Quantum Cryptanalysis en el **Schloss Dagstuhl**, **Leibniz-Zentrum für Informatik GmbH (LZI)**, 19421, del 13 al 18 de octubre de 2019.

B) SEMINARIOS CIENTÍFICOS IMPARTIDOS POR INVITACIÓN

1. *Combinatorial Group Theory and Cryptography*, **Instituto IAKS/EISS, Universität Karlsruhe**, Alemania, noviembre 2000.

2. *Nociones de seguridad en Criptografía de Clave Pública*, **Universidad de Oviedo**, diciembre 2002.

3. *Aplicaciones de la Teoría de Grupos a la Criptografía*, **Universidad de Zaragoza**, enero 2003.

4. *Construcción de un esquema de Clave Pública IND-CCA2 a partir de grupos abelianos,* **Universidad de Oviedo**, enero 2003.

5. *Groups and Encryption* Schemes**, Universitá degli Studio de Firenze**, abril 2004.

6. *Constructing group based provably secure encryption schemes: a methodology*, Instituto **IAKS/EISS, Universität Karlsruhe**, Alemania, octubre 2004.

7. *Lattice reduction in cryptology: a survey*, Instituto **IAKS/EISS, Universität Karlsruhe**, Alemania, mayo 2005.

8. *Non Abelian Cryptographic Schemes: designs and attacks*, Seminario impartido en el **University College London**, Londres, Reino Unido, noviembre 2005.

9. *Constructing Group Based Provable Secure PKEs*, Charla invitada en el seminario de la **Universidad de Rennes 1**, abril 2006.

10. *Participación en mesa redonda 'Privacidad y Seguridad de la Información'*, VI Semana de la Ciencia y la Tecnología de la **Universidad de Oviedo**, noviembre 2006.

11. *Cryptographic constructions using non abelian groups: a survey of designs and attacks* Séminaire Cryptographie, Codes et Algorithmique, **ENSTA**, Paris, noviembre 2006. U

12. *Criptografía de clave pública basada en grupos: diseños, ataques y nuevas direcciones* Dept. de Matemáticas, **U. Autónoma de Madrid**, marzo 2007.

13. *Group based cryptography: constructions, attacks and new research directions,* **CRM**, Barcelona, noviembre 2007.

14. *Password Authenticated Group Key Establishment: Recent proposals without random oracles*, MAC Seminar, **Universitat Politècnica de Catalunya**, noviembre 2007.

15. *Group Key establishment using password authentication*, Mathematical Sciences Colloquium, **Florida Atlantic University**, diciembre 2007.

16. *Public Key Cryptography: Mathematical Models for Provable Security*, Colloquium del Dpto. de Matemáticas de la **U. Carlos III de Madrid**, 17 octubre 2008.

17. *Tokenización vs cifrado clásico.* Seminario de la cátedra URJC-I4S. **Centro de Innovación BBVA**, 19 Enero de 2015.

18. *Criptografía Matemática* (qué es, qué no es y por qué debería importarte**), Inf-Tech URJC,** Febrero de 2015.

19. *Size-Hiding Private Set Intersection*, Seminario de Geometría Algebraica, **U. Complutense de Madrid**, 4 de mayo, 2015.

20. *Multi-Party Computation: Cryptography for the not so good, the not so bad, and the not so ugly*, Colloquium del Dept. de Matemáticas, **U. Carlos III de Madrid**, 12 de marzo 2015.

21. *Mejor en privado: operaciones conjuntistas con garantías de privacidad y aplicaciones.* Seminario de Matemática Aplicada, **URJC**, Mayo 2018.

22. Anonymity in Authenticated Key Exchange. NTNU, Trondheim, Noruega, junio 2023.

C) **TRIBUNALES DE TESIS**

1. *Criptoanálisis de generadores no lineales de números pseudoaleatorios.*
   D. Domingo Gómez Pérez, U. de Cantabria, 2006.

2. *Lightweight Cryptography in RFID Systems*.
   D. Pedro Peris López, U. Carlos III, 2008.

3. *Privacy Providing Signatures and their applications*.
Dña. Somayeh Heidervand, UPC, 2010.

4. *Compilers and Protocols for Key Establishment*.
Dña. Adriana Suarez Corona, U. de Oviedo, 2012.

5. *New security definitions, constructions and applications of proxy re-encryption.*
D. David A. Nuñez Montañez, UMA, 2017.

6. *Automation and Modularity of Cryptographic Proofs*
D. Juan Manuel Crespo, UPM, 2017.

7. *Métodos algebraicos en criptografía multivariable*
D. Jorge Linde Díaz, UCM, 2018.

8. *Cryptographic Techniques for the Security of Cloud and Blockchain Systems*
D. Luca Nizzardo, UPM, 2018.

9. *Quantum-Resistant Key Agreement and Key Encapsulation*
Angela Robinson, Florida Atlantic University, 2018.

10. *Automated Analysis of Cryptographic Constructions,*
D. Miguel Ambrona, UPM, 2018.

11. *On the security of Cache algorithms,*
D. Pablo Cañones, UPM, 2019.

12. *Análisis y Mejora de la Seguridad y Privacidad de Esquemas Federados para la Gestión de Identidades y Accesos*,
D. Jorge Navas, URJC, 2020.

13. *Identificación de la Fuente de Adquisición en Vídeos Digitales de Dispositivos Móviles,*
D. Raquel Ramos López, UCM, 2021.

14. *Ad-nilpotent elements in algebras and superalgebras*
D. Guillermo Vera de Salas, URJC, 2022.

15. *Ontology for Cross-Site-Scripting (XSS) attack in Cybersecurity*
MSc. Ing. Jean Rosemond Dora, Slovak Academy of Sciences, 2022.

16. *Post-Quantum Key Establishment*
Ing. Peter Spacek, Slovak University of Technology, 2022

17. *ARCHITECH: Advanced Research of Cryptographic Techniques to build efficient blockchains with privacy and security*

Dña. Anaïs Querol Cruz, Imdea Software, 2022.

18. *From lattice crypto to Laettis Crypto*
Bor de Kock, NTNU, Noruega, Junio 2023

19. *Seguridad Adaptativa: mecanismos y dominios de aplicación*
Miguel Calvo, Junio 2023

20. *Towards Improved Homomorphic Encryption for Privacy-Preserving Deep Learning*
José Cabrero, UC3M, Junio 2023

D) PERTENENCIA A SOCIEDADES CIENTÍFICO-PROFESIONALES

- Miembro de la International Association for Cryptologic Research (IACR)
- Miembro de la Real Sociedad Matemática Española (RSME)-- desde diciembre de 2017, vocal de la Junta de Gobierno de la misma. Miembro además de la Comisión de Publicaciones desde 2019 y de la Comisión de Transferencia desde 2021.

TRANSFERENCIA

I. PROYECTOS Y CONTRATOS DE I+D CON EMPRESAS

A) PROYECTOS EN LOS QUE LA CANDIDATA FUE IP Ó CO-IP

1. Título del proyecto: Estudio de algoritmos para la creación de una aduana de datos
Entidad financiadora: I4S (Art. 83) - Catedra URJC-I4S
Fecha de ejecución 1.10.2014 – 13/03/2017
Cuantía de la subvención: 45.000€
Investigador principal: Regino Criado Herrero, María Isabel González Vasco
Número de investigadores participantes: 4

2. Título del proyecto: Algoritmo de Tokenización
Entidad financiadora: I4S (Art. 83) - Catedra URJC-I4S
Fecha de ejecución1 de marzo – 30 de junio de 2014
Cuantía de la subvención: 45.000€
Investigador principal: Regino Criado, María Isabel González Vasco
Número de investigadores participantes: 4

3. Título del proyecto:CRIPTOGRAFÍA POST-CUÁNTICA Y CIFRADO BASADO EN ATRIBUTOS
Entidad financiadora: Blue Indico Investments SL

Duración: 13.07.2018- 15.10.2018
Cuantía de la subvención: 18750€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo.

4. Título del proyecto:CRIPTOGRAFÍA POST-CUÁNTICA Y CIFRADO BASADO EN ATRIBUTOS
Entidad financiadora: BBVA Next Technologies
Duración: 16.06.2019- 01.11.2019
Cuantía de la subvención: 15.000€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo.

5. Título del proyecto: Criptografía Post-Cuántica en Sistemas Embebidos (SeQure2021)
Entidad financiadora: ARQUIMEA CENTRO DE INVESTIGACIONES AVANZADAS SLU
Duración: del 14 de mayo al 31 de diciembre de 2021.
Cuantía de la subvención: 25.000€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo, Misael E. Marriaga

6. Título del proyecto: Criptografía segura frente a adversarios cuánticos (Formación)
Entidad financiadora: CNI – Ministerio de Defensa
Duración: Curso de 16 horas, octubre 2021.
Cuantía de la subvención: 40.300€
Investigador principal: María Isabel González Vasco

7. Título del proyecto: Criptografía Post-Cuántica en Sistemas Embebidos (SeQure2022)
Entidad financiadora: ARQUIMEA CENTRO DE INVESTIGACIONES AVANZADAS SLU
Duración: del 15 de marzo al 23 de diciembre de 2022.
Cuantía de la subvención: 36.300€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo, Misael E. Marriaga

8. Título del proyecto: Criptografía Post-Cuántica en Sistemas Embebidos (SeQure2023)
Entidad financiadora: ARQUIMEA CENTRO DE INVESTIGACIONES AVANZADAS SLU
Duración: del 1 de marzo al 15 de diciembre de 2023.
Cuantía de la subvención: 30.000€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo, Misael E. Marriaga

9. Título del proyecto: Solución de identidad Autosoberana
Entidad financiadora: GMV
Duración: del 20 de julio de 2023 al 19 de julio de 2026.
Cuantía de la subvención: 105.000€
Investigador principal: María Isabel González Vasco
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo, Vicente Muñoz

B) PROYECTOS EN LOS QUE LA CANDIDATA FORMÓ PARTE DEL EQUIPO DE INVESTIGACIÓN

1.Título del proyecto: Modelos cuantitativos para la predicción y el análisis de la disponibilidad de parques de ATMs
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: septiembre 2011-junio 2012
Cuantía de la subvención: 42.327€ (+ IVA)
Investigador responsable: Miguel Romance del Rio
Número de investigadores participantes: 4

2. Título del proyecto: Análisis de algoritmos de tokenización y asesoramiento teórico para su implementación.
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: diciembre 2010- septiembre 2011
Cuantía de la subvención: 34.317€ (+ IVA)
Investigador responsable: Regino Criado Herrero
Número de investigadores participantes: 4

3. Título del proyecto: Análisis de algoritmos de tokenización: estado del arte
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: septiembre 2010-junio 2011
Cuantía de la subvención:17.601€ (+ IVA)
Investigador responsable: Regino Criado Herrero
Número de investigadores participantes: 4

4. Título del proyecto: Análisis de Riesgos Tecnológicos, inversión vs nivel de servicio
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: septiembre 2010-junio 2011
Cuantía de la subvención: 39.597€ (+ IVA)
Investigador responsable: Regino Criado Herrero
Número de investigadores participantes: 4

5.Título del proyecto: Obsolescencia de ATMs. Fase II.
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: septiembre 2012-junio 2013
Cuantía de la subvención: 46.566,22€ (+ IVA)
Investigador responsable: Regino Criado Herrero, Miguel Romance del Rio.
Número de investigadores participantes: 4

6. Título del proyecto: Modelo para la gestión del riesgo digital: riesgo dinámico
Entidad financiadora: BBVA (Art. 83)
Fecha de ejecución: septiembre 2012-junio 2013
Cuantía de la subvención: 137.236,97€ (+ IVA)
Investigador responsable: Regino Criado Herrero N
Número de investigadores participantes: 5

7. Título del proyecto: Base de datos (Dataset)
Entidad financiadora: I4S (Art. 83) - Catedra URJC-I4S
Fecha de ejecución 1.10.2014 – 30 .06. 2015
Cuantía de la subvención: 65.000€
Investigador responsable: Regino Criado, Miguel Romance
Número de investigadores participantes: 4

8. Título del proyecto:Whitebox cryptography y searchable encryption
Entidad financiadora: I4S (Grupo BBVA)
Entidades participantes: I4S (Grupo BBVA), URJC
Duración: marzo-julio 2017
Cuantía de la subvención: 30.500€
Director: Regino Criado
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo.

9. Título del proyecto:Criptografía y algoritmos post-cuánticos
Entidad financiadora: I4S (Grupo BBVA)
Entidades participantes: I4S (Grupo BBVA), URJC
Duración: marzo-julio 2017
Cuantía de la subvención: 30.500€
Director: Regino Criado
Equipo: Maria Isabel González Vasco, Ángel L. Pérez del Pozo.

10. Título del proyecto: ASESORAMIENTO Y DEMOSTRACIÓN DE ACTIVIDADES FORMATIVAS INNOVADORAS EN CIBERSEGURIDAD PARA CYBERCAMP18
Entidad financiadora: INCIBE
Duración: Noviembre 2018
Cuantía de la subvención: 3000E
Director: Ana Isabel González-Tablas Ferreres
Equipo: Ana Isabel González-Tablas Ferreres, Maria Isabel González Vasco, Álvaro Palomino.

II. DIVULGACIÓN CIENTÍFICA

A) PUBLICACIONES

1. [LIBRO]*Las matemáticas de la criptología.* Colección Miradas Matemáticas, Ed. Catarata, ISBN: 987-84-9097-505-3, pp. 1-104. 2018.
2. [ARTÍCULO EN PRENSA] La indomable imaginación de la primera programadora de la historia. Café y Teoremas, El Pais, 27 de noviembre de 2018.
3. [ARTÍCULO EN PRENSA] (con A. Timón) Muere Ann Mitchell: cazadora de patrones criptográficos en la lucha contra los nazis. Café y Teoremas, El Pais, 3 de junio, 2020.
4. [ARTÍCULO EN PRENSA] Ida Rhodes: el poder de la mujer máquina. Café y Teoremas, El Pais, 19 de mayo, 2020.

5. [COLABORACIÓN] Nueva pista para solucionar Kryptos, el gran enigma cifrado de la CIA. El Pais Retina, 2 de febrero de 2020.
6. [COLABORACIÓN] Criptografía, qué es y por qué deberías usarla en tu teléfono para que no te espíen. BBC World, 26 de diciembre de 2019. L
7. [ENTRADA EN BLOG] Matemáticas y Secretos: Fundamentos Matemáticos de la Nueva Criptología. Weblog Madrid I+D, Febrero 2007.
8. [CONTRIBUCIÓN A REVISTA NO CIENTÍFICA]. Colaboradora habitual de la sección de ciencia de la revista "Azul Eléctrico", artículos publicados:
    a. *Tras la huella de Pi; círculos, trascendencia y elefantes, num 4, 2006.*
    b. *Resolviendo Problemas en los 90: el último Teorema de Fermat, num 6, 2007.*
    c. *Gregory Perelman y la ética científica, num 7, 2008.*
    d. *El diablo en el espejo, num 8, 2008.*
    e. *La olvidada ciencia del glamour, num 9, 2009.*
    f. *Emoción fractal, num 10, 2009.*
    g. *No disparen al matemático, num 11, 2010.*
    h. *Sangre y números, num 12, 2010.*
9. [contribución a revista de Colegio Oficial de Doctores y Licenciados en Filosofía en Letras y en Ciencias] Matemáticas que custodian secretos, Abril-Mayo 2019.
10. El enemigo a las puertas: avances en criptografía clásica para un mundo cuántico. Gaceta de la RSME, Vol 23 (1), pp. 187—204, 2020.
11. (con L. J. Rodríguez-Muñiz, R. Crespo, I. Díaz, M. Fioravanti, L. Miguel García-Raffi, L. González-Vega, M. Lafuente, J. Montejo-Gámez, F.A. Ortega y R. Mallavibarrena) Los estudios de matemáticas en el ámbito universitario. Capítulo del Libro Blanco de las Matemáticas. D. Martín de Diego (Coord). RSME – Fund. Ramón Areces, 2020.
12. Coordinación con Bernardo Marín de la sección Desafíos Criptográficos del periódico El País; búsqueda, selección y edición de propuestas (2 propuestas propias, 8 de otros investigadores). Propuestas propias:
    1. *El misterio de la carta del soldado alemán* (julio 2022)
    2. *El acertijo de la cámara secreta* (agosto 2022)

B) IMPARTICIÓN DE CHARLAS/SEMINARIOS PARA PÚBLICO NO ESPECIALIZADO

1. *Matemática como lenguaje formal para la Criptología*, charla invitada en el curso "Tendencias actuales de la Matemática Interdisciplinar" del IMI, 2 horas, Cursos de Verano UCM en El Escorial, 24 de julio de 2008.

2. *Matemáticas y Secretos: una introducción a la criptografía*, charla invitada en el curso "Las Matemáticas en el aula y en el mundo real", 2 horas, XXVIII Universidad

de Otoño, Ilustre Colegio Oficial de Doctores y Licenciados en Filosofía y Letras y en Ciencias de Madrid, 23 de septiembre de 2008.

3. *Criptología: secretos, mentiras y matemáticas*. charla invitada en el curso "Matemáticas: un camino hacia el futuro" 2 horas, Cursos de Verano UCM en El Escorial, julio de 2010.

4. *Bombas, enigmas y crucigramas: Alan Turing y la criptología.* charla invitada en el curso "En memoria de Alan Turing (1912-1954): el fundador de la informática, cien años después" 2 horas, Cursos de Verano UCM en El Escorial, julio de 2012.

5. *Protocolos Criptográficos Eficaces.* Curso de Verano "Matemáticas para todo y para todos", U. Menendez Pelayo, 9 de julio, 2015.

6. Participación en la *mesa redonda "Criptografía Práctica"* dentro del curso de Verano UCM organizado por el IMI titulado, "Matemáticas, ¿para qué?" 5 de julio 2017.

7. Participación en la mesa redonda de Matemáticas, II Semana de Formación del Colegio San Agustín, Salamanca, enero 2018.

8. *Computando con tu enemigo, una introducción al as técnicas criptográficas para la privacidad.* URJC Tech-Fest, 20 de abril, 2018.

9. *Alicia contra Eva: una breve historia de criptografía y matemáticas.* IV Jornadas de Mujeres en Ciencia e Ingeniería, mayo 2018.

10. *Aprendiendo matemáticas a través de la criptografía*, 2 horas, XXVIII Universidad de Otoño, Ilustre Colegio Oficial de Doctores y Licenciados en Filosofía y Letras y en Ciencias de Madrid, septiembre 2018.

11. Grandes Retos de la Ciberseguridad. Presentación como ponente en el comité Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en el evento URJCmun 2019, 5 de febrero de 2019.

12. *Criptografía Matemática, qué es, qué no es, y por qué debería importarte.* Seminario de Matemáticas, U. de Málaga, 15 marzo 2019.

13. *Criptografía: una historia divertida de secretos y matemáticas*. Celebración del día de la mujer y la niña en la ciencia. Colegio Federico García Lorca, Leganés, Madrid, febrero 2020.

14. *De Espías y Matemáticas, breve historia de la criptografía*. Celebración del día de la mujer y la niña en la ciencia. Colegio Amanecer, Alcorcón, Madrid, febrero 2021.

15. *Criptografía y matemáticas: una breve historia de victorias y derrotas,* Bidebarrieta Kultugunea, IV Edición del Ciclo "Las matemáticas en la vida cotidiana" Bilbao, abril 2022.bao

16. *Intercambio de clave en grupo en la era cuántica.* I Encuentro QTEC (Tecnologías Cuánticas), Centro Criptológico Nacional, Madrid, 2022.

17. *Criptografía Post-Cuántica para Muggles*. RootedCon, Madrid, 2023.

18. *El futuro de la Criptografía*. Webinario, Agencia Española de Protección de Datos, Junio 2023.

19. *Integración de tecnologías clásicas y cuánticas para la seguridad,* Curso de Verano "Computación cuántica y ciberseguridad: certezas, riesgos e incertidumbres", Universidad de Málaga, julio de 2024

C) OTROS

1. Autora (con A.I. González Tablas Ferreres) del juego de cartas Crypto Go. (solicitado Registro de la Propiedad Intelectual, expediente 09-RTPI-8240.2/2018).

Impartición de diversos talleres asociados (Semana de la Ciencia 2018, HoneCon2018, Cybercamp 2018), con la colaboración de Alvaro Planet. La impartición de talleres en Cybercamp fue financiada con el Proyecto- Artículo 83 ASESORAMIENTO Y DEMOSTRACIÓN DE ACTIVIDADES FORMATIVAS INNOVADORAS EN CIBERSEGURIDAD PARA CYBERCAMP18 con el Instituto Nacional de Ciberseguridad (INCIBE).
Cuatro participaciones en jornadas (Jornadas Nacionales de Investigación en Ciberseguridad, - 7.D.9), Jornadas de Innovación Docente en grados y posgrados en Ciencias Experimentales e Ingenierías), HackOn, T3chfest.

III. PATENTES Y MODELOS DE UTILIDAD

INVENTORES (p.o. de firma): María Isabel González Vasco, Angel L. Pérez del Pozo, Claudio Soriente
TITULO: DAPAKE: Dynamic Anonymous Password-Based Key Exchange Nº DE SOLICITUD: 62/688,342, US publication No. 2019/0349191A1
PAÍS DE PRIORIDAD: E.E.U.U.
FECHA: Junio 2018 (contrato de cesión) , noviembre 2019 (publicación)
ENTIDAD TITULAR: NEC Laboratories Europe
RENDIMIENTO INICIAL: **URJC vende su participación a NEC Laboratories por 2750€.**

INVENTORES (p.o. de firma): A. Faonio, María Isabel González Vasco, Angel L. Pérez del Pozo, Claudio Soriente
TITULO: Password Authenticated Public Key Establishment.
Nº DE SOLICITUD: 62/941,908

PAÍS DE PRIORIDAD: E.E.U.U.
FECHA: 2020 (contrato de cesión), ENTIDAD TITULAR: NEC Laboratories Europe
RENDIMIENTO INICIAL: **URJC vende su participación a NEC Laboratories por 1700€.**

IV. OTROS MÉRITOS

- Miembro del **Comité de Normalización CTN 320**, "Ciberseguridad y protección de datos personales" dependiente de la Asociación Española de Normalización (UNE) , desde el 13 de diciembre de 2018.

- Promotora de una **nominación exitosa a los premios FRONTERAS DEL CONOCIMIENTO DE LA FUNDACIÓN BBVA**, en su décima edición (2018). Los nominados por la solicitante (Prof. Shafi Goldwasser y Prof. Adi Shamir) obtuvieron el premio en la categoría de *Teoría de la Información y las Comunicaciones.*

DOCENCIA

I. DOCENCIA IMPARTIDA

Docencia impartida en 1 curso académico (durante 3 meses) como no doctora (2003-2004) y **17 cursos académicos como doctor** (2004-05 a 2021-22). La solicitante cuenta con **2852** horas de clase impartidas, siendo en la gran mayoría de las asignaturas que ha impartido la profesora encargada de las mismas, habiendo impartido por tanto las clases de teoría y práctica y organizando la planificación y gestión del material.

Docencia de Grado/Ingenierías: 2523 horas (255 en inglés y 40 en un grado on-line). Docencia de Postgrado: 215 horas en máster oficial y 40 horas en doctorado. En los últimos diez cursos académicos he impartido 150 horas en asignaturas de máster oficial.

Resumen de asignaturas impartidas:

1. **Grado en Matemáticas**
1.1. Matemática discreta y Álgebra (6 cursos, 312 horas)
1.2. Estructuras algebraicas avanzadas (5 cursos, 140 horas)

2. Titulaciones relacionadas con **Ingeniería Informática** (Informática Técnica, Grado en Ing. Informática, Grado en Ing. del Software, Grado en Ing. de la Ciberseguridad)
2.1. Matemática discreta (3 cursos, 225 horas)
2.2. Seguridad Informática (1 curso, 20 horas)
2.3. Lógica (3 cursos, 108 horas)
2.4. Matemática discreta y Álgebra (1 curso, 40 horas en la titulación on-line, resto solapa con 1.1.)
2.5. Metodología de la programación (1 curso, 30 horas)
2.6. Criptografía (4 cursos, 240 horas)

3. Titulaciones de la **Escuela de Ciencias Experimentales y Tecnología** (Ing. en Organización Industrial, Ing. de Materiales, Ing. Ambiental, Grado en Ciencia y Tecnología de los Alimentos).
3.1. Matemáticas I (Álgebra lineal y Cálculo) (7 cursos, 504 horas)
3.2. Matemáticas II (Cálculo vectorial y Ecuaciones diferenciales) (8 cursos, 480 horas)
3.3. Matemáticas (1 curso, 20 horas)

5. **Ingeniería en Telecomunicación**
5.1. Algebra lineal - en inglés (3 cursos, 180 horas)
5.2. Criptografía y seguridad (6 cursos 270 horas)

6. **Ingeniería Biomédica**
6.1. Algebra- en inglés (1 curso, 75 horas)

7. **Doctorado** (Programa en Informática y modelización matemática y programa en Ingeniería Informática y Nuevas Tecnologías de la Información)
7.1. Criptografía (2 cursos, 40 horas)

8. **Máster Oficial** (215 horas en total)
8.1. Máster oficial en Redes y Servicios de Comunicación Móviles; "Criptografía y Seguridad en Redes Inalámbricas (1 curso, 15 horas)
8.2. Máster oficial en Tecnologías y Sistemas Informáticos; "Criptografía: métodos clásicos y modernos para la seguridad de la información" (4 cursos, 200 horas)

9. **Docencia singular**
9.1. Docencia impartida en el programa "Universidad de Mayores" (24 horas), dentro de la asignatura "Cuentos con Cuentas" centrada en la matemática recreativa.
9.2. Docencia impartida en los cursos cero de matemáticas para la preparación de alumnos de nuevo ingreso (50 horas)

9.3. Docencia en Títulos propios
9.3.1. Máster no-oficial (título propio On-line): Criptografía y Criptanálisis en el Máster en Ciberseguridad y Privacidad, (5 cursos, 150 horas)
9.3.2. Curso Experto (título propio On-line): Cifrado de Datos y Comunicaciones Seguras, en el Curso Experto en Privacidad y Protección de Datos (1 curso, 10 horas)

II. TRABAJOS DIRIGIDOS

1. Trabajos fin de grado

1.1. Alumno: Juan Rodríguez Sabín. Una herramienta para el cifrado de bases de datos para identificacions Biométricas. Doble grado en Ingeniería del Software y Matemáticas. Curso 2015-16. Sobresaliente (10)

1.2. Alumno: Daniel de las Heras Montero. Implementación del esquema McEliece para la nube sin delegación de claves. Grado en Ing. Del Software. Curso 2016-2017. Notable (8,5)

1.3. Alumno: Daniel de las Heras Montero. Cifrado McEliece de datos en la nube sin delegación de claves. Grado en Ing. Del Software. Curso 2016-2017. Matrícula de Honor (10)

1.4. Alumno: Dimas Muñoz Montesinos. Intercambio de clave: esquemas cuánticos y postcuánticos. Doble grado en Ing. del Software y Matemáticas. Curso 2017-2018. Matrícula de Honor, (9,5)

1.5. Alumno: Carlota Martínez-Aedo Sanchez. Protección de infraestructuras críticas en el sector del agua. Doble Grado en Ing. Ambiental e Ing. De Organización Industrial. Curso 2017-2018. Aprobado (5)

1.6. Alumno: JAVIER REDONDO ANTON. Doble grado en Ing. Informática y Matemáticas. Esquemas de Intercambio de Clave Anónimos con Autenticación por Contraseñas. Curso 2019-2020. 10 Propuesto para MH

1.7. Alumno: ANA GONZÁLEZ SANTAMARÍA. Doble grado en Ing. Informática y Matemáticas. Esquemas de Compartición de Secretos con Detección de Usuarios Maliciosos. Curso 2019-2020. 10 Propuesto para MH

1.8. Alumno: Alejandro Garcia Carretero. Doble grado en Ing. Informática y Matemáticas. Análisis de un esquema de cifrado basado en cuasigrupos. Curso 2019-2020. 10 Propuesto para MH

1.9. Alumno: Iván Martín Sanz. Doble grado en Ing. Softwared y Matemáticas. Cifrado Buscable y su aplicación al PNR (Passenger Name Record). Curso 2020-2021. 10 Propuesto para MH

1.10. Alumno: Christian Alcaide Moreno. Análisis de variantes de esquemas de cifrado de clave pública. Curso 2021-2022. Sobresaliente (9)

2. Proyectos fin de carrera

2.1. Alumno: Ouafae Debdi. Una implementación del criptosistema RSA. Ing. Técnico en Informática de Gestión. Curso 2006-2007. Sobresaliente. (9)

2.2. Alumno: Gema Martínez Fernández. Diseño de aplicaciones Web para generar exámentes de test utilizando el criptosistema Knapsack. Ingeniero Técnico en Informática de Gestión Móstoles. Curso 2008-2009.

3. Trabajos fin de master

3.1. Alumno: Franco Foresti. NAXOS authenticated key Exchange. Máster en Ciberseguridad y Privacidad. Curso 2017-2018. Sobresaliente. (10)

3.2. Daniel de las Heras Montero. Máster en Ciberseguridad y Privacidad. Diseño e implementación de un esquema de intercambio de clave para n-usuarios. Curso 2019-2020. Matrícula de Honor (10)

2.3. Sara Lucas Hernández. Curso 2021-2022. Generación Verificable de Claves Criptográficas. Sobresaliente. (10).

4. DEA (Diploma estudios avanzados)

4.1. Alumno: Pedro Taborda Duarte. Commitment Schemes and Logarithmic Signatures. APTO. Curso 2009.

5. Organización de escuelas de investigación o reuniones científicas similares internacionalmente reconocidas

2.1. International School on Mathematical Cryptology 2008: Mathematical Foundations of Cryptology, Barcelona, del 22 al 26 de septiembre de 2008 - Miembro del comité organizador

2.2. (en colaboración con la Red Europea de Excelencia ECrypt II) International School on Mathematical Cryptology 2009. Provable Security. Barcelona, del 7 al 9 de septiembre de 2009. – Miembro del comité organizador

6. **Tesis doctorales dirigidas**

3.1. (Co-dirección, con otros 2 profesores) *Estudio de los criterios de localización de emplazamientos para almacenamiento geológico de CO2*. Jose Francisco Fdez. Ordás, defendida en León, 28 de septiembre de 2017, Calificación: Sobresaliente.

3.2. *Criptografía segura frente a adversarios cuánticos. Análisis y variantes de propuestas para estandarización,* Jose I. Escribano Pablos, Programa de doctorado en Ciencias, URJC, defendida en julio de 2022. Calificación de Sobresaliente Cum Laude.

3.3 La solicitante dirige en la actualidad a :
- Victoria Aguilar, en su tercer año, dentro del Programa de doctorado en Ciencias de la URJC.
- David Balbás (en co-dirección con Dario Fiore), en su segundo año, en el instituto Imdea Software de Madrid.

3.4. En el pasado, la solicitante dirigió a Pedro Taborda Duarte, que no llegó a defender la tesis por motivos personales. Sus resultados conjuntos quedan constatadas en las dos publicaciones en JCR:

> M.I. González Vasco, A.L. Pérez del Pozo y P. Taborda Duarte. A note on the security of MST3. Designs Codes and Cryptography, Vol. 55, p.189--200, 2010.
> Doi: 10.1007/s10623-010-9373-0
> JCR 2010: 0.771, Matemática Aplicada, 121/236. Q3, T2
> Citas:18, Fuente: Google Scholar

> M.I. González Vasco, A.L. Pérez del Pozo, P. Taborda Duarte y J.L. Villar. Cryptanalysis of a key exchange scheme based on block matrices. Information Sciences, Vol. 276, pp. 319-331, 2014. Doi: 10.1016/j.ins.2013.11.009
> JCR 2014: 4.038 Computer science, information systems. 6/139 Q1 – T1
> Citas:11, Fuente: Google Scholar

III. PUBLICACIONES DOCENTES

A) LIBROS/CAPÍTULOS DE LIBROS

1. (con A.L. Pérez del Pozo) *Criptografía Esencial. Principios básicos para el diseño de esquemas y protocolos seguros.* Ra-Ma. 2021.

2. Privacidad en redes sociales: amenazas y soluciones. Capítulo del libro BIG DATA. Eje estratégico en la industria audiovisual. Eva P. Fernandez (Coord). Manual, Ed. UOC, pp. 141- 159, 2016.

B) ARTÍCULOS LISTADOS EN JCR

Nota: a continuación de cada artículo se incluye el índice de impacto, que, salvo reseña explícita, es del año de publicación. Además, se incluye el área JCR en la que aparece, y su lugar relativo/número total de revistas.

1. (con A.I. González Tablas, I. Cascos y A. Planet Palomino) *Shuffle, Cut and Learn: Crypto Go, a Card Game for Teaching Cryptography.* Special Issue Mathematical Modeling and Simulation in Science and Engineering Education II. Mathematics, 8 (11), 1993, 2020.

https://Doi.org/10.3390/math8111993
JCR 2019: 1.471. Mathematics, 28/325, Q1.

IV. CONGRESOS Y SEMINARIOS DOCENTES

1. Ponencias impartidas

1.1. *Aprendiendo en la sobremesa: CryptoGo, un juego de cartas para dominar la criptografía simétrica*. (con A.I. González-Tablas) I Jornadas de Innovación Docente en Grados y Posgrados en Ciencias Experimentales e Ingenierías, URJC, septiembre 2018.

1.2. *Ejemplos de aplicación para asignaturas de Álgebra y Matemática Discreta en titulaciones de Informática*, Seminario de reflexión crítica sobre la enseñanza de las Ciencias en la URJC, junio de 2017.

2. Asistencia a eventos

2.1. *VI Jornada sobre evaluación de competencias en el marco del espacio europeo de educación superior*. Julio de 2014.

3. **Organización de eventos**

3.1. Miembro del Comité Organizador de la l Jornada *Usos y Avances en la Docencia de las Matemáticas en las Enseñanzas Universitarias,* Universidad Rey Juan Carlos, septiembre de 2019

3.2. Co-organizadora con Javier López, UMA, del Curso de Verano "Computación cuántica y ciberseguridad: certezas, riesgos e incertidumbres", Universidad de Málaga, julio de 2024.

V. CURSOS DE FORMACIÓN DOCENTE RECIBIDOS

1. Taller de gestión de calificaciones en Aula Virtual, 4 horas, febrero de 2018.
2. Curso Básico de Introducción a Moodle, 5 horas, enero de 2015.
3. Elaboración de guías docentes, 5 horas, junio de 2011.

VI. OTROS MÉRITOS

1. **4 Tramos reconocidos en el programa DOCENTIA** de la URJC. (Cursos 2005-06, 06-07 y 07-08, Cursos 2011-12,12-13 y 13-14, Cursos 2014-15,15-16 y 16-17, cursos 2017-18, 2018-19, 2019-20)

2. Diseño, dirección e impartición de **cursos fuera de la institución** a la que pertenece.

2.1. Mathematical Cryptology: An Introduction, curso de 5 horas impartido dentro del Encuentro Matemático Hispano Marroquí, organizado por el CEMAT en Casablanca, Marruecos, del 12 al 15 de noviembre de 2008.

2.2. Public Key Cryptography: An introduction, curso de 10 horas impartido dentro de la Escuela JAE de Matemáticas, ICMAT, junio 2018.

3. Impartición de **docencia on-line**

3.1. Impartición de 40 horas de docencia en grado oficial (Algebra lineal y Matemática Discreta en el grado de Ing. Informática on-line de la URJC)

3.2. Docencia y gestión de dos títulos propios on-line en la URJC

4. **Otros méritos**

4.1. Participación en la asignatura "Redes e Información: Las matemáticas de Internet", dentro del proyecto **ADA-Madrid** (2005 y 2006).

4.2. Miembro de la **Comisión de Garantía de Calidad** del Grado de Matemáticas de la URJC (desde el curso 2015-16 hasta la actualidad) .

4.3. Colaboración con la **Comisión de Adaptaciones y Convalidaciones** de la Escuela Superior de Ingeniería Informática de la URJC (Curso 2014-2015)

4.4. Actividad como **tutora integral**. El programa de Tutorías Integrales de la URJC plantea una tutorización personalizada del alumno, desde su entrada en la universidad hasta su graduación, con reuniones periódicas grupales e individuales con el tutor (al menos tres por curso).

- Grado en Matemáticas (5 cursos, fechas nombramientos 1.09.2012, 01.09.2014, 01.09.2015, 01.09.2016,01.09.2017),
- Doble Grado Ing. Informática y Matemáticas (5 cursos, fechas nombramientos 1.09.2013, 01.09.2014,01.09.2015, 01.09.2016,01.09.2017),
- Doble Grado Ingeniería del Software y Matemáticas (3 cursos, fechas nombramientos, 01.09.2015,01.09.2016, 01.09.2017)

4.5. Tutora en el **proyecto de Aprendizaje Servicio** "¿Seguro que estás seguro?" Ing. en Ciberseguridad, curso 2018-19.

GESTIÓN

---

1. **Claustral de la U. de Oviedo** representando al colectivo de Estudiantes de Tercer Ciclo, (de marzo de 2001, a octubre de 2003)

2. **Miembro de la Comisión de Selección del Área de Gestión de Matemáticas**, Programa Nacional de Proyectos de Investigación Fundamental, MTM, (2011).

3. Miembro **(vocal) de la Junta de Gobierno de la Real Sociedad Matemática Española desde noviembre de 2017**. Miembro además de la **Comisión de**

Publicaciones desde junio de 2019, secretaria de la **Comisión de Transferencia** desde octubre de 2021.

4. Miembro de la **Comisión de Investigación del Departamento MACIMTE** en la URJC (desde 2014).

5. Miembro de la **Comisión de Doctorado de la Universidad Rey Juan Carlos** (desde julio de 2014 hasta octubre de 2019)

6. Miembro de la **Comisión de Garantía de Calidad de la Titulación del Grado de Matemáticas de la ETSII**, Universidad Rey Juan Carlos, desde diciembre de 2015.

7. Miembro Electo del **Claustro de la Universidad Rey Juan** Carlos (desde julio de 2022).