

ÁLGEBRA, CODIFICACIÓN Y CRIPTOGRAFÍA

Características generales

Características del Equipo de Investigación

Características de la Investigación



IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	ÁLGEBRA, CODIFICACIÓN Y CRIPTOGRAFÍA
UNIDAD/DEPARTAMENTO DE PERTENENCIA	DEPARTAMENTO DE MATEMÁTICAS
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	UNIVERSIDAD DE OVIEDO



DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	CONSUELO MARTINEZ LOPEZ	TELÉFONO	985103337
ROL EN EL EQUIPO	INVESTIGADOR PRINCIPAL	MAIL	cmartinez@uniovi.es
WEB DEL EQUIPO	catedraia2.com		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Facultad de Ciencias	CENTRO	
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Federico García Lorca
NÚMERO	18	CIUDAD	Oviedo
PROVINCIA	Asturias	CÓDIGO POSTAL	33007

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Vicerrectorado de Investigación
MAIL	
TELÉFONO	
WEB	www.unioiv.es

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Edificio Histórico de la Universidad d Oviedo	CENTRO	
TIPO DE VÍA	Plaza	NOMBRE DE LA VÍA	Plaza de Riego
NÚMERO	s/n	CIUDAD	Oviedo
PROVINCIA	Asturias	CÓDIGO POSTAL	33003

ÁLGEBRA, CODIFICACIÓN Y CRIPTOGRAFÍA

Características generales

Características del Equipo de Investigación

Características de la Investigación



INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Consuelo Martínez López	Matemáticas

TRAYECTORIA PROFESIONAL

Realizó la licenciatura de matemáticas en la Universidad de Zaragoza, finalizando en junio de 1977. Realizó la tesis doctoral en el periodo 77-80 con una beca FPU y un contrato de profesora ayudante a tiempo parcial. Opositó al cuerpo de profesores adjuntos de universidad en 1982. Desempeñó su actividad docente e investigadora como profesora Titular de Universidad en la Universidad de Zaragoza hasta septiembre de 1993. Desde entonces ha desarrollado su actividad profesional en la Universidad de Oviedo como Titular de Universidad hasta octubre de 2005 y como Catedrática de Universidad desde esa fecha, después de haber superado la habilitación a Catedrático de Universidad a finales de 2003. Ha dirigido 5 tesis doctorales en los últimos 10 años y 15 a lo largo de su actividad académica. En la actualidad dirige tres tesis doctorales. Dirección de trabajos académicos, tesinas, trabajos fin de grado y fin de máster. Coordinadora del Programa de doctorado de Matemáticas y Estadística de la Universidad de Oviedo desde 2010 hasta 2018. Actualmente el programa es interuniversitario con las universidades del País Vasco, Pública de Navarra, La Laguna y Zaragoza. Ha sido coordinadora del Máster de Modelización e Investigación Matemática, Estadística y Computación de la Universidad de Oviedo, máster interuniversitario con las universidades del País Vasco, Pública de Navarra, La Laguna, La Rioja y Zaragoza. Miembro del Comité 1 de la CNEAI en 2016 y Presidenta del mismo en 2017. Miembro del Comité de Evaluación constituido por ANECA para las becas FPU en el área científica Matemáticas en 2014 y Coordinadora del mismo en 2015 y 2016. Adjunta de Algebra al Coordinador de Matemáticas de la ANEP desde enero de 2006 hasta diciembre de 2008. Evaluadora de la ANEP y de la ANECA (Programa ACADEMIA). Ha sido colaboradora de la ACSUCyL (Agencia para la Calidad del Sistema Universitario de Castilla y León), la AVAP (Agencia Valenciana d'Avaluació y Prospectiva, UNIBASQ y la ACSUG (Agencia para la Calidad del Sistema Universitario de Galicia) y AQU (Agencia de calidad de Cataluña). Miembro de la comisión de complementos del profesorado en Ciencias de UNIBASQ en 2016 y 2017 y actualmente presidenta de la misma. Miembro del Consejo de dirección del proyecto "Consolider i-math" durante todo el desarrollo del mismo. Miembro de la comisión elaboradora del informe SISE 2007 y 2008. Miembro del Consejo Director del Campus de Excelencia Internacional de la Universidad de Oviedo. Miembro del CRM Adviser Committee desde mayo de 2011 hasta 2017. Ha sido secretaria de la Comisión Científica de RSME y miembro del Comité Organizador o Científico de varios congresos. Participación como conferenciante invitada en varios congresos. Invitaciones a impartir conferencias y Seminarios en centros internacionales de prestigio (Cunty y Stevens Institute of Technology en 2016). Invitada por la London Mathematical Society a impartir conferencias en las Universidades de Dublin, Belfast y Queen Mary (London) en 2013. Estancias de investigación en diversos centros: MSRI, Yale University, Universidad de Chicago, ..., En los últimos 10 años realiza estancias todos los años en el KIAS de Seúl trabajando con E. Zelmanov.

WEB Y REDES SOCIALES



MIEMBROS DEL EQUIPO

Santos González Jiménez	Lorenzo Fernández, Esther	Fernández Rúa, Ignacio
García García, Beatriz	Piñera Nicolas, Alejandro	Molina Gómez, Fabian
Couselo Hernández, Elena	Consuelo Martínez López I.P.	López Díaz, Concepción

ÁLGEBRA, CODIFICACIÓN Y CRIPTOGRAFÍA

Características generales

Características del Equipo de Investigación

Características de la Investigación



LÍNEAS Y ÁREAS DE INVESTIGACIÓN

ÁREAS DE INVESTIGACIÓN

PRIVACIDAD

PRINCIPALES LÍNEAS DE INVESTIGACIÓN

Análisis Big Data enfocado al respeto de la privacidad
Protocolos criptográficos de preservación de la privacidad



PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2018

E. Martínez-Moro, A. Piñera-Nicolás, I.F. Rúa , Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over F_4 , *Journal of Pure and Applied Algebra* 222, 359-367, 2018

E. Martínez-Moro, A. Piñera-Nicolás, I.F. Rúa, Codes over Affine Algebras with a Finite Commutative Chain coefficient ring, *Finite Fields and their Applications* 49, 94-107, 2018

I.F. Rúa, E.F. Combarro, Cryptographic Uncertainty: Some Experiments on Finite Semifield Based Substitution Boxes, *The Mathematics of the Uncertain, Studies in Systems, Decision and Control (Studies in Systems, Decision and Control)* 142, 485-492, 2018

M.I. González Vasco, S. González, C. Martínez, A. Suárez Corona, The Roll of Dices in Cryptology, : Gil E., Gil E., Gil J., Gil M. (eds) *The Mathematics of the Uncertain. Studies in Systems, Decision and Control*, vol 142. Springer, Cham, 2018

PUBLICACIONES AÑO 2019

E.F. Combarro, J. Ranilla, I.F. Rúa, Experiments Testing the Commutativity of Finite-Dimensional Algebras with a Quantum Adiabatic Algorithm, *Computational and Mathematical Methods* 1, 01-011, 2019

E.F. Combarro, J. Ranilla, I.F. Rúa, Quantum walks for the determination of commutativity of finite dimensional algebras, *Journal of Computational and Applied Mathematics* 354, 496-506, 2019

E.F. Combarro, J. Ranilla, I.F. Rúa, A quantum algorithm for the commutativity of finite dimensional algebras, *IEEE Access* 7, 45554-45562, 2019

C. García Pillado, S. González, V. Markov, O. Markova and C. Martínez, Group codes of dimension 2 and 3 are abelian, *Fields and their Applications Group codes of dimension 2 and 3 are abelian* 55, Páginas, inicial : 167 final: 176, 2019

S. González, V. Markov, O. Markova, C. Martínez, Group Codes, *Communications in Computer and Information Sciences* 1133, 2019

PUBLICACIONES AÑO 2020

E.F. Combarro, A.P. Nicolás, J. Ranilla, I.F. Rúa, On finite division rings with a designed automorphism group, *Mathematical Methods in the Applied Sciences* 43(7), 3982-3994, 2020

I.F. Rúa, Nonbinary Delsarte-Goethals codes and finite semifields, *Glasgow Mathematical Journal*, 62(S1), 186-205, 2020.

M. Epelde, X. Larrucea, I.F. Rúa, On quaternary Goppa codes, *Discrete Mathematics* 343(9), 111962, 2020

E.F. Combarro, J. Ranilla, I.F. Rúa, Quantum Abstract Detecting Systems, *Quantum Information Processing* 19, 258, 2020

F. Rabanal, C. Martínez, Cryptography for big data environments: Current status, challenges, and opportunities, *Comp and Math Methods*, 2020, e1075

E.F. Combarro, F. Carminati, S. Vallecorsa, J. Ranilla, I.F. Rúa, On protocols for increasing the uniformity of random bits generated with noisy quantum computers, *Journal of Supercomputing* (pendiente de aparecer)

E.F. Combarro, A. Piñera-Nicolás, J. Ranilla, I.F. Rúa, An explanation of the Bernstein-Vazirani and Deutsch-Josza algorithms with the quantum stabilizer formalism, *Computational and Mathematical Methods* (pendiente de aparecer)

ÁLGEBRA, CODIFICACIÓN Y CRIPTOGRAFÍA

Características generales

Características del Equipo de Investigación

Características de la Investigación



PROYECTOS RELEVANTES

Título del proyecto: ESTRUCTURAS ALGEBRAICAS Y APLICACIONES. CODIFICACION Y CRIPTOGRAFIA
Entidad financiadora: Ministerio de Economía, Industria y Competitividad (Secretaría de Estado de Investigación, Desarrollo e Innovación) (MTM2017-83506-C2-2-P)
Entidades participantes: Universidad de Oviedo
Duración, desde: 01-01-2018 hasta: 31-12-2021
Investigador responsable: Consuelo Martínez López e Ignacio Fernández Rúa
Número de investigadores participantes: 10

Título del proyecto: Grupo de Álgebra, Codificación y Criptografía.
Entidad financiadora: FICYT del Principado de Asturias (FC-GRUPIN – IDI/2018/000193)
Entidades participantes:
Duración, desde: 1-12-2018 hasta: 31-12-2020
Investigador responsable: Consuelo Martínez López
Número de investigadores participantes: 6