Fecha del CVA	03.05.2024

Parte A. DATOS PERSONALES

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

A.1. Situación profesional actual

Organismo	Universidad Carlos III de Madrid			
Dpto./Centro	Escuela Politécnica Superior			
Dirección	Avda. de la Universidad, 30. 28911 Leganés (Madrid) España			
Teléfono		correo electrónico	Mariaisabel.gonzalez@uc3m.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 transferencia.**
Google Scholar**: 863 citas totales, 250 desde 2019, índice-h 17**

Autora/co-autora de **68 publicaciones, incluyendo 5 congresos de máximo nivel y 32 artículos en revistas listadas en JCR, seis de ellas en primer cuartil.** Co-autora de **dos patentes**, cuyos derechos sobre la propiedad intelectual fueron adquiridos por la empresa NEC Labs. Europe para su explotación. **Co-editora de tres Special Issues** en revistas listadas en JCR. Co-autora (con R. Steinwandt) del libro ***Group Theoretic Cryptography***, publicado en la serie Cryptography and Information Security de la editorial Chapman & Hall. Es además autora de **un libro de divulgación** (*Las matemáticas de la Criptología*, ed. Catarata) y un libro docente (con A.L. Pérez del Pozo, *Criptografía Esencial*, ed. RAMA).

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

Licenciada en Matemáticas y doctora por la Universidad de Oviedo (en ambos casos con Premio Extraordinario). Actualmente es Catedrática del área de Matemática Aplicada en la Universidad Carlos III de Madrid donde ocupa una Cátedra de Excelencia (desde diciembre de 2022). Se encuentra en comisión de servicios de su puesto de Catedrática en la Universidad Rey Juan Carlos (obtenida en 2021), en la que también ocupó una plaza de Profesora Titular desde 2009 y 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) y ha sido Affiliate Research Professor de la Florida Atlantic University entre 2015 y 2020.

Desarrolla su labor investigadora en el campo de la Criptografía Matemática desde 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 la actualidad, su trabajo se centra en el diseño y análisis formal de seguridad de esquemas de intercambio de clave para entornos multiusuario, con garantías de privacidad y/o frente a

adversarios cuánticos. En este ámbito, ha recibido financiación (como directora del nodo español) de dos proyectos dentro del programa Science for Peace and Security de la OTAN; "Secure Communication in the Quantum Era" (finalizado en 2022) y "Secure Communication via Classical and Quantum Tehnologies", que finaliza en 2026.

Desarrolla una intensa actividad relacionada con la Asociación Internacional de Investigación en Criptología (IACR), en particular, relativa a sus congresos, consideraros los foros de difusión más competitivos en criptografía: coautora de tres publicaciones IACR (TCC 2007 y 2005, PKC 2004), tres veces miembro de Comités de Programa asociados (PKC 2008 y 2010, Asiacrypt 2021), y program Co-Chair del Workshop Mathematical Cryptology (afiliado al Crypto 2023). Además de dirigir numerosos proyectos de investigación financiados en convocatorias públicas, ha liderado numerosos contratos (Art. 83 / Art. 60) 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). En 2022 coordinó además, con Bernardo Marín, la sección "Desafíos Criptográficos" del periódico El País. Es co-autora del juego de cartas para enseñar criptografía CryptoGo. Desde 2017 es miembro (vocal) de la Junta de Gobierno de la Real Sociedad Matemática Española, pertenece además a la Comisión de Publicaciones y es vicepresidenta de la Comisión de Transferencia de dicha sociedad. En 2023 recibió Premio de Honor del Jurado en la categoría de Talento STEM de los We Leadership Awards Madrid.

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

C.1. Publicaciones

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

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

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

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

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

6. J.M. Bohli, M.I. González Vasco y R. Steinwandt. *Building Group Key Establishment on Group Theory: A Modular Approach.*
Symmetry, 12(2), 197, 2020.
JCR 2020: 2.7, Multidisciplinary Sciences; 33/72. Q2

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

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

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

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

C.2. Proyectos

1. 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)

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

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

C.3. Contratos, méritos tecnológicos o de transferencia

1. 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.

2. 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.

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

4. Título del proyecto: Criptografía segura frente a adversarios cuánticos (Formación)
Entidad financiadora: CNI – Ministerio de Defensa Duración: Curso de 16 horas, 2021.
Cuantía de la subvención: 4.300€
Investigador principal: María Isabel González Vasco

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

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

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

---

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 tres Special Issues:
- *Mathcrypt 2023*, Mathematical Cryptology, 2023.
- *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, ummer School on Provable Security, (ambas en Barcelona, septiembre 2008, sept 2009). Miembro del comité de programa de numerosos congresos internacionales, resaltando PKC 2008 y 2010, ACISP 2009 y 2011, ICITS 2011, PQCrypto 2018.
