Currículum Vítae

Ángel Luis Pérez del Pozo

Septiembre 2023

Índice

1 Situación profesional actual

Entidad empleadora: Universidad Rey Juan Carlos.
Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
Categoría profesional: Profesor Titular de Universidad.

2 Formación académica

1. **Titulación:** Licenciado en Matemáticas.
   Perfil: Matemática Fundamental.
   Entidad de titulación: Universidad Complutense de Madrid.
   Fecha de titulación: 10/07/2001.
   Calificación media del expediente académico: 2,97 (1=aprobado, 2=notable, 3=sobresaliente, 4=matrícula de honor).
   Premios: Premio extraordinario de licenciatura.

2. **Titulación:** Doctor en Matemáticas.
   Entidad de titulación: Universidad Complutense de Madrid.
   Fecha de titulación: 10/11/2005.
   Título de la tesis: Concursos invariantes en superficies de Riemann.
   Codirectores: Emilio Bujalance García y José Manuel Gamboa Mutuberría.
   Calificación: Sobresaliente cum laude.

3 Experiencia Docente

3.1 Resumen

- Horas impartidas en estudios de grado: 2.500.
- Horas impartidas en estudios de licenciatura e ingeniería (plan antiguo): 715.
- Horas impartidas en estudios de máster: 195.
- Trabajos de fin de grado dirigidos: 7.

3.2 Asignaturas de grado impartidas en la URJC

1. **Asignatura:** Estructuras Algebraicas.
   Titulación: Grado en Matemáticas (y dobles grados vinculados).
   Cursos académicos: 8 (de 2014/15 a 2021/22).
   Horas impartidas: 480.

2. **Asignatura:** Estructuras Algebraicas Avanzadas.
   Titulación: Grado en Matemáticas (y dobles grados vinculados).

Cursos académicos: 1 (2021/22).
Horas impartidas: 30.

3. **Asignatura:** Lógica.
   Titulación: Grado en Matemáticas (y dobles grados vinculados).
   Cursos académicos: 7 (de 2015/16 a 2021/22).
   Horas impartidas: 420.

4. **Asignatura:** Matemática Discreta.
   Titulación: Grado en Matemáticas (y dobles grados vinculados).
   Cursos académicos: 5 (de 2017/18 a 2021/22).
   Horas impartidas: 150.

5. **Asignatura:** Criptografía.
   Titulación: Grado en Ingeniería de la Ciberseguridad.
   Cursos académicos: 3 (de 2018/19 a 2020/21).
   Horas impartidas: 60.

6. **Asignatura:** Lógica.
   Titulación: Grado en Ingeniería del Software.
   Cursos académicos: 7 (de 2014/15 a 2020/21).
   Horas impartidas: 370.

7. **Asignatura:** Lógica.
   Titulación: Grado en Ingeniería Informática.
   Cursos académicos: 2 (2018/19 y 2019/20).
   Horas impartidas: 20.

8. **Asignatura:** Matemática Discreta y Álgebra.
   Titulación: Grado en Ingeniería Informática.
   Cursos académicos: 2 (2016/17 y 2017/18).
   Horas impartidas: 130.

9. **Asignatura:** Cálculo.
   Titulación: Grado en Ingeniería de Computadores.
   Cursos académicos: 1 (2016/17).
   Horas impartidas: 6.

10. **Asignatura:** Matemáticas.
    Titulación: Grado en Ciencias Ambientales.
    Cursos académicos: 3 (de 2014/15 a 2016/17).
    Horas impartidas: 215.

11. **Asignatura:** Álgebra Lineal.
    Titulación: Grado en Matemáticas (y dobles grados vinculados).
    Cursos académicos: 1 (2015/16).
    Horas impartidas: 30.

12. **Asignatura:** Matemáticas II.
    Titulación: Grado en Ingeniería Ambiental.
    Cursos académicos: 2 (2011/12 y 2015/16).
    Horas impartidas: 47.

13. **Asignatura:** Lógica.
    Titulación: Grado en Ingeniería Informática Online.
    Cursos académicos: 2 (2013/14 y 2014/15).
    Horas impartidas: 75.

14. **Asignatura:** Matemática Discreta y Álgebra.
    Titulación: Grado en Ingeniería del Software.
    Cursos académicos: 5 (2009/2010, 2010/11, 2011/12, 2013/14 y 2014/15).
    Horas impartidas: 260.

15. **Asignatura:** Matemáticas I.
    Titulación: Grado en Ingeniería de la Energía.
    Cursos académicos: 1 (2014/15).
    Horas impartidas: 20.

16. **Asignatura:** Álgebra.
    Titulación: Grado en Ingeniería de Computadores.
    Cursos académicos: 1 (2011/12).
    Horas impartidas: 80.

17. **Asignatura:** Matemáticas I.
    Titulación: Grado en Ingeniería en Tecnologías Industriales.
    Cursos académicos: 1 (2011/12).
    Horas impartidas: 37.

18. **Asignatura:** Matemáticas II.
    Titulación: Grado en Ingeniería de Materiales.
    Cursos académicos: 1 (2011/12).
    Horas impartidas: 20.

19. **Asignatura:** Matemáticas.
    Titulación: Grado en Ciencia y Tecnología de los Alimentos.
    Cursos académicos: 1 (2010/11).
    Horas impartidas: 20.

20. **Asignatura:** Matemáticas II.
    Titulación: Grado en Ingeniería Química.
    Cursos académicos: 1 (2009/10).
    Horas impartidas: 30.

3.3 Asignaturas de licenciatura e ingeniería (plan antiguo)

1. **Asignatura:** Lógica Matemática.
   Titulación: Ingeniería Informática.

Universidad: URJC.
Cursos académicos: 3 (de 2007/08 a 2009/2010).
Horas impartidas: 99.

2. **Asignatura:** Matemática Discreta y Álgebra.
   Titulación: Ingeniería Informática.
   Universidad: URJC.
   Cursos académicos: 3 (de 2007/08 a 2009/2010).
   Horas impartidas: 206.

3. **Asignatura:** Seguridad Informática.
   Titulación: Ingeniería Informática.
   Universidad: URJC.
   Cursos académicos: 2 (2008/09 y 2009/2010).
   Horas impartidas: 60.

4. **Asignatura:** Álgebra.
   Titulación: Ingeniería Técnica en Informática de Sistemas.
   Universidad: URJC.
   Cursos académicos: 1 (2007/08).
   Horas impartidas: 35.

5. **Asignatura:** Matemática Aplicada a la Geología.
   Titulación: Licenciatura en Geología.
   Universidad: Universidad Complutense de Madrid.
   Cursos académicos: 1 (2006/07).
   Horas impartidas: 90.

6. **Asignatura:** Álgebra Lineal y Geometría.
   Titulación: Licenciatura en Matemáticas.
   Universidad: Universidad Complutense de Madrid.
   Cursos académicos: 1 (2005/06).
   Horas impartidas: 120.

7. **Asignatura:** Ingeniería Asistida por Ordenador I.
   Titulación: Ingeniería Técnica en Diseño Industrial.
   Universidad: Universidad Antonio de Nebrija.
   Cursos académicos: 1 (2005/06).
   Horas impartidas: 90.

8. **Asignatura:** Álgebra.
   Titulación: Ingeniería Informática.
   Universidad: Universidad Complutense de Madrid.
   Cursos académicos: 1 (2004/05).
   Horas impartidas: 15.

3.4 Asignaturas de máster impartidas en la URJC

1. **Asignatura:** Criptografía y Criptoanálisis.
   Titulación: Máster en Ciberseguridad y Privacidad (título propio).
   Cursos académicos: 5 (de 2017/2018 a 2021/2022).
   Horas impartidas: 150.

2. **Asignatura:** Modelado Geométrico Avanzado.
   Titulación: Máster en Informática Gráfica, Juegos y Realidad Virtual.
   Cursos académicos: 3 (de 2007/08 a 2009/2010).
   Horas impartidas: 45.

3.5 Trabajos de fin de grado dirigidos en la URJC

1. **Título:** Bases de Gröbner.
   Titulación: Grado en Matemáticas.
   Curso: 2021/22.

2. **Título:** Estudio algebraico de un rompecabezas clásico: el cubo mágico.
   Titulación: Grado en Matemáticas.
   Curso: 2020/21.

3. **Título:** Métodos numéricos para el Álgebra Lineal: resolución directa de sistemas y cálculo y aproximación de autovalores y autovectores.
   Titulación: Grado en Matemáticas.
   Curso: 2020/21.

4. **Título:** Criptografía poscuántica basada en isogenias.
   Titulación: Grado en Matemáticas.
   Curso: 2020/21.
   Premios: Accésit al premio "Tengo un proyecto" del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" al mejor TFG o TFM en el Área de Criptología y Seguridad de la Información.

5. **Título:** Criptografía sobre curvas elípticas. Cifrado basado en identidades.
   Titulación: Grado en Matemáticas.
   Curso: 2019/20.

6. **Cotutor:** Marta Beltrán Pardo. **Título:** Uso de blockchain como respaldo para el proceso de alta.
   Titulación: Grado en Ingeniería del Software.
   Curso: 2019/20.

7. **Título:** Herramientas en Teoría de Números: hacia la demostración del Último Teorema de Fermat.
   Titulación: Grado en Matemáticas.
   Curso: 2018/19.

4 Experiencia investigadora

4.1 Resumen

- Evaluación positiva de un sexenio en el tramo 2005-2016.
- Publicaciones en revistas indexadas en JCR: 18.
- Publicaciones en congresos internacionales con revisión anónima por pares: 4.
- Otras ponencias impartidas y publicaciones en congresos: 3.
- Participación en proyectos de investigación internacionales: 2.
- Participación en proyectos de investigación nacionales: 9.
- Participación en contratos de investigación: 12.
- Patentes: 2.

4.2 Publicaciones en revistas indexadas en JCR

1. **Autores:** Carlos E. González-Guillén; María Isabel González Vasco; Floyd Johnson; Ángel Luis Pérez del Pozo;
   Título: *An Attack on Zawadzki's Quantum Authentication Scheme.*
   Revista: Entropy. 23 (4), pp. 389. 2021.
   DOI: `https://doi.org/10.3390/e23040389`
   Impacto JCR: 2,738. **Puesto JCR:** 42/86 en Physics, Multidisciplinary (Q2).

2. **Autores:** María Isabel González Vasco; Ángel Luis Pérez del Pozo; Claudio Soriente.
   Título: *A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols.*
   Revista: IEEE Transactions on Dependable and Secure Computing. 18 (3), pp. 1336 - 1353. 2021.
   DOI: `https://doi.org/10.1109/TDSC.2019.2919013`
   Impacto JCR: 6,791. **Puesto JCR:** 25/164 en Computer Science, Information Systems (Q1).

3. **Autores:** José Ignacio Escribano Pablos; María Isabel González Vasco; Misael Enrique Marriaga; Ángel Luis Pérez del Pozo.
   Título: *Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber.*
   Revista: Mathematics. 8 (10), pp. 1853. 2020.
   DOI: `https://doi.org/10.3390/math8101853`
   Impacto JCR: 2,258. **Puesto JCR:** 24/330 en Mathematics (Q1).

4. **Autores:** María Isabel González Vasco; Ángel Luis Pérez del Pozo; Rainer Steinwandt.
   Título: *Group Key Establishment in a Quantum-Future Scenario.*

Revista: Informatica. 31 (4), pp. 751 - 768. 2020.
DOI: https://doi.org/10.15388/20-INFOR427
Impacto JCR: 2,688. **Puesto JCR:** 35/265 en Mathematics, Applied (Q1).

5. **Autores:** David Aleja; Regino Criado; Alejandro J. García del Amo; Ángel Luis Pérez del Pozo; Miguel Romance.
Título: *Non-backtracking PageRank: From the classic model to Hashimoto matrices.*
Revista: Chaos, Solitons and Fractals. 126, pp. 283 - 291. 2019.
DOI: https://doi.org/10.1016/j.chaos.2019.06.017
Impacto JCR: 3,764. **Puesto JCR:** 10/106 en Mathematics, Interdisciplinary Applications (Q1).

6. **Autores:** José Ignacio Escribano Pablos; María Isabel González Vasco; Misael Enrique Marriaga; Ángel Luis Pérez del Pozo.
Título: *The Cracking of WalnutDSA: A Survey.*
Revista: Symmetry. 11 (9), pp. 1072. 2019.
DOI: https://doi.org/10.3390/sym11091072
Impacto JCR: 2,645. **Puesto JCR:** 29/71 en Multidisciplinary Sciences (Q2).

7. **Autores:** Regino Criado; Julio Flores; Esther García; Alejandro J. García del Amo; Ángel Luis Pérez del Pozo; Miguel Romance.
Título: *On the alpha-nonbacktracking centrality for complex networks: existence and limit cases.*
Revista: Journal of Computational and Applied Mathematics. 350, pp. 35 - 45. 2019.
DOI: https://doi.org/10.1016/j.cam.2018.09.048
Impacto JCR: 2,037. **Puesto JCR:** 43/261 en Mathematics, Applied (Q1).

8. **Autores:** Regino Criado; Santiago Moral; Ángel Luis Pérez del Pozo; Miguel Romance.
Título: *On the edges' PageRank and line graphs.*
Revista: Chaos. 28. 2018.
DOI: https://doi.org/10.1063/1.5020127
Impacto JCR: 2,643. **Puesto JCR:** 19/254 en Mathematics, Applied (Q1).

9. **Autores:** Maria Isabel González Vasco; Ángel Luis Pérez del Pozo; Adriana Suárez Corona.
Título: *Group key exchange protocols withstanding ephemeral key reveals.*
Revista: IET Information Security. 12 (1), pp. 79 - 86. 2018.
DOI: https://doi.org/10.1049/iet-ifs.2017.0131
Impacto JCR: 0,949. **Puesto JCR:** 71/104 en Computer Science, Theory and Methods (Q3).

10. **Autores:** Paolo D'Arco; María Isabel González Vasco; Ángel Luis Pérez del Pozo; Claudio Soriente; Rainer Steinwandt.
Título: *Private Set Intersection: New Generic Constructions and Feasability Results.*

Revista: Advances in Mathematics of Communications. 11 (3), pp. 481 - 502. 2017.
DOI: http://dx.doi.org/10.3934/amc.2017040
Impacto JCR: 0,564. **Puesto JCR:** 217/242 en Mathematics, Applied (Q4).

11. **Autores:** María Isabel González Vasco; Ángel Luis Pérez del Pozo; Adriana Suárez Corona.
Título: *Pitfalls in a Server-Aided Authenticated Group Key Establishment.*
Revista: Information Sciences. 363, pp. 1 (7). 2016.
DOI: https://doi.org/10.1016/j.ins.2016.05.004
Impacto JCR: 4,832. **Puesto JCR:** 7/146 en Computer Science, Information Systems (Q1).

12. **Autores:** Santiago Moral; Víctor Chapela; Regino Criado; Ángel Luis Pérez del Pozo; Miguel Romance.
Título: *Efficient algorithms for estimating loss of information in a complex network: Applications to intentional risk analysis.*
Revista: Networks and heterogeneus media. 10 (1), pp. 195 - 208. 2015.
DOI: http://dx.doi.org/10.3934/nhm.2015.10.195
Impacto JCR: 0,925. **Puesto JCR:** 62/101 en Mathematics, Interdisciplinary Applications (Q3).

13. **Autores:** María Isabel González Vasco; Ángel Luis Pérez del Pozo; Pedro Taborda Duarte; Jorge L. Villar.
Título: *Cryptanalysis of a key exchange scheme based on block matrices.*
Revista: Information Sciences. 276, pp. 319 - 331. 2014.
DOI: https://doi.org/10.1016/j.ins.2013.11.009
Impacto JCR: 4,038. **Puesto JCR:** 6/139 en Computer Science, Information Systems (Q1).

14. **Autores:** Paolo D'Arco; Ángel Luis Pérez del Pozo.
Título: *Toward tracing and revoking schemes secure against collusion and any form of secret information leakage.*
Revista: International Journal of Information Security. 12 (1), pp. 1 - 17. 2013.
DOI: http://dx.doi.org/10.1007%2Fs10207-012-0186-1
Impacto JCR: 0,941. **Puesto JCR:** 41/102 en Computer Science, Theory and Methods (Q2).

15. **Autores:** María Isabel González Vasco; Ángel Luis Pérez del Pozo; Pedro Taborda Duarte.
Título: *A note on the security of MST3.*
Revista: Designs, Codes, and Cryptography. 55 (2), pp. 189 - 200. 2010.
DOI: https://doi.org/10.1007/s10623-010-9373-0
Impacto JCR: 0,771. **Puesto JCR:** 121/236 en Mathematics, Applied (Q3).

16. **Autores:** Ángel Luis Pérez del Pozo.
Título: *Automorphism groups of compact bordered Klein surfaces with invariant subsets.*

Revista: Manuscripta Mathematica. 122 (2), pp. 163 - 172. 01/02/2007.
DOI: https://doi.org/10.1007/s00229-006-0061-3
Impacto JCR: 0,316. **Puesto JCR:** 172/207 en Mathematics (Q4).

17. **Autores:** Ángel Luis Pérez del Pozo.
Título: *On the weights of the fixed points of an automorphism of a compact Riemann surface.*
Revista: Archiv der Mathematik. 86 (1), pp. 50 - 55. 2006.
DOI: https://doi.org/10.1007/s00013-005-1473-0
Impacto JCR: 0,341. **Puesto JCR:** 139/187 en Mathematics (Q4).

18. **Autores:** Ángel Luis Pérez del Pozo.
Título: *Gap sequences on Klein surfaces.*
Revista: Journal of Pure and Applied Algebra. 195 (3), pp. 281 - 292. 2005.
DOI: https://doi.org/10.1016/j.jpaa.2004.08.002
Impacto JCR: 0,551. **Puesto JCR:** 61/181 en Mathematics (Q2).

4.3 Publicaciones en congresos internacionales con revisión anónima por pares

1. **Congreso:** International Symposium on Mathematical Foundations of Computer Science (MFCS), 2018.
Autores: Paolo D'Arco; Roberto De Prisco; Alfredo De Santis; Ángel Luis Pérez del Pozo; Ugo Vaccaro.
Título: *Probabilistic Secret Sharing.*
Actas: Leibniz International Proceedings in Informatics (LIPIcs). 117, pp. 64:1 - 64:16. 2018.
DOI: https://doi.org/10.4230/LIPIcs.MFCS.2018.64
Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

2. **Congreso:** Cyberspace Safety and Security (CCS), 2018.
Autores: Paolo D'Arco; Roberto De Prisco; Ángel Luis Pérez del Pozo.
Título: *An Efficient and Reliable Two-Level Lightweight Authentication Protocol.*
Actas: Lecture Notes in Computer Science (LNCS). 11161, pp. 168–180. 2018.
DOI: https://doi.org/10.1007/978-3-030-01689-0_14

3. **Congreso:** AFRICACRYPT, 2012
Autores: Paolo D'Arco; María Isabel González Vasco; Ángel Luis Pérez del Pozo; Claudio Soriente.
Título: *Size-Hiding in Private Set Intersection: Existential Results and Constructions.*
Actas: Lecture Notes in Computer Science (LNCS). 7374, pp. 378 – 394. 2012.
DOI: https://doi.org/10.1007/978-3-642-31410-0_23
Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

4. **Congreso:** International Conference on Applied Cryptography and Network Security (ACNS), 2011.
   Autores: Paolo D'Arco; Ángel Luis Pérez del Pozo.
   Título: *Fighting Pirates 2.0.*
   Actas: Lecture Notes in Computer Science (LNCS). 6715, pp. 359 – 376. 2011.
   DOI: `https://doi.org/10.1007/978-3-642-21554-4_21`
   Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

4.4 Otras ponencias impartidas y publicaciones en congresos

1. **Congreso:** X Reunión Española sobre Criptología y Seguridad de la Información (RECSI), 2008.
   Lugar de celebración: Salamanca, España. **Autores:** Maria Isabel González Vasco; Ángel Luis Pérez del Pozo.
   Título: *Related message attacks: a formal treatment.*
   Actas: Actas X Reunión Española Sobre Criptografía y Seguridad de la Información (RECSI X). pp. 111 - 118. ISBN 978-84-691-5158-7.
   Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

2. **Congreso:** Reunión anual del RAAG, 2004.
   Lugar de celebración: Salamanca, España. **Autores:** Ángel Luis Pérez del Pozo.
   Título: *Gap sequences on real algebraic curves.*
   Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

3. **Congreso:** Conformal Geometry, Discrete Groups and Surfaces, 2003.
   Lugar de celebración: Bedlewo, Polonia. **Autores:** Ángel Luis Pérez del Pozo.
   Título: *Special points on Klein surfaces.*
   Ponencia: Ángel Luis Pérez del Pozo impartió una ponencia en el congreso.

4.5 Participación en proyectos de investigación internacionales

1. **Título:** Secure Communication in the Quantum Era.
   Referencia: SPSG5448.
   Entidad financiadora: OTAN (programa Science for Peace and Security).
   Fecha inicio: 30/09/2018. **Fecha finalización:** 30/09/2021.
   Investigadores principales: Otokar Grosek y María Isabel González Vasco (co-IP España).
   Cuantía: 264.200€.

2. **Título:** Real Algebraic and Analytic Geometry.
   Referencia: HPRN-CT-2001-00271.
   Entidad financiadora: Comisión Europea.
   Fecha inicio: 01/01/2002. **Fecha finalización:** 31/12/2005.

Investigadores principales: Niels Schwarz y Antonio Díaz-Cano Ocaña (co-IP España).
Número de investigadores: 70. **Cuantía:** 224.867€.

4.6 Participación en proyectos de investigación nacionales

1. **Título:** Criptografía para retos digitales emergentes: escenarios multi-usuario y seguridad post-cuántica (CREEME).
   Referencia: PID2019- 109379RB-100.
   Entidad financiadora: Ministerio de Ciencia e Innovación.
   Fecha inicio: 1/01/2020. **Fecha finalización:** 31/10/2022.
   Investigadores principales: Javier Herranz Sotoca y María Isabel González Vasco.
   Número de investigadores: 9. **Cuantía:** 37.147€.

2. **Título:** Criptografía avanzada para afrontar nuevos retos de la sociedad digital.
   Referencia: MTM2016-77213-R.
   Entidad financiadora: Ministerio de Economía y Empresa.
   Fecha inicio: 30/12/2016. **Fecha finalización:** 29/09/2020.
   Investigadores principales: Javier Herranz Sotoca.
   Número de investigadores: 10. **Cuantía:** 84.337€.

3. **Título:** Hacia una sociedad digital segura: avances matemáticos en criptografía y su impacto en las tecnologías digitales.
   Referencia: MTM2013-41426-R.
   Entidad financiadora: Ministerio de Economía y Empresa.
   Fecha inicio: 01/01/2014. **Fecha finalización:** 31/12/2017.
   Investigadores principales: Jorge Villar Santos.
   Número de investigadores: 10. **Cuantía:** 42.350€.

4. **Título:** Seguridad demostrable: validación de herramientas criptográficas a través del Álgebra y la Matemática Discreta.
   Referencia: MTM2010-15167.
   Entidad financiadora: Ministerio de Economía y Empresa.
   Fecha inicio: 01/01/2011. **Fecha finalización:** 31/12/2014.
   Investigadores principales: María Isabel González Vasco.
   Número de investigadores: 5. **Cuantía:** 40.777€.

5. **Título:** Matemáticas e Información Cuántica.
   Referencia: CCG08-UCM/ESP.
   Entidad financiadora: Universidad Complutense de Madrid/Comunidad de Madrid.
   Fecha inicio: 01/01/2009. **Fecha finalización:** 31/12/2009.
   Investigadores principales: David Pérez García.
   Número de investigadores: 8. **Cuantía:** 6.000€.

6. **Título:** Geometría Algebraica y Analítica Real.
   Referencia: GRUPO UCM 910444.

Entidad financiadora: Universidad Complutense de Madrid.
Fecha inicio: 01/01/2006. **Fecha finalización:** 31/12/2008.

7. **Título:** Geometría Real.
   Referencia: MTM2005-02865.
   Entidad financiadora: Dirección General de Investigación Científica y Técnica.
   Fecha inicio: 01/01/2006. **Fecha finalización:** 31/12/2008.
   Investigadores principales: Jesús Ruiz Sancho.
   Número de investigadores: 22. **Cuantía:** 99.000€.

8. **Título:** Geometría, Álgebra y Algoritmos Reales.
   Referencia: BFM2002-04797.
   Entidad financiadora: Dirección General de Investigación Científica y Técnica.
   Fecha inicio: 01/01/2003. **Fecha finalización:** 31/12/2005.
   Investigadores principales: Jesús Ruiz Sancho.
   Número de investigadores: 15. **Cuantía:** 57.600€.

9. **Título:** Geometría Algebraica y Analítica Real y Algoritmos.
   Referencia: PB98-0756-C02-01.
   Entidad financiadora: Dirección General de Investigación Científica y Técnica.
   Fecha inicio: : 01/01/2002. **Fecha finalización:** 31/12/2002.

4.7 Participación en contratos de investigación

1. **Título:** Criptografía Post-Cuántica en Sistemas Embebidos (SeQure2022).
   Entidad financiadora: Arquimea Centro de Investigaciones Avanzadas SLU.
   Fecha inicio: 15/03/2022. **Fecha finalización:** 23/12/2022.
   Investigadores responsables: María Isabel González Vasco.
   Número de investigadores: 3. **Cuantía:** 36.300€.

2. **Título:** Criptografía Post-Cuántica en Sistemas Embebidos (SeQure2021).
   Entidad financiadora: Arquimea Centro de Investigaciones Avanzadas SLU.
   Fecha inicio:14/05/2021. **Fecha finalización:** 31/12/2021.
   Investigadores responsables: María Isabel González Vasco.
   Número de investigadores: 3. **Cuantía:** 25.000€.

3. **Título:** Criptografía Post-Cuántica y Cifrado Basado en Atributos.
   Entidad financiadora: BBVA Next Technologies.
   Fecha inicio: 16/06/2019. **Fecha finalización:** 01/11/2019.
   Investigadores responsables: María Isabel González Vasco.
   Número de investigadores: 2. **Cuantía:** 15.000€.

4. **Título:** Criptografía Post-Cuántica y Cifrado Basado en Atributos.
   Entidad financiadora: Blue Indico Investments SL.
   Fecha inicio: 13/07/2018. **Fecha finalización:** 15/10/2018.
   Investigadores responsables: María Isabel González Vasco.
   Número de investigadores: 2. **Cuantía:** 18.750€.

5. **Título:** Criptografía y algoritmos post-cuánticos.
   Entidad financiadora: I4S (Grupo BBVA).
   Fecha inicio: 01/03/2017. **Fecha finalización:** 31/07/2017.
   Investigadores responsables: Regino Criado Herrero.
   Número de investigadores: 3. **Cuantía:** 30.500€.

6. **Título:** Whitebox cryptography y searchable encryption.
   Entidad financiadora: I4S (Grupo BBVA).
   Fecha inicio: 01/03/2017. **Fecha finalización:** 31/07/2017.
   Investigadores responsables: Regino Criado Herrero.
   Número de investigadores: 3. **Cuantía:** 30.500€.

7. **Título:** Estudio de algoritmos para la creación de una aduana de datos.
   Entidad financiadora: I4S (Grupo BBVA).
   Fecha inicio: 01/10/2014. **Fecha finalización:** 30/06/2015.
   Investigadores responsables: Regino Criado Herrero y María Isabel González Vasco.
   Número de investigadores: 4. **Cuantía:** 45.000€.

8. **Título:** Base de datos (Dataset).
   Entidad financiadora: I4S (Grupo BBVA).
   Fecha inicio: 01/10/2014. **Fecha finalización:** 30/06/2015.
   Investigadores responsables: Regino Criado Herrero y Miguel Romance del Río.
   Número de investigadores: 4. **Cuantía:** 65.000€.

9. **Título:** Modelos cuantitativos para la predicción y el análisis de la disponibilidad de parques de ATMs.
   Entidad financiadora: BBVA.
   Fecha inicio: 01/09/2011. **Fecha finalización:** 30/06/2012.
   Investigadores responsables: Regino Criado Herrero.
   Número de investigadores: 4. **Cuantía:** 42.327€.

10. **Título:** Análisis de algoritmos de tokenización y asesoramiento teórico para su implementación.
    Entidad financiadora: BBVA.
    Fecha inicio: 01/12/2010. **Fecha finalización:** 30/09/2011.
    Investigadores responsables: Regino Criado Herrero.
    Número de investigadores: 4. **Cuantía:** 34.317€.

11. **Título:** Análisis de Riesgos Tecnológicos, inversión vs nivel de servicio.
    Entidad financiadora: BBVA.
    Fecha inicio: 01/09/2010. **Fecha finalización:** 30/06/2011.
    Investigadores responsables: Regino Criado Herrero.
    Número de investigadores: 4. **Cuantía:** 39.597€.

12. **Título:** Análisis de algoritmos de tokenización: estado del arte.
    Entidad financiadora: BBVA.

Fecha inicio: 01/09/2010. **Fecha finalización:** 30/06/2011.
Investigadores responsables: Regino Criado Herrero.
Número de investigadores: 4. **Cuantía:** 17.601€.

4.8 Patentes

1. **Inventores:** Antonio Faonio, María Isabel González Vasco, Ángel Luis Pérez del Pozo, Claudio Soriente.
Título: Password Authenticated Public Key Establishment.
Nº de solicitud: 62/941,908
País de prioridad: EE.UU.
Fecha 2020 (contrato de cesión).
Entidad titular: NEC Laboratories Europe.
Rendimiento inicial: URJC vende su participación a NEC por 1.700€.

2. **Inventores:** María Isabel González Vasco, Ángel Luis Pérez del Pozo, Claudio Soriente.
Título: DAPAKE: Dynamic Anonymous Password-Based Key Exchange.
Nº de solicitud: 62/688,342
Nº publicación: US publication No. 2019/0349191A1
País de prioridad: EE.UU.
Fecha 2018 (contrato de cesión), 2019 (publicación).
Entidad titular: NEC Laboratories Europe.
Rendimiento inicial: URJC vende su participación a NEC por 2.750€.

5 Estancias de investigación en centros extranjeros

1. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
Fecha inicio: 20/05/2018. **Fecha fin:** 09/06/2018.
Resultados obtenidos: Esta estancia dio lugar a la publicación *An Efficient and Reliable Two-Level Lightweight Authentication Protocol* en el congreso CCS 2018.

2. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
Fecha inicio: 17/05/2017. **Fecha fin:** 07/06/2017.
Resultados obtenidos: Esta estancia dio lugar a la publicación *Probabilistic Secret Sharing* en el congreso MFCS 2018.

3. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
Fecha inicio: 01/07/2015. **Fecha fin:** 11/07/2015.
Resultados obtenidos: El trabajo de esta estancia, junto con la anterior en 2014, dio lugar a la publicación *Toward tracing and revoking schemes secure against collusion and any form of secret information leakage* en la revista International Journal of Information Security.

4. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
Fecha inicio: 25/05/2014. **Fecha fin:** 06/06/2014.

Resultados obtenidos: Se inicia el trabajo en esquemas de trazado y revocación que, continuado en la estancia de 2015, dio lugar a la publicación que se menciona como resultado de dicha estancia.

5. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
   Fecha inicio: 05/05/2012. **Fecha fin:** 17/05/2012.
   Resultados obtenidos: El trabajo de esta estancia, junto con la anterior en 2011, dio lugar a las publicacies *Size-Hiding in Private Set Intersection: Existential Results and Constructions* en el congreso AFRICACRYPT 2012 y *Private Set Intersection: New Generic Constructions and Feasability Results* en la revista Advances in Mathematics of Communications.

6. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
   Fecha inicio: 10/03/2011. **Fecha fin:** 14/04/2011.
   Resultados obtenidos: Se inicia el trabajo en protocolos para el cálculo privado de la intersección de conjuntos que, continuado en la estancia de 2012, dio lugar a la publicaciones que se mencionan como resultado de dicha estancia.

7. **Centro:** Dipartimento di Informatica. Università di Salerno. Italia.
   Fecha inicio: 29/06/2009. **Fecha fin:** 27/07/2009.
   Resultados obtenidos: Esta estancia dio lugar a la publicación *Fighting Pirates 2.0* en el congreso ACNS 2011.

8. **Centro:** Department of Mathematics, Computer Science and Statistics. Purdue University Calumet. EEUU.
   Fecha inicio: 02/09/2004. **Fecha fin:** 20/12/2004.
   Resultados obtenidos: Durante esta estancia predoctoral se avanzó en varios de los problemas que dieron lugar a la tesis doctoral *Conjuntos invariantes en superficies de Riemann.*

6 Ayudas y becas recibidas

1. Ayuda a la movilidad.
   Entidad financiadora: Universidad Rey Juan Carlos.
   Programa: Programa propio de fomento y desarrollo de la investigación.
   Propósito: Estancia de investigación en la Università di Salerno.
   Año: 2009. **Cuantía:** 2.050€.

2. Beca para la Formación del Profesorado Universitario (FPU).
   Entidad financiadora: Ministerio de Educación y Cultura.
   Institución: Universidad Complutense de Madrid.
   Centro: Facultad de Matemáticas.
   Fecha inicio: 01/01/2002. **Fecha fin:** 30/11/2005.

7 Experiencia profesional

7.1 Puestos desempeñados en la universidad

1. **Categoría:** Profesor titular de universidad.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
   Fecha inicio: 16/12/2022. **Fecha fin:** -

2. **Categoría:** Profesor contratado doctor.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
   Fecha inicio: 10/10/2022. **Fecha fin:** 15/12/2022.

3. **Categoría:** Profesor contratado doctor interino.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
   Fecha inicio: 14/12/2020. **Fecha fin:** 09/10/2022.

4. **Categoría:** Profesor ayudante doctor.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
   Fecha inicio: 18/11/2019. **Fecha fin:** 13/12/2020.

5. **Categoría:** Profesor visitante.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica.
   Fecha inicio: 23/04/2014. **Fecha fin:** 17/11/2019.

6. **Categoría:** Profesor visitante.
   Dedicación: Tiempo parcial.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada.
   Fecha inicio: 01/09/2013. **Fecha fin:** 22/04/2014.

7. **Categoría:** Profesor visitante.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.

Departamento: Matemática Aplicada.
Fecha inicio: 01/09/2011. **Fecha fin:** 31/08/2012.

8. **Categoría:** Personal investigador.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada.
   Fecha inicio: 01/10/2010. **Fecha fin:** 31/08/2011.

9. **Categoría:** Profesor ayudante doctor.
   Dedicación: Tiempo completo.
   Entidad: Universidad Rey Juan Carlos.
   Departamento: Matemática Aplicada.
   Fecha inicio: 01/10/2007. **Fecha fin:** 30/09/2010.

10. **Categoría:** Profesor ayudante.
    Dedicación: Tiempo completo.
    Entidad: Universidad Complutense de Madrid.
    Departamento: Matemática Aplicada - Biomatemática.
    Fecha inicio: 24/11/2006. **Fecha fin:** 30/09/2007.

11. **Categoría:** Profesor titular de universidad interino.
    Dedicación: Tiempo completo.
    Entidad: Universidad Complutense de Madrid.
    Departamento: Álgebra.
    Fecha inicio: 22/02/2006. **Fecha fin:** 31/08/2006.

12. **Categoría:** Becario FPU.
    Dedicación: Tiempo completo.
    Entidad: Universidad Complutense de Madrid.
    Departamento: Álgebra.
    Fecha inicio: 01/01/2002. **Fecha fin:** 31/12/2005.

7.2 Experiencia profesional fuera de la universidad

1. Consultor de seguridad en las empresas Solium e Innovation For Security (100% participadas por el grupo BBVA).
   Fecha inicio: 01/09/2012. **Fecha fin:** 21/04/2014.

2. Aprobada la oposición para profesor de enseñanza secundaria de Matemáticas en el año 2006. Profesor de Matemáticas en el IES Máximo Trueba de Boadilla del Monte.
   Fecha inicio: 01/09/2006. **Fecha fin:** 23/11/2006.

8 Evaluación de la actividad docente

8.1 Tramos de Docentia

Obtenidos dos tramos del programa Docentia en la Universidad Rey Juan Carlos:

- Convocatoria Docentia 2020: Notable.
- Convocatoria Docentia 2017: Favorable.

8.2 Encuentas de alumnos

Se incluyen los resultados de encuestas realizadas a los alumnos de la mayoría de las asignaturas impartidas en la URJC. Las valoraciones se realizan respondiendo a varias preguntas, en una escala del 1 al 5.

Asignatura	Titulación	Curso	Valoración
Lógica Matemática	Ingeniería Informática	2007/08	3,86
Álgebra	Ing. Téc. en Inf. de Sist.	2007/08	3,98
Mat. Disc. y Álgebra	Ingeniería Informática	2007/08	4,13
Álgebra	Ing. Téc. en Inf. de Gest.	2007/08	3,94
Mod. Geom. Avanz.	Mást. Inf. Gráf., Jue. y R.V.	2007/08	3,43
Lógica Matemática	Ingeniería Informática	2008/09	3,61
Mat. Disc. y Álgebra	Ingeniería Informática	2008/09	4,14
Seguridad Informática	Ingeniería Informática	2008/09	3,95
Mod. Geom. Avanz.	Mást. Inf. Gráf., Jue. y R.V.	2008/09	3,75
Mat. Disc. y Álgebra	Gr. en Ing. Soft.	2009/10	4,40
Matemáticas II	Gr. en Ing. Quím.	2009/10	4,24
Seguridad Informática	Ingeniería Informática	2009/10	3,95
Mat. Disc. y Álgebra	Gr. en Ing. Soft.	2010/11	4,60
Matemáticas I	Gr. en Ing. Tec. Ind.	2011/12	4,54
Mat. Disc. y Álgebra	D. Gr. en Ing. Soft. y Mat.	2011/12	4,53
Matemáticas II	Gr. en Ing. Amb.	2011/12	4,06
Álgebra	Gr. en Ing. Comp.	2011/12	4,40
Matemáticas II	Gr. en Ing. Mat.	2011/12	3,98
Mat. Disc. y Álgebra	D. Gr. en Ing. Inf. y Mat.	2013/14	4,25
Lógica	Gr. en Ing. Inf. Online	2013/14	4,31
Matemáticas I	Gr. en Ing. Energ.	2014/15	3,74
Lógica	Gr. en Ing. Soft.	2014/15	4,45
Mat. Disc. y Álgebra	Gr. en Ing. Soft.	2014/15	4,37
Matemáticas	Gr. en Ciencias Amb.	2014/15	4,00
Álgebra	Gr. en Ing. Comp.	2014/15	3,88
Estructuras Algebraicas	Gr. en Matemáticas	2014/15	4,08
Álgebra Lineal	Gr. en Matemáticas	2015/16	3,79
Lógica	Gr. en Matemáticas	2015/16	4,75
Lógica	Gr. en Ing. Soft.	2015/16	4,38
Matemáticas	Gr. en Ciencias Amb.	2015/16	4,13
Estructuras Algebraicas	Gr. en Matemáticas	2015/16	4,57
Matemáticas II	Gr. en Ing. Amb.	2015/16	4,19

Lógica	Gr. en Matemáticas	2016/17	4,38
Mat. Disc. y Álgebra	Gr. en Ing. Inf.	2016/17	4,44
Lógica	Gr. en Ing. Soft.	2016/17	4,39
Matemáticas	Gr. en Ciencias Amb.	2016/17	4,07
Estructuras Algebraicas	Gr. en Matemáticas	2016/17	4,67
Lógica	Gr. en Matemáticas	2017/18	4,51
Mat. Disc. y Álgebra	Gr. en Ing. Inf.	2017/18	4,53
Lógica	Gr. en Ing. Soft.	2017/18	4,28
Estructuras Algebraicas	Gr. en Matemáticas	2017/18	4,34
Lógica	Gr. en Matemáticas	2018/19	4,58
Mat. Disc.	Gr. en Matemáticas	2018/19	4,68
Lógica	Gr. en Ing. Soft.	2017/18	4,49
Estructuras Algebraicas	Gr. en Matemáticas	2018/19	4,50
Criptografía	Gr. en Ing. Ciber.	2018/19	4,29
Lógica	Gr. en Matemáticas	2019/20	4,60
Mat. Disc.	Gr. en Matemáticas	2019/20	4,20
Lógica	Gr. en Ing. Soft.	2019/20	4,30
Estructuras Algebraicas	Gr. en Matemáticas	2019/20	4,80
Mat. Disc.	Gr. en Matemáticas	2020/21	4,40
Estructuras Algebraicas	Gr. en Matemáticas	2020/21	4,40
Criptografía	Gr. en Ing. Ciber.	2020/21	4,70
Lógica	Gr. en Matemáticas	2021/22	4,70
Mat. Disc.	Gr. en Matemáticas	2021/22	4,80

9 Formación para la docencia

9.1 Titulaciones

1. **Titulación:** Certificado de Aptitud Pedagógica (CAP).
   Institución: Universidad Complutense de Madrid.
   Centro: Instituto de Ciencias de la Educación.
   Año de obtención: 2002.

9.2 Cursos recibidos

1. **Título:** Summer School on Provable Security 2009.
   Entidad organizadora: ECRYPT II / Red Temática Matemáticas en la Sociedad de la Información / iMath.
   Año impartición: 2009. **Nº horas:** 20.

2. **Título:** Summer School on Provable Security 2008.
   Entidad organizadora: ECRYPT II / Red Temática Matemáticas en la Sociedad de la Información / iMath.
   Año impartición: 2008 **Nº horas:** 20.

3. **Título:** Fundamentos Matemáticos de la Computación Segura.
   Entidad organizadora: Universidad Complutense de Madrid.
   Año impartición: 2007. **Nº horas:** 20.

4. **Título:** Summer school on Coding Theory.
   Entidad organizadora: University of Oslo.
   Año impartición: 2007.

5. **Título:** Taller de Astronomía: El universo en tus manos.
   Entidad organizadora: Universidad Complutense de Marid.
   Año impartición: 2006.

6. **Título:** Las Matemáticas en Secundaria: un enfoque distinto del habitual.
   Entidad organizadora: Universidad Complutense de Madrid
   Año impartición: 2005. **Nº horas:** 30.

7. **Título:** Introducción al software libre.
   Entidad organizadora: Universidad Complutense de Madrid
   Año impartición: 2005. **Nº horas:** 30.

8. **Título:** Usando la criptografía clásica para explicar matemáticas en secundaria.
   Entidad organizadora: Universidad Complutense de Madrid
   Año impartición: 2005. **Nº horas:** 30.

9. **Título:** Problemas de máximos y mínimos: una aproximación a la investigación operativa.
   Entidad organizadora: Universidad Complutense de Madrid
   Año impartición: 2005. **Nº horas:** 30.

10 Otros méritos

10.1 Acreditaciones

1. Acreditación ANECA para la figura de Profesor Titular de Universidad.
   Rama de conocimiento: Ciencias. **Fecha:** 26/11/2021.

2. Acreditación ANECA para la figura de Profesor Contratado Doctor.
   Rama de conocimiento: Ciencias Experimentales. **Fecha:** 15/06/2011.

10.2 Publicaciones docentes

1. **Título:** Criptografía esencial: Principios básicos para el diseño de esquemas y protocolos seguros.
   Autores: María Isabel González Vasco; Ángel Luis Pérez del Pozo.
   Editorial: Ra-Ma. **Año de publicación:** 2021.
   ISSN: 978-84-18551-23-9
   Descripción: Pensado como libro de texto que pueda ser utilizado en asignaturas de grado o máster en cuyo temario esté incluida la Criptografía.

10.3 Participación en proyectos de innovación docente

1. **Título:** Coordinación de asignaturas para el desarrollo compartido y evaluación de competencias en el título de Grado en Ciencia y Tecnología de los Alimentos de la URJC.
   Entidad financiadora: Universidad Rey Juan Carlos.
   Fecha inicio: 01/09/2010. **Fecha finalización:** 31/08/2011.
   Investigadores principales: Isabel Sierra.

10.4 Organización de jornadas sobre docencia

1. **Función:** Miembro del comité organizador.
   Título de las jornadas: Usos y Avances en la Docencia de las Matemáticas en las Enseñanzas Universitarias (ENSEMAT 2019).
   Entidad organizadora: Universidad Rey Juan Carlos.
   Fecha: 19/09/2019. **Duración:** 8 horas.

10.5 Idiomas

1. Inglés: Completada la Escuela Oficial de Idiomas (seis años, último curso nivel Avanzado II, correspondiente a nivel B2).