Fecha del CVA	25/05/21

Parte A. DATOS PERSONALES

Nombre y apellidos	Josep M. Miret Biosca		
DNI/NIE/pasaporte	40872349S	Edad	61
Núm. identificación del investigador	Researcher ID	K-9274-2017	
	Código Orcid	0000-0003-4631-4294	

A.1. Situación profesional actual

Organismo	Universitat de Lleida			
Dpto./Centro	Departamento de Matemática			
Dirección	Jaume II, 69, 25001-Lleida			
Teléfono	973702776	Correo electrónico	miret@matematica.udl.cat	
Categoría profesional	Catedrático Universidad		Fecha inicio	11/10/19
Espec. cód. UNESCO	120101 - 120308 - 120501			
Palabras clave	Curvas algebraicas, Criptografía, Teoría algebraica de grafos			

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

Licenciatura/Grado/Doctorado	Universidad	Año
Licenciatura Matematicas	Universitat de Barcelona	1983
Doctorado Matematicas	Universitat Politècnica de Catalunya	1999

A.3. Indicadores generales de calidad de la producción científica *(véanse instrucciones)*
Número de sexenios de investigación: 4
Fecha del último sexenio concedido: 2013-2018 (5 de junio de 2019)
Número de tesis doctorales dirigidas (últimos 10 años): 5 Total Finalizadas: 6
Citas totales (fuente Scopus): 199
Promedio de citas/año durante los últimos 5 años: 19'4
Índice h (fuente Scopus): 8
Publicaciones totales en primer cuartil (Q1): 3
Publicaciones totales en segundo cuartil (Q2): 17
Publicaciones totales en tercer cuartil (Q3): 13
Publicaciones totales en cuarto cuartil (Q4): 8
Publicaciones en congresos internacionales: 22
Publicaciones en congresos nacionales: 31

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

Obtuve mi licenciatura en Ciencias Matemáticas por la Universidad Barcelona (1983), iniciando en septiembre de ese mismo año mi actividad docente en la Faculdad de Matemáticas de la Universidad de Barcelona, primero como ayudante y desde el 1987 como profesor asociado. El curso 1990-91 me incorporo a la Escuela Universitaria de Informática de Lleida, más adelante Escuela Universitaria Politécnica y actualmente Escuela Politécnica Superior de la Universitat de Lleida (UdL), donde he impartido e imparto docencia en las titulaciones de Ingeniería en Informática.

Mi actividad investigadora se inicia en el ámbito de la Geometría Algebraica bajo la dirección de Sebastián Xambó, con quien realicé mi tesina en la Universidad de Barcelona (1985) y el Doctorado en Matemáticas por la Universidad Politécnica de Catalunya (1999), donde me fue concedido el premio extraordinario de Doctorado. Actualmente, mi actividad de investigación se centra en el estudio de problemas computacionales con curvas elípticas e hiperelípticas sobre cuerpos finitos, así como en sus aplicaciones en el diseño de algoritmos y protocolos criptográficos que garanticen la seguridad en las comunicaciones. Formo parte del grupo de investigación de Criptografía y Grafos (C&G) de la UdL (http://www.cig.udl.cat/), del que soy coordinador. El grupo ha sido reconocido por la Generalitat de Catalunya, primero como

emergente 2009SGR-442 y más adelante como grupo consolidado 2014SGR-1666 y 2017SGR 1158. También colaboro en otra línea de investigación del grupo: aplicación de técnicas algebraicas en el estudio del problema del grado/diámetro para grafos y digrafos. Junto con los miembros del grupo C&G, mantengo una estrecha colaboración con el grupo de Codificación de la Información de Valladolid dirigido hasta hace unos años por Juan Tena, el grupo de Teoría de Números de la UPC, con Mireille Fouquet de la Univ. París-Diderot y con Nicolas Thériault de la Univ. de Santiago de Chile, entre otros.

Desde el 2006 al 2009 he sido el responsable de la red temática Matemáticas en la Sociedad de la Información (MatSI) que aglutina más de 30 grupos de investigación de España. He participado en 10 proyectos de investigación del plan nacional, siendo el investigador principal de 6 de ellos. También he participado en distintos proyectos de transferencia de tecnología financiados con las empresas BDigital y Scytl. Mi investigación ha dado lugar a un buen número de publicaciones tanto en revistas internacionales como en congresos nacionales e internacionales. He organizado varias conferencias sobre Criptografía, Matemática Discreta y Teoría de Números. Cabe señalar que en el año 2020, el grupo C&G organizará en la Univ. de Lleida la XVI Reunión Española de Criptología y Seguridad de la Información.

En cuanto a tareas de gestión en la UdL, he sido director de la Escuela Universitaria Politécnica (1993-2001), vicedirector de la Escuela Politécnica Superior (2004-2007), director del Dep. de Matemática (2007-2013) y coordinador Programa de Doctorado en Ingeniería y Tecnologías de la Información (2013-2018). Desde mayo 2019 a octubre 2020, Vicerector de Profesorado.

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

C.1. Publicaciones

R. Garra, J. Miret, J. Pujolàs, N. Thériault
The 2-adic valuation of the cardinality of Jac. genus 2 curves over quadratic towers of finite fields
Journal of Algebra and its Applications 18, no. 7, pp. 1950135, 2019
Cuartil: Q3

M. Fouquet, J. Miret, J. Valera,
Distorting the volcano,
Finite Fields and Their Applications 49, pp.108-125, 2018
Cuartil: Q2

M. Miller, J. Miret, A. Sillasen,
On digraphs of excess one,
Discrete Applied Mathematics 238, pp. 161-166, 2018
Cuartil: Q2

N. López, J. Miret,
On mixed almost Moore graphs of diameter two,
The Electronic Journal of Combinatorics 23(2), #P2.3, 2016
Cuartil: Q3

J. Miret, J. Pujolàs, N. Thériault,
Bisection and squares in genus 2,
Finite Fields and Their Applications 36, pp. 170-188, 2015
Cuartil: Q1

J. Conde, J. Gimbert, J. González, M. Miller, J. Miret,
On the nonexistence of almost Moore digraphs,
European Journal of Combinatorics, 39, pp. 170–177, 2014,
Cuartil: Q2

S. Martínez, J. Miret, R. Tomàs R, M. Valls
Security analysis of order preserving symmetric cryptography
Applied Mathematics & Information Sciences, Vol. 7 (4), pp.1285-1295, 2013
Cuartil: Q1

J. Conde, J. Gimbert, J. González, J. Miret, R. Moreno,
Nonexistence of almost Moore digraphs of diameter four,
The Electronic Journal of Combinatorics, 20, no. 1, #P75, 2013.
Cuartil: Q3

J. Miret, R. Moreno, A. Rio, M. Valls
Computing the l-power torsion of an elliptic curve over a finite field
Mathematics of Computation, Vol. 78 (267), pp.1767-1786, 2009
Cuartil: Q1

M. Cardona, M.A. Colomer, J. Conde, J. Miret, J. Miró, A. Zaragoza,
Chains computing limit existence and approximations with DNA
Biosystems 81, 261-266, 2005.
Cuartil: Q3

C.2. Proyectos

Criptografía con Curvas Algebraicas para la e-Sociedad,
MTM2013-46949-P - MEYC Ministerio de Economía y Competitividad.
Investigador Principal: J.M. Miret Biosca, F. Sebé Feixas
Fechas: 01/01/2014 - 31/12/2017
Importe: 100.430,00 €

Privacy-preserving and efficient smart metering,
57049770-DAAD–Acción Integrada Hispano-Alemana (German AcademicExchange Service)
Investigador Principal: M. Valls Marsal.
Fechas: 01/01/2014 - 31/12/2015
Importe: 13.478 €
Participación: Investigador

Bosnia and Herzegovina Qualification Framework for Higher Education,
544464-TEMPUS-1-2013-1-DE-TEMPUS-SMHES - UNER Unión Europea
Investigador Principal.: J.M. Ribo Balust
Fechas: 01/12/2013 - 30/11/2016
Importe: 30.678,00 €
Participación: Investigador

Técnicas criptográficas con curvas elípticas e hiperelípticas,
MTM2010-21580-C02-01 - MCIN Ministerio de Ciencia e Innovación.
Investigador Principal.: J.M. Miret Biosca
Fechas: 01/01/2011 - 30/09/2014
Importe: 78.287,00 €

Number Theoretic Algorithms inspired by Cryptography,
Ref: 1110578 – CONICYT, Chile
Investigador Principal.: Nicolas Thériault
Fechas: 06/03/2011 - 15/03/2015
Importe: 40.336,00 €
Participación: Investigador

Algoritmos y protocolos criptográficos con curvas elípticas e hiperelípticas,
MTM2007-66842-C02-02, MECI - Ministerio de Educación y Ciencia
Investigador Principal: J.M. Miret Biosca
Fechas: 01/10/2007 - 03/08/2010
Importe: 70.543,00 €

C.3. Contratos, méritos tecnológicos o de transferencia

Solucions de seguretat I ciberseguretat en utilities per a protecció d'infrastructures crítiques
Ref: COMRDI16-1-0060
Programa: Comunitat Ris3cat: Utilities 4.0 (Acció: Fons Europeu FEDER)
Empresa Partner: Fundació Eurecat
Investigador Principal UdL: J.M. Miret Biosca
Fechas: 01/06/2017 - 31/03/2021

BallotNext: Diseño y desarrollo de un sistema de votación avanzado basado en papel.
Programa: Proyecto INNPACTO, IPT-2012-0603-430000, MINECO - Ministerio de Economía y Competitividad.
Empresa Partner: Scytl Secure Electronic Voting SA
Investigador Principal UdL: J.M. Miret Biosca
Fechas: 01/01/2013 - 31/12/2014
Importe: 175.560,00 €

C.4. Patentes
Inventores: J.Puiggalí, S. Guasch, F. Sebé, J. Miret
Título: Method for verification of decryption processes
Número de solicitud: PCT/ES2009/000568
País de prioridad: PCT
Fecha de prioridad: 12/11/2009
Paises a los que se ha extendido: USA y EP
Empresa que la explota: Scytl Secure Electronic Voting, SA

C.5. Formación de doctores

Doctorando: Ramiro Moreno Chiral
Título: Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos
Directores: Josep M. Miret, Anna Rio (UPC)
Fecha lectura y calificación: 29/06/2005, Sobresaliente Cum Laude

Doctorando: Rosana Tomàs Cuñat
Título: Volcanes de isogenias de curvas elípticas: aplicaciones criptográf. a tarjetas inteligentes
Directores: Josep M. Miret, Daniel Sadornil (Univ. Cantabria)
Fecha lectura y calificación: 07/03/2011, Sobresaliente Cum Laude

Doctorando: Josep Conde Colom
Título: Contribuciones al estudio de los grafos y digrafos próximos a los de Moore
Directores: Joan Gimbert (UdL), Josep M. Miret
Fecha lectura y calificación: 06/03/2013, Sobresaliente Cum Laude

Doctorando: Víctor Mateu Meseguer
Título: New approaches for electronic voting paradigms
Directores: Josep M. Miret, Francesc Sebé (UdL)
Fecha lectura y calificación: 21/12/2015, Sobresaliente Cum Laude

Doctorando: Javier Valera Martín
Título: Contribuciones a la cardinalidad de curvas elípticas y a los volcanes de isogenias
Directores: Mireille Fouquet (Univ. Paris-Diderot), Josep M. Miret
Fecha lectura y calificación: 22/09/2017, Sobresaliente Cum Laude

Doctorando: Ricard Garra Oronich
Título: Algebraic curves and cryptographic protocols for the e-society
Directores: Josep M. Miret
Fecha lectura y calificación: 14/09/2018, Sobresaliente Cum Laude