Parte A. DATOS PERSONALES

Fecha del CVA	17/02/2021

Nombre y apellidos	Juan Ramón Velasco Pérez		
DNI/NIE/pasaporte	[redacted]	Edad	[redacted]
Núm. identificación del investigador	Researcher ID	B-5807-2009	
	Código Orcid	0000-0003-0239-1116	

A.1. Situación profesional actual

Organismo	Universidad de Alcalá		
Dpto./Centro	Departamento de Automática		
Dirección	Escuela Politecnica Superior. Crtra N-II, Km 31,600		
Teléfono	[redacted]	correo electrónico	[redacted]
Categoría profesional	Catedrático de Universidad	Fecha inicio	18/01/2008
Espec. cód. UNESCO	3325		
Palabras clave	Agentes inteligentes, Aprendizaje automático, Internet de las cosas, sensores		

A.2. Formación académica *(título, institución, fecha)*

Licenciatura/Grado/Doctorado	Universidad	Año
Ingeniero de telecomunicación	Politécnica de Madrid	1987
Doctor Ing. de Telecomunicación	Politécnica de Madrid	1991

A.3. Indicadores generales de calidad de la producción científica

- Tramos de productividad investigadora: 4 (1993-98, 2000-08, 2009-14 y 2015-20)
- Tramo de Transferencia: 1 (1994-2003)
- Tesis doctorales dirigidas en los últimos 10 años: 4 +1 tutorizada
- Datos según Web of Science de Thomson Reuters.
  - Indice H: 9 / Citas totales: 304
- Datos según Google académico (incluyendo todas las publicaciones)
  - Indice H: 20 / Citas totales: 1801
  - Promedio de citas/año (5 años): 70,6

Parte B. RESUMEN LIBRE DEL CURRÍCULUM

JUAN R. VELASCO (Ciudad Real, [redacted]) es Ing. de Telecomunicación (1987) y Dr. Ing. de Telecomunicación (1991) por la Universidad Politécnica de Madrid. Tras unos años como Becario de F.P.I. y profesor interino, en 1993 fue Profesor T. U. en Ingeniería Telemática en la U.P.M. Entonces colaboró en la fundación de DAEDALUS – Data, Decisions and Language, S.A., una spin-off del Grupo de Investigación en Sistemas Inteligentes de esa universidad. Entre 1998 y 2002 colaboró como gestor de la misma y Director del área de Data Mining. En 2002 se traslada al Departamento de Automática de la U. de Alcalá, donde es Catedrático de Universidad desde 2008. Ya en la UAH, entre 2003 y 2005 ha sido Gestor de Fondos FEDER para infraestructura científica en el área de comunicaciones del Ministerio de Ciencia y Tecnología. Fue Subdirector de Investigación y Relaciones con Empresas de la Escuela Politécnica Superior entre 2004 y 2008, y posteriormente Inspector Adjunto de la Inspección de Servicios de esta universidad hasta marzo de 2010. Durante 2007 y 2008 fue el coordinador del área de Tecnología Electrónica y Comunicaciones de la Comisión de Evaluación de Becas de FPU del Mº de Ciencia e Innovación. Durante el periodo 2010-2018 se hizo cargo del Vicerrectorado de Posgrado y Educación Permanente, y desde 2018 es Vicerrector de Estrategia y Planificación.

Ha formado parte de la junta directiva de la Asociación Española para la Inteligencia Artificial (AEPIA) entre 1997 y 2001, ha sido miembro de la junta directiva de la Asociación de Telemática desde su fundación hasta 2015 y es miembro de la junta directiva de la

Asociación Española de Ingenieros de Telecomunicación en la Demarcación de Castilla-La Mancha desde su creación hasta la actualidad.

Coordina el Grupo de Investigación de Alto Rendimiento en Redes y Sistemas Inteligentes, formado por 25 profesores e investigadores de los Departamentos de Automática y de Física y Matemáticas. Ha sido codirector de la Cátedra para la Mejora de la Autonomía Personal de Telefónica en la Universidad de Alcalá. A lo largo de su vida profesional ha participado en 50 proyectos y contratos de investigación (más de 30 como investigador principal), tanto con financiación pública como privada, y tiene más de 160 publicaciones científicas. Su línea principal de investigación en la actualidad se centra en la utilización de la internet de las cosas para la detección precoz de trastornos de salud, en el sentido más amplio. En 2001 le fue concedido el segundo premio “Nuevas Aplicaciones para Internet” convocado por la Cátedra Telefónica para Internet de Nueva Generación en la UPM, y en 2009 el premio a la Innovación en Comunicaciones Móviles que otorga la Fundación Vodafone España.

Parte C. MÉRITOS MÁS RELEVANTES *(ordenados por tipología)*

C.1. Publicaciones

- D. Rivera, A. García, J.E. Ortega, B. Alarcos, K. van der Meulen, J.R. Velasco, C. del Barrio. Intraindividual Variability Measurement of Fine Manual Motor Skills in Children Using an Electronic Pegboard: Cohort Study. JMIR mHealth and uHealth. Vol 7 (8). 2019. Pag. e12434.. DOI: 10.2196/12434
- D Rivera, A. Garcia, ML Martín-Ruiz, B. Alarcos, JR Velasco, A. Gomez Oliva. Secure Communications and Protected Data for an Internet of Things Smart Toy Platform. IEEE Internet of Things Vol. 6 (2), 2019. pag. 3785-3795 DOI: 10.1109/JIOT.2019.2891103
- D. Rivera, L Cruz-Piris, S. Fernández, B. Alarcos, A. García y JR Velasco. A novel method for automatic detection and classification of movement patterns in short duration playing activities. IEEE Access 2018 Vol 6). Pp 53409-53425. DOI: 10.1109/ACCESS.2018.2871732
- L Cruz-Piris, D Rivera, I Marsa-Maestre, E de la Hoz, JR Velasco. Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources. Sensors 2018, 18(3), 917, 22p; doi:10.3390/s18030917
- Fabrizio Taffoni, Diego Rivera, Angelica La Camera, Andrea Nicolò, Juan Ramón Velasco, Carlo Massaroni. A Wearable System for Real-Time Continuous Monitoring of Physical Activity. Journal of healthcare engineering, 2018 (16 pag); doi.org/10.1155/2018/1878354
- Susel Fernandez, Rafik Hadfi, Takayuki Ito, Ivan Marsa-Maestre y Juan R. Velasco. Ontology-Based Architecture for Intelligent Transportation Systems Using a Traffic Sensor Network. Sensors 2016, 16, 1287 (17 pág); doi:10.3390/s16081287
- Diego Rivera, Antonio García, Bernardo Alarcos, Juan R. Velasco, José Eugenio Ortega and Isaías Martínez-Yelmo. Smart Toys Designed for Detecting Developmental Delays. Sensors 2016, 16(11), 1953 (22 pág); doi:10.3390/s16111953
- Fernandez, S.; Marsa-Maestre, I.; Velasco, J.R.; Alarcos, B. Ontology Alignment Architecture for Semantic Sensor Web Integration. Sensors 13(9), pp:12581-12604. 2013
- Jose Angel Fernandez-prieto, Joaquin Canada-bago, Manuel Angel Gadeo-martos, Juan R. Velasco. Optimisation of control parameters for genetic algorithms to test computer networks under realistic traffic loads. Applied Soft Computing 11(4), pp: 3744-3752. 2011
- Manuel Angel Gadeo-martos, Jose Angel Fernandez-prieto, Joaquin Canada-bago, Juan Ramon Velasco-perez. An Architecture for Performance Optimization in a Collaborative Knowledge-Based Approach for Wireless Sensor Networks. Sensors 11(10), pp: 9136-9159. 2011
- Lopez-Carmona, Miguel A.; Marsa-Maestre, Ivan; de la Hoz, Enrique; Velasco, Juan R. A Region-Based Multi-Issue Negotiation Protocol For Non-Monotonic Utility Spaces. Computacional Intelligence 27(2), pp: 166-217. 2011

- Miguel A. Lopez-Carmona, Ivan Marsa-Maestre, Enrique de la Hoz and Juan R. Velasco. Using RFID to Enhance Security in Off-Site Data Storage. Sensors 10(9), pp: 8010-8027. 2010
- Joaquin Canada-Bago, Jose Angel Fernandez-Prieto, Manuel Angle Gadeo-Martos and Juan R. Velasco. A New Collaborative Knowledge-Based Approach for Wireless Sensor Networks. Sensors 10(6), pp: 6044-6062. 2010
- Miguel A. López-Carmona, Iván Marsá-Maestre, Guillermo Ibañez, Juan A. Carral, and Juan R. Velasco. Improving Trade-offs in Automated Bilateral Negotiations for Expressive and Inexpressive Scenarios. Journal of Intelligent & Fuzzy Systems 21(3), pp: 165-174. 2010

C.2. Proyectos

- TRASGO – Detección precoz de TRAStornos de desarrollo mediante el uso de juGuetes y Objetos cotidianos. M. de Ciencia, Innovación y Universidades. Referencia: RTI2018-101962-B-I00. Fechas: 01/2019-12/2022. Investigador principal. Cuantía total de la subvención: 88.935 €
- TAPIR – Técnicas Avanzadas para Potenciar la Inteligencia de las Redes 5G. Consejería de Educación, Juventud y Deporte de la CAM. Programa de Actividad de I+D entre Grupos de Investigación de la CAM. Referencia: P2018/TCS-4496. Fechas: 2019-2022. Investigador principal solicitante del grupo UAH. Cuantía total de la subvención: 819.950€
- TIGRE5 – Tecnologias integradas de gestión y operación de Red 5G. Consejería de Educación, Juventud y Deporte de la CAM. Programa de Actividad de I+D entre Grupos de Investigación de la CAM. S2013/ICE-2919. Fechas: 2014-2017. Investigador principal solicitante del grupo UAH. Cuantía total de la subvención: 569.250 €
- EDUCERE - Desarrollo de juguetes inteligentes para atención temprana a niños con trastornos del desarrollo en el entorno educativo y en el hogar digital. MINECO TIN2013-47803-C2-2-R. Fechas: 2014-2016. Investigador principal del grupo UAH. Cuantía de la subvención a la UAH: 54.450 €
- Social Internet of Things Apps by and for the Crowd (SITAC). PROYECTO ITEA-2, FINANCIADO POR EL MINECO-Programa INNPACTO. IPT-2012-0839-430000. Fechas: 7/2012-12/2015. Investigador (Investigador Principal: Ivan Marsá Maestre). Cuantía de la subvención a la UAH: 167.246 €
- MEDIANET - Integración de Servicios Multimedia de Siguiente Generación en la Internet del Futuro. Direccion General de Universidades e Investigación. (Consejería de Educación de la CAM). Programa de Actividad de I+D entre Grupos de Investigación de la CAM. S2009/TIC-1468. Fechas: 2010-1013. Investigador principal del grupo UAH. Cuantía de la subvención a la UAH: 190,062.28 €
- DiYSE -Do It Yourself Smart Experiences. PROYECTO ITEA, Financiado por MITYC - TSI-020400-2009-124. Fechas: 6/2009-12/2009. Investigador Principal del Grupo UAH. Cuantía de la subvención: 81.239€. No se obtuvo subvencion para los dos años siguientes por un error en la solicitud por parte del socio principal Español, ATOS Origin.

C.3. Contratos

- Cátedra de Autonomía Personal Telefónica-Universidad de Alcalá, financiada por TELEFONICA con 170.000€ entre 2010 y 2014. Codirector de la Cátedra de Invesitgación.
- Evaluación de Tecnologías en el Ámbito de la Gestión de Crisis. Financiado por Dynamic Conculting International Telecommunications Spain, S.L. con 9.758€ entre 10/2008 y 12/2008. Investigador principal.
- Desarrollo de una herramienta para la generación de interfaces. Financiado por Dynamic Conculting International Telecommunications Spain, S.L. con 70,000 € entre 10/2008 y 12/2008. Investigador principal.
- SATI-TDT. Asistencia técnica referente al desarrollo de aplicaciones interactivas de TV con tarjetas smartcard y lenguaje Java. Financiado por Informática en Corte

Inglés con 63.800 entre 01/2007 y 12/2007. Investigador (Investigador principal: Sebastián Sánchez Prieto)

- SECUR – Custodia de cintas basado en RFID – Parte II, financiado por BSCM, S.L con 15.000€ entre 07/2007 y 06/2008. Investigador principal
- Biometría y sistema inteligente de control de seguridad integral sobre protocolo TCP/IP. Financiado por Intelligent Data, S. L. Con 26.000€ entre 01/2007 y 12/2008. Investigador Principal
- Plataforma integral de seguridad e identificación en entorno cliente servidor sobre Internet. Financiado por Intelligent Data, S. L. Con 10.000€ entre 01/2007 y 12/2008. Investigador Principal

C.4. Patentes

- JR. Velasco y 28 investigadores más. N. de solicitud: P201600945. TABLERO DE CLAVIJAS MULTIACTIVIDAD MONITORIZADO. Fecha de concesión: 22/02/2019. U. de Alcalá U. Politécnica de Madrid, U. Autónoma de Madrid
- JR. Velasco y 28 investigadores más. N. de solicitud: P201600597. SISTEMA DE SONDAS INTELIGENTES DE MONITORIZACIÓN APLICADO A OBJETOS DE USO COTIDIANO. Fecha de concesión: 28/03/2019. U. de Alcalá U. Politécnica de Madrid, U. Autónoma de Madrid.
- Inventores (p.o. de firma): Ivan Marsá Maestre, Juan R. Velasco, Victor Brea Luján, Miguel A. Lopez-Carmona, Enrique de la Hoz de la Hoz, Antonio J. De Vicente Rodriguez, Bernardo Alarcos Alcazar. N. de solicitud: P201131275. MARCO DIGITAL MULTIMEDIA PERSONALIZABLE POR MEDIO DE IDENTIFICACIÓN DE USUARIOS. Fecha de concesión: 1/10/2014. Universidad de Alcalá.

C.5 Actividades de Gestión Científica y Académica

- Vicerrector de Estrategia y Planificación de la Universidad de Alcalá – marzo de 2018 hasta la fecha
- Vicerrector de Posgrado y Educación Permanente de la Universidad de Alcala – marzo de 2010 a marzo de 2018
- Director del Grupo de Investigación en Ingeniería de Servicios Telemáticos de la Universidad de Alcalá, registrado con el número CCTT2006/F45 desde su creación hasta la actualidad.
- Inspector adjunto en la Inspección de Servicios de la Universidad de Alcalá desde el 1 de abril de 2008 hasta el 23 de marzo de 2010
- Coordinador del Área de Tecnología Electrónica y Comunicaciones. Becas de FPU, Subdirección General de Formación y Movilidad en Posgrado y Posdoctorado del Ministerio de Ciencia e Innovación. Años 2006 y 2007
- Subdirector de la Escuela Politécnica Superior de la Universidad de Alcalá desde el 28 de abril de 2004 hasta el 31 de marzo de 2008
- Gestor de fondos FEDER para infraestructura científica en el área de comunicaciones. Subdirección General de Coordinación Institucional e Infraestructura Científica del Ministerio de Ciencia y TecnologíaDesde el 1 de abril de 2003 hasta el 30 de diciembre de 2005

C.6 Premios

- En 2009 le fue concedido el premio en la III Edición de los Premios Vodafone a la Innovación en Comunicaciones Móviles que otorga la Fundación Vodafone con el proyecto denominado “ANEGSYS Mobile: Sistema de negociación automática para preventa en ferias comerciales”, desarrollado por Miguel Ángel López Carmona, Juan Ramón Velasco Pérez, Iván Marsá Maestre y Javier de la Red Sánchez.

Fecha del CVA	03-07-2021

Parte A. DATOS PERSONALES

Nombre y apellidos	Juan Rafael Sendra Pons		
DNI/NIE/pasaporte		Edad	
Núm. identificación del investigador	Researcher ID	K-3420-2014	
	Código Orcid	0000-0003-2568-1159	

A.1. Situación profesional actual

Organismo	Universidad de Alcalá		
Dpto./Centro	Dpto. de Física y Matemáticas/ Facultad de Ciencias		
Dirección	Ap. de correos 20, 28871 Alcalá de Henares		
Teléfono		correo electrónico	Rafael.sendra@uah.es
Categoría profesional	Catedrático de Universidad	Fecha inicio	25/11/2002
Espec. cód. UNESCO	120101, 120113		
Palabras clave	Cálculo simbólico, algoritmos efectivos, curvas y superficies algebraicas, diseño asistido por ordenador		

A.2. Formación académica *(título, institución, fecha)*

Licenciatura/Grado/Doctorado	Universidad	Año
Licenciatura Matemáticas	Universidad Complutense de Madrid	1985
Doctorado en Matemáticas	Universidad de Alcalá	1990

A.3. Indicadores generales de calidad de la producción científica

Indicadores de calidad:
N. de sexenios: 5
Fecha del último concedido: 31/12/2016
Citas totales (Google Scholar): 2496
h-index (Google Scholar): 28

Identificadores
ResearcherID: K-3420-2014
Scopus Author ID: 7006497283
ORCID: 0000-0003-2568-1159

Parte B. RESUMEN LIBRE DEL CURRÍCULUM *(máximo 3500 caracteres, incluyendo espacios en blanco)*

Juan Rafael Sendra Pons se licenció en Ciencias Matemáticas en 1985 en la Universidad Complutense de Madrid y se doctoró en 1990, bajo la dirección del profesor J. Llovet Verdugo, en el departamento de Matemáticas de Universidad de Alcalá con una tesis sobre cálculo simbólico en anillos polinomiales; el contenido de la tesis se publicó en 6 trabajos, 3 de ellos en revistas indexadas JCR y el resto como capítulos de libro. La tesis recibió el premio extraordinario de doctorado. Previamente realizó una estancia de investigación de 1 año en RISC-LINZ (Research Institute for Symbolic Computation) de la Univ. Johannes Kepler de Linz, Austria, con los profesores Bruno Buchberger (creador de las bases de Gröbner) y Franz Winkler. Como resultado de esta estancia se arrancó un nuevo frente de trabajo (cálculo efectivo en geometría algebraica) paralelo al mencionado en la tesis, pero ubicado en el mismo campo temático, que ha conducido a numerosos artículos así como a la publicación del libro, de carácter científico, [*J.R. Sendra, F. Winkler, S. Perez-Diaz. Rational Algebraic Curves: A Computer Algebra Approach. Series: Algorithms and Computation in Mathematics , Vol. 22. Springer Verlag 2007* (289 según Google Scholar)]. Obsérvese que este es uno de los ámbitos de trabajo es en el que enmarca el proyecto solicitado.

La investigación del profesor Sendra se desarrolla en el lugar de encuentro del álgebra, la geometría, las ecuaciones diferenciales, la algoritmia, tanto simbólica como híbrido simbólico-numérica, y las aplicaciones de la matemática. Dicha actividad se puede estructurar en las siguientes líneas interrelacionadas de trabajo. En 1990, arrancó su línea troncal de trabajo **(L1)** centrada en el álgebra

y la geometría algebraica constructiva. En 1997, con su primer trabajo sobre variedades offset, comenzó una segunda línea **(L2)** dedicada a la aplicación de la geometría algebraica simbólica al diseño geométrico asistido por ordenador. Por otra parte, en 2010, comenzó a trabajar en el estudio y resolución de ecuaciones diferenciales mediante técnicas algebro-geométricas y en la utilización del álgebra simbólica en la manipulación de seudo-inversas y matrices bohemias **(L3).** Aunque, la línea L2 tiene una componente alta de aplicabilidad, es en 2011 cuando aparecen las primeras contribuciones aplicadas a otros campos. Así, mediante la colaboración con el profesor L. Álvarez León, y más tarde con el profesor M. Beltrametti, consiguió sus primeros resultados en visión artificial y en detección de imágenes mediante la transformada de Hough **(L4)**; cabe también señalar la colaboración científica en temas del campo de la ingeniería.

L1 abarca la aplicabilidad simbólica de matrices en teoría de la eliminación, los trabajos en álgebra tropical y más concretamente en la caracterización, vía resultantes, del número de raíces comunes de dos polinomios tropicales, así como el desarrollo de algoritmos para la manipulación de curvas y superficies algebraicas. Posiblemente, la aportación más relevante en esta línea es la resolución del problema de la optimalidad algebraica de curvas, en su versión implícita, mediante la generalización del teorema de Hilbert Hurwitz para curvas adjuntas que se publicó en [R Sendra. F. Winkler. Parametrization of Algebraic Curves over Optimal Field Extensions. Journal of Symbolic Computation 23/2,3, 191-207 (1997)]. Indicar que 2010, en trabajo conjunto con T. Recio,L.F. Tabera, C. Villarino, resuelve la versión paramétrica del mismo problema, en este caso mediante la generalización del método de descenso de Weil. Asimismo, en esta línea se abordan los problemas de suprayectividad, inyectividad, radicalidad y optimalidad aritmética de variedades algebraicas. Esta línea ha tenido una productividad de 37 artículos (31 JCR), 16 capítulos de libros, 1 libro y 5 ediciones, con más de 1400 citas.

En L2, ha trabajado con variedades offset, concoidales, bisectores, etc. Como resultado destable cabe mencionar entre otros la caracterización de la unirracionalidad de hipersuperficies offset, la introducción del concepto de degeneración fuerte y débil y la obtención de la fórmula del género de curvas offsets. Señalar asimismo que, como consecuencia de las cuestiones emergentes en esta línea, inició el tratamiento simbólico-numérico de objetos geométricos. Esta línea ha tenido una productividad de 29 artículos (25 JCR) y 5 capítulos de libros, con más de 618 citas

En L3, ha investigado en la determinación simbólica de soluciones de ecuaciones diferenciales mediante el estudio de la variedad algebraica subyacente. Así, se ha analizado el caso de soluciones racionales, radicales y mediante series de Puiseux. Por otra parte, en esta línea se ha abordado también la manipulación de inversas generalizadas y de matrices bohemias. En este sentido cabe destacar, pues abre un camino de generalización en la metodología de trabajo, el artículo [A5] (véase sección 3), publicado en 2017. En este trabajo se investiga sobre la inversa de Moore-Penrose en cuerpos con un automofismo involutivo, se introduce el concepto de cuerpo de Moore-Penrose y se desarrollan las bases para el cálculo de inversas con funcionales meromorfas. Esta línea ha tenido una productividad de 14 artículos (12 JCR), 5 capítulos de libros y 1 edición, con más de 120 citas

En L4, ha trabajado en la aplicación de técnicas algebraicas en visión artificial y en detección de imágenes. En el artículo [A4] (veáse sección 3), con 83 citas, como las técnicas algebraicas de teoría de la eliminación permites diseñar modelos algebraicos para la modelización del fenómeno de la distorsión radial en imágenes. Por otro parte, ha generalizado la aplicabilidad de la transformada de Hough al caso de curvas algebraicas planas y de superficies, mostrado su utilidad en imágenes médicas. Esta línea ha tenido una productividad de 7 artículos (6 JCR), con más de 150 citas.

El profesor Sendra ha publicado con diversos investigadores nacionales (E. Arrondo, T. Recio, L. González-Vega, F. Castro, L. Álvarez, L. F. Tabera, J. Cano, C. Andradas, etc) y extranjeros (R. Corless, I. Emiris, H. Hong, M. Nnuk, M. Peternel, C. Ngo, J. Schicho, F. Winkler, S.Winkler, P.

Stanimirovic, D. Wang, etc) y ha colaborado con grupos de diversos países (España, Austria, Alemania, Serbia, Italia, Grecia, Canadá, USA, China, Vietnam, Corea del sur).

Asimismo, ha participado en múltiples actividades de organización, evaluación y gestión de la investigación entre las que cabe destacar su labor editorial, dirección de proyectos y de tesis doctoral, pertenencia a paneles de evaluación, etc.

Parte C. MÉRITOS MÁS RELEVANTES

C.1. Publicaciones

[1] P. S. Stanimirovic, J.R. Sendra R. Behera, J. K. Sahoo,D. Mosic, J. Sendra, A.Lastra. Computing tensor generalized inverses via specialization and rationalization. Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas (2021) 115:116 pp.1-16 https://doi.org/10.1007/s13398-021-01057-9

[2] P- S. Stanimirovic, J.R. Sendra, M. Ciric, A. Lastra, J.Sendra. Representations and symbolic computation of generalized inverses over fields with Applied Mathematics and Computation 406 (2021) 126287 https://doi.org/10.1016/j.amc.2021.126287

[3] J. Caravantes, J.R.Sendra. D. Sevilla, C. Villarino..Transforming ODEs and PDEs from radical coefficients to rational coefficients. Mediterranean Journal of Mathematics (2021) 18:96

[4] M.C. Beltrametti, J.R. Sendra J. Sendra, L.M. Torrente. Moore-Penrose approach in the Hough transform framework. Applied Mathematics and Computation 375 (2020) 125083

[5] E. Y. S. Chan, R. M. Corless, L. Gonzalez-Vega, J.R. Sendra, J. Sendra. Algebraic Linearizations of Matrix Polynomials. Linear Algebra and its Applications 563 (2019) 373-399.

[6] M- C. Beltrametti, J.R. Sendra L.M. Torrente.r-norm bounds and metric properties for zero loci of real analytic functions. Journal of Computational and Applied Mathematics 336 (2018) 375-393

[7] Sendra J.R., Sendra J. (2016), "Symbolic computation of Drazin inverses by specializations". Journal of Computational and Applied Mathematics 301 (2016) 201-212.

[8] Sendra J.R., Sendra J (2017), "Computation of Moore-Penrose Generalized Inverses of Matrices with Meromorphic Function Entries". Applied Mathematics and Computation 313C (2017) pp. 355-366.

[9] Sendra J.R., Sevilla D., Villarino C. (2015). " Missing sets in rational parametrizations of surfaces of revolution". Computer-Aided Design 66 (2015) 55--61.

[10] Sendra J.R., Sevilla D., Villarino C. "Covering Rational Ruled Surfaces". Mathematics of Computation Volume 86, Number 308, November 2017, Pages 2861–2875

[11] Sendra J.R., Sevilla D., Villarino C. "Algebraic and algorithmic aspects of radical parametrizations." Computer Aided Geometric Design 55 1-14. (2017)

[12] Sendra J.R., Winkler St. (2016). "A Heuristic and Evolutionary Algorithm to Optimize the Coefficients of Curve Parametrizations." Journal of Computational and Applied Mathematics 305 (2016) 18--35.

[13] Rueda S., Sendra J., Sendra J.R. "Rational Hausdorff Divisors: a New approach to the Approximate Parametrization of Curves" Journal of Computational and Applied Mathematics 263C (2014), pp. 445-465

[14] Sendra J.R., Sevilla D. First Steps Towards Radical Parametrization of Algebraic Surfaces. Computer Aided Geometric Design Volume 30, Issue 4, pp. 374-388 (2013).

[15] T.Recio, J.R. Sendra L.F. Tabera C. Villarino. Generalizing circles over algebraic extensions. Mathematics of Computation vol. 79, num. 270, pp. 1067-1089 (2010).

[16] J.R. Sendra, F. Winkler, S. Perez-Diaz. Rational Algebraic Curves: A Computer Algebra Approach. Series: Algorithms and Computation in Mathematics , Vol. 22. Springer Verlag (2007) ISBN 978-3-540-73725-4v

C.2. Proyectos

[1] Título del Proyecto: COMPUTACION SIMBOLICA: NUEVOS RETOS EN ALGEBRA Y GEOMETRIA Y SUS APLICACIONES
Entidad financiadora: Ministerio de Economía y Competitividad MTM2017-88796-P.
Duración: 2018-2019-2020
Investigador responsable: Laureano González-Vega
[2] Título del proyecto: CONSTRUCCIONES ALGEBRO-GEOMETRICAS: FUNDAMENTOS, ALGORITMOS Y APLICACIONES. http://www3.uah.es/cag_faa/indexcag_faa_es.html#
Entidad financiadora: **M**inisterio de Economía y Competitividad MTM2014-54141-P
Duración: 2015-2016-2017
Investigador responsable: L. González Vega
[3] Título del proyecto: CONSTRUCCIONES ALGEBRO-GEOMETRICAS: FUNDAMENTOS, ALGORITMOS Y APLICACIONES. http://www3.uah.es/cag_faa/indexcag_faa_es.html#
Entidad financiadora: **M**inisterio de Economía y Competitividad MTM2014-54141-**Duración:** 2015-2016-2017
Investigador responsable: L. González Vega
[4] Título del proyecto: Algoritmos y Aplicaciones en Geometría de Curvas y Superficies. http://www2.uah.es/aayag
Entidad financiadora: Ministerio de Ciencia e Innovación (MTM2011-25816-C02-00)
Entidades participantes: Universidades de Alcalá y Cantabria (Proyecto coordinado)
Duración: 2012-2013-2014 **Financiación:** 58443 euros
Investigador responsable: J. RAFAEL SENDRA
Coordinador general: J. RAFAEL SENDRA
[5] Título del proyecto: Variedades Paramétricas: algoritmos y aplicaciones
Entidad financiadora: Ministerio de Ciencia e Innovación (MTM2008-04699-C03-01)
Entidades participantes: Universidades de Alcalá y Cantabria (Proyecto coordinado)
Duración: 2009-2010-2011 **Financiación:** 73689 euros
Investigador responsable: J. RAFAEL SENDRA
Coordinador general: J. RAFAEL SENDRA
[6] Título del proyecto: Curvas y superficies: computación híbrida y aplicaciones
Entidad financiadora: Comunidad Autónoma de Madrid, Universidad de Alcalá (CAMUAH2005/053)
Entidades participantes: Universidad de Alcalá
Duración: 2006 **Financiación:** 10500 euros
Investigador responsable: J. RAFAEL SENDRA
[7] Título del proyecto: Resolución Simbólico Numérica de Problemas para Curvas y Superficies Reales
Entidad financiadora: Ministerio de Educación y Ciencia (MTM2005-08690-C02-01)
Entidades participantes: Universidades de Alcalá y Cantabria (Proyecto coordinado)
Duración 2006-2007-2008 **Financiación:** 72847 euros
Investigador responsable: J. RAFAEL SENDRA
Coordinador general: J. RAFAEL SENDRA
[8] Título del proyecto: Curvas y superficies: fundamentos, algoritmos y aplicaciones
Entidad financiadora:MINISTERIO DE CIENCIA Y TECNOLOGIA.BFM2002-04402-C02-01
Entidades participantes: Universidades de Alcalá y Cantabria (Proyecto coordinado)
Duración 2003-2004-2005 **Financiación:** 35600 euros
Investigador responsable: J. RAFAEL SENDRA
Coordinador general: J. RAFAEL SENDRA
[9] Título del proyecto: DISEÑO GEOMETRICO ASISTIDO POR ORDENADOR MEDIANTE METODOS SIMBOLICO NUMERICOS
Entidad financiadora: MINISTERIO DE ASUNTOS EXTERIORES. HU2001-0002
Entidades participantes: Universidad de Alcalá, Johannes Kepler Universität (Austria)
Duración: 2003-2004 **Financiación:** 8714,68 euros
Investigador responsable: J.Rafael Sendra
[10] Título del proyecto: METODOS ALGEBRAICOS-GEOMETRICOS PARA LA MANIPULACION DE CURVAS Y SUPERFICIES
Entidad financiadora: MINISTERIO DE EDUACION Y CIENCIA. PB98-0713-C02-01

Entidades participantes: Universidades de Alcalá y Cantabria (Proyecto Coordinado)
Duración: 1999-2000-2001 **Financiación:** 2.000.000pts
Investigador responsable: J. RAFAEL SENDRA
Coordinador general: J. RAFAEL SENDRA

C.5 Dirección de tesis doctorales

[1] Título: Power Series Solutions of AODEs: Existence, Uniqueness, Convergence and Computation.
Doctorando: Sebastian Falkensteiner. **Universidad:** Johannes Kepler Universität Linz, Austra
Fecha: Junio/2020
Codirigida con F. Winkler
[2] Título: Effective Algorithms for the Study of the Degree of Algebraic Varieties in Offsetting Processes
Doctorando: Fernando San Segundo Barahona. **Universidad:** UNIV. DE ALCALA
Fecha: Febrero/2010
[3] Título: Effective Algorithms for the Study of the Topology of Algebraic Varieties, and Applications (recibió premio extraordinario de doctorado)
Doctorando: Juan Gerardo Alcazar Arribas. **Universidad:** UNIV. DE ALCALA.
Fecha: marzo/2007
[4] Título: Algoritmos de Optimalidad Algebraica y de Cuasi-Polinomialidad para Curvas Racionales
Doctorando: Carlos Villarino Cabellos. **Universidad:** UNIV. DE ALCALA.
Fecha: mayo/2007
[5] Título: Parametric varieties: algorithms and applications to geometric blending. (recibió premio extraordinario de doctorado)
Doctorando: SONIA PEREZ DIAZ. **Universidad:** UNIV. DE ALCALA
Fecha: 15/09/2003
[6] Título: Effective algorithms for the manipulations of offsets to hypersurfaces.
Doctorando: JUANA SENDRA. **Universidad:** UNIVERSIDAD POLITÉCNICA DE MADRID
Fecha: 29/10/1999

C.6 Pertenencia comités editoriales revistas científicas internacionales

Miembro del equipo editorial de la revista *Journal of symbolic computation* (http://www.journals.elsevier.com/journal-of-symbolic-computation/) desde 2002

C.7 Organización de eventos científicos internacionales

[1] EVENTO: Special Session on "Algebraic Geometry in Applications and Algorithms" at the Conference "First Joint International Meeting RSME-SCM-SEMA-SIMAI-UMI". **PUESTO:** Organizador. **Fecha:** julio 2014. **Lugar:** Bilbao (http://www.ehu.es/en/web/fjim2014)
[2] EVENTO: ACM International Symposium on Symbolic and Algebraic Computation (2008). **PUESTO:** General Chair. **Fecha:** julio 2008. **Lugar:** RISC-LINZ, Austria. (http://www.risc.jku.at/conferences/issac2008/
[3] EVENTO: Workshop on Computer Algebra in Geometric Modeling and Industry
PUESTO: Miembro del Comité Científico y Organizador. **Fecha:** 17-21-Diciembre 2007.**Lugar**: Centro Internacional de Encuentros Matematicos, Castro Urdiales. (http://www.ciem.unican.es/workshop-computer-algebra-geometric-modeling-and-industry)
[4] EVENTO: ACM International Symposium on Symbolic and Algebraic Computation (2007). **PUESTO:** TUTORIAL CHAIR. **Fecha:** julio-2007. **Lugar:** Waterloo, Canada. (https://cs.uwaterloo.ca/conferences/issac2007/

Parte A

Fecha del CVA	05/07/2021

Nombre y apellidos	María de los Ángeles Hernández Cifre

A.1. Situación profesional actual

Organismo	Universidad de Murcia			
Dpto./Centro	Departamento de Matemáticas/Facultad de Matemáticas			
Dirección	Campus de Espinardo, 30100 Murcia			
Teléfono	868887661	correo electrónico	mhcifre@um.es	
Categoría profesional	Catedrático de Universidad		Fecha inicio	13/10/2018
Espec. cód. UNESCO	120403, 120505, 120206			
Palabras clave	Teoría de Brunn-Minkowski, convexidad, desigualdades funcionales y geométricas, geometría de números, geometría discreta			

A.2. Formación académica

Licenciatura/Grado/Doctorado	Universidad	Año
Licenciado en Matemáticas	Universidad de Murcia	1995
Doctor en Matemáticas	Universidad de Murcia	1998

A.3. Indicadores generales de calidad de la producción científica

- 4 sexenios de investigación otorgados por la CNEAI (1997/2002, 2003/2008, 2009/2014, 2015/2020; fecha del último: 31 de mayo de 2021).
- 5 tesis doctorales dirigidas en los últimos 10 años; una sexta se defenderá en septiembre de 2022.
- 60 artículos de investigación, 3 capítulos de libro, 2 libros y editor de 2 proceedings.
- Índice h=9.

Parte B. RESUMEN LIBRE DEL CURRÍCULUM

Parte C. MÉRITOS MÁS RELEVANTES

C.1. Publicaciones *(últimos 10 años)*

1. M. A. Hernández Cifre, E. Saorín: Isoperimetric relations for inner parallel bodies. To appear in Commun. Anal. Geom.
2. D. Alonso Gutiérrez, M. A. Hernández Cifre, M. Roysdon, J. Yepes Nicolás, A. Zvavitch: On Rogers-Shephard type inequalities for general measures. To appear in Int. Math. Res. Not. IMRN.
3. M. A. Hernández Cifre, M. Tárraga: On the (dual) Blaschke diagram. To appear in Bull. Braz. Math. Soc. New Series.
4. D. Alonso-Gutiérrez, M. A. Hernández Cifre, J. Yepes Nicolás: Further inequalities for the (generalized) Wills functional. To appear in Commun. Contemp. Math.
5. D. Alonso-Gutiérrez, M. A. Hernández Cifre, M. Roysdon, J. Yepes Nicolás, A. Zvavitch: On Rogers-Shephard type inequalities for general. To appear in Int. Math. Res. Not. IMRN.
6. D. Alonso-Gutiérrez, M. A. Hernández Cifre, M. Henk: A characterization of dual querma-ssintegrals and the roots of dual Steiner polynomials. Adv. Math. 331 (2018), 565-588.
7. D. Iglesias, M. A. Hernández Cifre, J. Yepes Nicolás: On a discrete Brunn-Minkowski type inequality. SIAM J. Discrete Math. 32 (2018), 1840-1856.
8. J. Abardia-Evéquoz, M. A. Hernández Cifre, E. Saorín: Mean projection and section radii of convex bodies. Acta Math. Hung. 155 (2018), 89-103.
9. D. Alonso-Gutiérrez, M. A. Hernández Cifre: Estimates for the integrals of powered i-th mean curvatures. In: Bianchi G., Colesanti A., Gronchi P. (eds), Analytic Aspects of Convexity. Springer INdAM Series, vol 25. Cham, Springer, 2018. pp. 19-37.
10. D. Alonso-Gutiérrez, M. A. Hernández Cifre, A. R. Martínez Fernández: Bounding the integral of powered i-th mean curvatures. Rev. Mat. Iberoam. 33 (4) (2017), 1197-1218.
11. M. A. Hernández Cifre, J. Yepes Nicolás: Brunn-Minkowski and Prékopa-Leindler's inequalities under projection assumptions. J. Math. Anal. Appl. 455 (2017), 1257-1271.

12. M. A. Hernández Cifre, A. R. Martínez Fernández, E. Saorín: Differentiability properties of the family of p-parallel bodies. Appl. Anal. Discr. Math. 10 (2016), 186-207.
13. M. Henk, M. Henze, M. A. Hernández Cifre: Variations of Minkowski's theorem on successive minima. Forum Math. 28 (2) (2016), 311-325.
14. M. A. Hernández Cifre, J. Yepes Nicolás: On Brunn-Minkowski type inequalities for polar bodies. J. Geom. Anal. 26 (2016), 143-155.
15. M. A. Hernández Cifre, A. R. Martínez Fernández: The isodiametric problem and other inequalities in the constant curvature 2-spaces. RACSAM 109 (2015), 315-325.
16. M. A. Hernández Cifre, J. Yepes Nicolás: On the roots of generalized Wills mu-polynomials. Rev. Mat. Iberoamericana 31 (2) (2015), 477-496.
17. B. González, M. A. Hernández Cifre, A. Hinrichs: Successive radii of families of convex bodies. Bull. Austral. Math. Soc. 91 (2015), 331-344.
18. D. Alonso-Gutiérrez, N. Dafnis, M. A. Hernández Cifre, J. Prochno: On mean outer radii of random polytopes. Indiana U. Math. J. 63 (2) (2014), 579-595.
19. M. A. Hernández Cifre, J. Yepes Nicolás: Refinements of the Brunn-Minkowski inequality. J. Convex Anal. 21 (3) (2014), 1-17.
20. M. A. Hernández Cifre, E. Saorín: Differentiability of quermassintegrals: a classification of convex bodies. Trans. Amer. Math. Soc. 366 (2014), 591-609.
21. B. González, M. A. Hernández Cifre: On successive radii and p-sums of convex bodies. Adv. Geom. 14 (1) (2014), 117-128.
22. M. A. Hernández Cifre, J. Yepes Nicolás: On the roots of the Wills functional. J. Math. Anal. Appl. 401 (2013), 733-742.
23. M. Henk, M. A. Hernández Cifre, E. Saorín: Steiner polynomials via ultra-logconcave sequences. Commun. Contemp. Math. 14 (6) (2012), 1-16.
24. B. González, M. A. Hernández Cifre: Successive radii and Minkowski addition. Monatsh. Math. 166 (2012), 395-409.
25. M. Henk, M. A. Hernández Cifre: Coverings and compressed lattices. Symmetry Cult. Sci. 22 (3-4) (2011), 307-316.
26. M. Henk, M. A. Hernández Cifre: On the location of roots of Steiner polynomials. Bull. Braz. Math. Soc. 42 (1) (2011), 153-170.
27. M. A. Hernández Cifre, E. Saorín: On inner parallel bodies and quermassintegrals. Israel J. Math. 177 (2010), 29-47.
28. M. A. Hernández Cifre, E. Saorín: On the volume of inner parallel bodies. Adv. Geom. 10 (2) (2010), 275-286.
29. M. A. Hernández Cifre, E. Saorín: On differentiability of quermassintegrals. Forum Math. 22 (1) (2010), 115-126.

C.2. Proyectos *(últimos 10 años)*

1. Referencia: **PGC2018-097046-B-I00**
   Título: Análisis Global en Geometría Diferencial y Convexa.
   Entidad financiadora: Ministerio de Ciencia, Innovación y Universidades.
   Investigador Principal: Luis J. Alías Linares, María A. Hernández Cifre (Univ. de Murcia)
   Fecha: del 01/01/19 al 31/12/21.
   Cuantía: 51.788€. Participación: Segundo investigador principal.
2. Referencia: **MTM2015-65430-P**
   Título: Análisis Global en Geometría Diferencial y Convexa.
   Entidad financiadora: MINECO.
   Investigador Principal: Luis J. Alías Linares (Univ. de Murcia)
   Fecha: del 01/01/16 al 31/12/18.
   Cuantía: 88.600€. Participación: Investigador.
3. Referencia: **19901/GERM/15**
   Título: Global Analysis in Differential and Convex Geometry. Ayudas a los Grupos de Excelencia Científica de la Región de Murcia.
   Entidad financiadora: Fundación Séneca, CARM.
   Investigador Principal: Luis J. Alías Linares, María A. Hernández Cifre (Univ. de Murcia)
   Fecha: del 01/01/16 al 31/12/20.
   Cuantía: 250.000€ (prevista). Participación: Segundo investigador principal.

4. Referencia: **MTM2012-34037**
   Título: Análisis Global en Geometría Diferencial y Convexa.
   Entidad financiadora: MINECO.
   Investigador Principal: Luis J. Alías Linares (Univ. de Murcia)
   Fecha: del 01/01/13 al 31/12/15.
   Cuantía: 123.000€. Participación: Investigador.
5. Referencia: **AIB2010DE-00082**
   Título: Raíces de polinomios de Steiner (Roots of Steiner polynomials).
   Entidad financiadora: MCI, DAAD.
   Investigador Principal: María A. Hernández Cifre (Univ. de Murcia), Martin Henk (Otto-von-Guericke Universität Magdeburg)
   Fecha: del 01/01/11 al 31/12/12.
   Cuantía: 17.966€ (8000€ + 9.966€). Participación: Investigador principal.
6. Referencia: **MTM2009-10418**
   Título: Geometría diferencial y convexa: Problemas variacionales y de optimización.
   Entidad financiadora: MICINN.
   Investigador Principal: Luis J. Alías Linares (Universidad de Murcia)
   Fecha: del 01/01/10 al 31/12/12.
   Cuantía: 174.239,98€. Participación: Investigador.
7. Referencia: **04540/GERM/06**
   Título: Problemas variacionales y de optimización en Geometría Diferencial y Convexa. Ayudas a los Grupos de Excelencia Científica de la Región de Murcia.
   Entidad financiadora: Fundación Séneca, CARM.
   Investigador Principal: Luis J. Alías Linares, Pascual Lucas Saorín (Univ. de Murcia)
   Fecha: del 01/01/08 al 31/07/14.
   Cuantía: 312.000€. Participación: Investigador.

C.3. Contratos, méritos tecnológicos o de transferencia

C.4. Patentes

C.5. Dirección de trabajos *(últimos 10 años)*

1. Título: On roots of general Steiner type polynomials. Doctorando: Miriam Tárraga Navarro. Fecha prevista: noviembre de 2020.
2. Título: On discrete Brunn-Minkowski type inequalities. Doctorando: David Iglesias López. Fecha: 13/12/19. Calificación: Sobresaliente cum Laude. Con mención internacional.
3. Título: Going further in the Lp-Brunn-Minkowski Theory: a p-difference of convex bodies. Doctorando: Antonio Roberto Martínez Fernández. Fecha: 28/01/16. Calificación: Sobresaliente cum Laude. Con mención internacional.
4. Título: From Brunn-Minkowski type inequalities to roots of geometric polynomials. Doctorando: Jesús Yepes Nicolás. Fecha: 17/11/14. Calificación: Sobresaliente cum Laude. Con mención europea.
5. Título: Successive radii of convex bodies. Doctorando: Bernardo González Merino. Fecha: 18/03/13. Calificación: Sobresaliente cum Laude. Con mención europea.

C.6. Estancias en centros extranjeros

1. Lugar: Otto-von-Guericke Universität Magdeburg (Institut für Algebra und Geometrie), Magdeburg, Alemania. Duración: 5 meses (2011-12).
2. Lugar: Otto-von-Guericke Universität Magdeburg (Institut für Algebra und Geometrie), Magdeburg, Alemania. Duración: 4 meses (2008-09).
3. Lugar: Otto-von-Guericke Universität Magdeburg (Institut für Algebra und Geometrie), Magdeburg, Alemania. Duración: 1 año (2006-07).

C.7. Participación en tareas de evaluación

1. Miembro de tribunales de tesis doctorales:
   - S. Rivollier, Ecole Nationale Supérieure des Mines de Saint-Etienne, Julio 2010.
   - Stefan König, Zentrum Mathematik, Technische Universität München, Agosto 2013.
   - Efstratios Vernadakis, Universidad de Granada, Junio 2014.

- Eric Dubon, Universidad de Murcia, Julio 2015.
- S. Rahmani, Ecole Nationale Supérieure des Mines de Saint-Etienne, Julio 2017.
- S. Berg, Technische Universität Berlin, Septiembre 2018.
- F. Xue, Technische Universität Berlin, Septiembre 2019.
- A. Delyon, Ecole Nationale Supérieure des Mines de Saint-Etienne, Noviembre 2020.

2. Miembro del jurado de los premios de investigación matemática Vicent Caselles 2021.
3. Evaluador de la Agencia Nacional de Evaluación y Prospectiva (ANEP), de la Agencia para la Calidad del Sistema Universitario de Castilla y León (ACSUCYL) y de la Agencia Andaluza de Evaluación (AGAE).

C.8. Comités editoriales

Miembro del comité editorial de la revista “Mathematical Inequalities & Applications”. Incluida en el Journal Citation Report list (JCR), área Mathematics, 1er quartil JCR 2019.

C.9. Invitaciones científicas

Invitación a impartir conferencias en centros/congresos de reconocido prestigio internacional: el Mathematisches Forschungsinstitut Oberwolfach (2018, 2015, 2012, 2009, 2006), la Technische Universität Berlin (2015), la Scuola Normale Superiore di Pisa en Cortona (2007, 2011), el Fields Institute de Toronto (2010), la Ecole Nationale Supérieure des Mines de Saint-Etienne (2017, 2010), la Technische Universität Munich (2007), el Banff International Research Station for Mathematical Innovation and Discovery (2006), etc.

C.10. Organización de eventos científicos

Organizador de 16 congresos de investigación, 12 de ellos de carácter internacional.
Miembro del comité científico de 3 congresos de investigación de carácter internacional.

Fecha del CVA	4.06.2021

Parte A. DATOS PERSONALES

Nombre y apellidos	María Isabel González Vasco		
DNI/NIE/pasaporte		Edad	
Núm. identificación del investigador	Researcher ID	D-8445-2016	
	Código Orcid	orcid.org/0000-0002-7452-9121	

A.1. Situación profesional actual

Organismo	Universidad Rey Juan Carlos			
Dpto./Centro	Escuela Superior de Ciencias Experimentales y Tecnología			
Dirección	c/ Tulipán, s/n, 28933, Móstoles			
Teléfono	914887605	correo electrónico	mariaisabel.vasco@urjc.es	
Categoría profesional	Catedrática de Universidad		Fecha inicio	25.03.2021
Espec. cód. UNESCO	1201, 1203			
Palabras clave	Criptografía de Clave Pública, Intercambio de Clave, Cifrado basado en Grupos			

A.2. Formación académica *(título, institución, fecha)*

Licenciatura/Grado/Doctorado	Universidad	Año
Licenciada en Matemáticas	Universidad de Oviedo	1999
Doctora	Universidad de Oviedo	2003

A.3. Indicadores generales de calidad de la producción científica *(véanse instrucciones)*

3 Sexenios de investigación (último, activo, concedido para el tramo 2012-2017). 1 Sexenio de tranferencia.
Google Scholar: 723 citas totales, 224 desde 2016, índice-h 16

27 publicaciones en JCR, seis de ellas en primer cuartil. Dos patentes en explotación. Tres Special Issues de revistas en JCR como editora/co-editora. Una monografía publicada por Taylor y Francis (co autor: R. Steinwandt).

Parte B. RESUMEN LIBRE DEL CURRÍCULUM *(máximo 3500 caracteres, incluyendo espacios en blanco)*

María Isabel González Vasco es licenciada en Matemáticas y doctora por la Universidad de Oviedo (obteniendo en ambos casos el Premio Extraordinario). Desarrolla su labor investigadora en el campo de la Criptografía Matemática desde el año 1999, en el que disfrutó de una estancia de investigación (Programa Leonardo da Vinci) en la empresa Philips Crypto B.V. (Eindhoven, Holanda). En los años siguientes su interés se centró en dos áreas de trabajo; funciones Hard-Core y Criptografía basada en Teoría de Grupos. En el primer campo, alcanzó importantes resultados (en colaboración con investigadores de la talla de Igor E. Spharlinski y M. Näslund) con implicaciones prácticas relativas a la seguridad del esquema de intercambio de clave de Diffie-Hellman. En cuanto a Criptografía basada en Teoría de Grupos, tema que centró su tesis doctoral, criptoanalizó numerosas propuestas para aplicar esta teoría al cifrado de mensajes y al intercambio seguro de claves criptográficas. Dicho trabajo se desarrolló en colaboración con investigadores del Instituto Europeo de Seguridad de Sistemas (IAKS/EISS) de la Universidad de Karlsruhe. Hoy en día es reconocida como una de las mayores expertas en este campo, habiendo publicado en 2015 un monográfico (editado por CRC Press) sobre el tema. Desde 2007 la solicitante se interesa además por la seguridad demostrable de esquemas de intercambio de clave multiusuario, en concreto por la búsqueda de diseños que permitan a un conjunto de usuarios acordar una clave criptográfica segura común comunicándose exclusivamente a través de una red vulnerable.

La solicitante ha publicado más de 50 artículos en revistas y actas de congresos especializados, es miembro del comité editorial de las revistas Journal of Mathematical Cryptology y International Journal of Computer Mathematics: Computer Systems Theory sirve de manera habitual como recensora de revistas de referencia en criptología (Journal of Cryptology, AAECC, Designs Codes and Cryptology, etc.). Participa frecuentemente en

comités de programa de conferencias internacionales (destacando PKC 2008 y 2010, ACISP 2009 y 2011, ICITS 2011, PQCrypto 2018). Ha dirigido distintos proyectos con financiación pública (Un proyecto del programa SPS de la OTAN, un proyecto del Plan Nacional, una Acción Integrada Hispano-Alemana) y privada (Fundación Banco Herrero). Ha participado en varios contratos (Art. 83 L.O.U) con empresas (Innovation for Security, Blue Indigo, BBVA next) en temas relacionados con su investigación). Destaca además su intensa labor divulgativa, habiendo impartido conferencias especializadas en numerosas universidades (U. College London, U. Florencia, INRIA, U. Rennes, Centro de innovación BBVA). Es miembro (vocal) de la Junta de Gobierno de la Real Sociedad Matemática Española, perteneciendo a su Comisión de Publicaciones.
En cuanto a su trayectoria profesional, es profesora titular del área de Matemática Aplicada desde 2009 en la Universidad Rey Juan Carlos, en la que ocupó distintas plazas laborales desde 2003. Ha realizado diversas estancias de investigación en centros de reconocido prestigio (Instituto IAKS de U. Karlsruhe, Florida Atlantic University, Instituto Imdea Software). Es además Affiliate Research Professor de la Florida Atlantic University desde 2015. Su actividad investigadora ha sido reconocida con tres sexenios CNAI.

Parte C. MÉRITOS MÁS RELEVANTES *(ordenados por tipología)*
C.1. Publicaciones

1. **M.I. González Vasco**, A.L. Pérez del Pozo, C. Soriente. A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols . IEEE Transactions on Dependable and Secure Computing, Volume 18, Issue 3, 2021.
2. C.González, **M.I. González Vasco**, F. Johnson, A.L. Pérez del Pozo. An Attack on Zawadzki's Quantum Authentication Scheme. Entropy, 23(4), 38, 2021.
3. A.I. González Tablas, **M.I. González Vasco**, I. Cascos. A. Planet Palomino. Shuffle, Cut, and Learn: Crypto Go, a Card Game for Teaching Cryptography Mathematics, 8.,(11), 1993, 2020.
4. Escribano Pablos, **M.I. González Vasco**, J.I., M.I.; Marriaga, M.E.; Pérez del Pozo, Á.L. Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber. Mathematics, 8, 1853, 2020.

5. **M.I. González Vasco**, A. Pérez del Pozo, R. Steinwandt. Group Key Establishment in a Quantum-Future Scenario. Informatica, Vol 31, 4, pp. 751-768, 2020.

6. J.-M. Bohli, **M.I. González Vasco**, R. Steinwandt. Building Group Key Establishment on Group Theory: A Modular Approach. Symmetry, 12(2), 197, 2020**.**

7. **M.I. González Vasco**, José Ignacio Escribano Pablos, Misael Enrique Marriaga and Ángel Luis Pérez del Pozo. *The Cracking of WalnutDSA: A Survey*, Symmetry 2019, 11(9), 1072.
8. **M.I. González Vasco**, J.M. Bohli and 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.
9. **M.I. González Vasco**, A.L. Pérez del Pozo and C. Soriente. *A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols* . IEEE Transactions on Dependable and Secure Computing, to appear.
10. **M.I. González Vasco**, E.P. Fernández-Manzano. *Analytic Surveillance: Big Data Business Models in the Time of Privacy Awareness.* El Profesional de la Información (EPI), Vol 27, núm 2, 2018.
11. **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.
12. 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
13. D. Fiore, **M.I. González Vasco** C. Soriente. *Partitioned Group Password-Based*

Authenticated Key Exchange. The Computer Journal, Vol 60, No. 12, pp.1912-1922, 2017.
14. **M.I. González Vasco**, F. Hess, R. Steinwandt. *Combined schemes for signature and encryption: the public-key and the identity-based setting*. Information and Computation, 246. pp. 1-10, 2016.
15. **M.I. González Vasco**, R. Steinwandt. *Group Theoretic Cryptography*, ISBN 978-1-58488-836-9. Editorial Chapman & Hall/CRC Press, pp. 1—230, 2015.

C.2. Proyectos

Título del proyecto: Seguridad demostrable: validación de herramientas criptográficas a través del álgebra y la matemática 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

Título del proyecto:"CArSD: Criptografía avanzada para afrontar nuevos retos de la sociedad digital" (MTM2016-77213-R.)
Entidad financiadora: MINECO (convocatoria RETOS)
Fechas iniciales: 01/01/2017 – 30/12/2019 (prorrogado hasta 30/09/2020);
Inv. Principal: Javier Herranz (UPC). Subvención: 84.337 €;
Participación: miembro del equipo investigador

Título del proyecto: ABC gates for Europe (ABC4EU)
Entidad financiadora: Comisión Europea. VII Programa Marco
Duración, desde: 01/01/2014 hasta:30/06/2017
Cuantía de la subvención: 666522,88 € (URJC), 12.015.246,04 (Total proyecto)
Investigador responsable: Cristina Conde Vilda (URJC), Entidad: URJC
Participación: Investigador.

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) M.I. González Vasco
Número de investigadores participantes: 4 (equipo español)

C.3. Contratos, méritos tecnológicos o de transferencia

1. (Art. 83) 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

2. (Art. 83) 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

3. (Art. 83) 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. (Art. 83) 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. (PATENTE) 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
País de prioridad: E.E.U.U.
Fecha: Junio 2018 (contrato de cesión)
Entidad titular: NEC Laboratories Europe
Rendimiento inicial: URJC vende su participación a NEC Laboratories por 2750€.

6. (PATENTE) Inventores (p.o. de firma): Antonio 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: Marzo 2020 (contrato de cesión)
Entidad titular: NEC Laboratories Europe
Rendimiento inicial: URJC vende su participación a NEC Laboratories por 1700€.

C.5. Gestión de la Actividad Científica
Título: Comisión de selección del Área de Gestión de Matemáticas (MTM), Programa Nacional de Proyectos de Investigación Fundamental.
Tipo de actividad: Miembro de la comisión de evaluación/selección de proyectos financiables a través del Plan Nacional de I+D+I, Ministerio de Ciencia e Innovación de España.
Fecha: 2011

C.6. Actividad Editorial
Miembro del Editorial Board, Journal of Mathematical Cryptology, Ed. Walter de Gruyter, desde 2008, International Journal of Computer Mathematics: Computer Systems Theory, desde 2019.

Co-Editora de dos Special Issues:
- *Applications of Algebra to Cryptography*, Discrete Applied Mathematics, 2008.
- *Interactions between Group Theory,* Symmetry and Cryptology, Symmetry, 2019.

C.7. Otras actividades de formación/difusión científica

Miembro del Comité Coordinador de la Red Española Matemáticas para la Seguridad de la Información (MatSi), de Noviembre 2006 – Noviembre 2009. Miembro del comité organizador de las escuelas: International School on Mathematical Cryptology 2008, Summer School on Provable Security, (ambas en Barcelona, septiembre 2008, sept 2009). Es miembro (vocal) de la Junta de Gobierno de la Real Sociedad Matemática Española desde 2017, perteneciendo a su Comisión de Publicaciones desde 2019. Miembro del comité de programa de numerosos congresos internacionales, resaltando PKC 2008 y 2010, ACISP 2009 y 2011, ICITS 2011, PQCrypto 2018.
