# Matemáticas en la Sociedad de la Información: Criptografía

**Equipo organizador**

- Miguel Beltrá Vidal (Universidad de Alicante)
- Sara Díaz Cardell (Universidad Estadual Paulista)
- Verónica Requena Arévalo (Universidad de Alicante)

**Descripción**

La teoría de la información fue introducida por Claude Shannon y Warren Weaver a finales de los años 40. Corresponde a una rama de las matemáticas y de la computación que estudia la transmisión y el procesamiento de datos. La criptografía es un método de protección de la información y las comunicaciones; además de una herramienta fundamental en la protección de la privacidad y la seguridad en la era digital, y su relación con las matemáticas es crucial. El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. La combinación de criptografía y tecnología proporciona la base para una infraestructura digital segura y eficiente en esta era digital. En esta sesión pretendemos recoger distintas nociones, métodos y algoritmos propios del álgebra, la geometría, la combinatoria, la estadística y la computación, que están siendo desarrolladas por diferentes investigadoras e investigadores españoles, atendiendo al área de la criptografía y sus variantes.

**Palabras clave:** Criptografía (94A60); Teoría de Códigos Algebraica: Criptografía (11T71); Aplicaciones a la Teoría de Códigos y la Criptografía de la Geometría Aritmética (14G50); Cifrado de datos (68P25); Criptografía Cuántica (81P94).

# Programa

JUEVES, 22 de enero

| | |
|---|---|
| 11:00 – 11:30 | Luís Hernández Encinas (CSIC)<br>*Estándares de la Criptografía Postcuántica y más* |
| 11:30 – 12:00 | Agustín Martín Muñoz (CSIC)<br>*Ataques por canal lateral usando inteligencia artificial* |
| 12:00 – 12:30 | Domingo Gómez Pérez (Universidad de Cantabria)<br>*Cyclotomic Mappings and Plateau Functions: Exploring Generalizations of APN Structures in Finite Fields* |
| 12:30 – 13:00 | Slobodan Petrović (Norwegian University of Science and Technology)<br>*El diseño de cifrados en flujo en el entorno no binario* |
| 15:30 – 16:00 | Ander Chueca Rodríguez (Universidad de León)<br>*Propuesta de Algoritmo de Cifrado de Imágenes Usando Caos y Autómatas Celulares* |
| 16:00 – 16:30 | José Andrés Armario (Universidad de Sevilla)<br>*Nonlinear Approximations in Linear Cryptanalysis using Hadamard Matrices* |
| 16:30 – 17:00 | Ignacio Cascudo (IMDEA Software Institute)<br>*Exceptional cliques of integer matrices and applications to secret sharing and zero-knowledge proofs* |
| 17:00 – 17:30 | Irene Urrutia Calvo (Universidad Carlos III de Madrid)<br>*Construcciones criptográficas basadas en grupos lineales de matrices* |
| 18:00 – 18:30 | Raúl M. Falcón (Universidad de Sevilla)<br>*Using mutually orthogonal local permutation polynomials in image symmetric encryption* |
| 18:30 – 19:00 | Juan Antonio López Ramos (Universidad de Almería)<br>*Criptografía basada en acciones con polinomios skew* |

VIERNES, 23 de enero

| | |
|---|---|
| 11:00 – 11:30 | Iván Blanco Chacón (Universidad de Alcalá)<br>*Fast Polynomial Arithmetic in Homomorphic Encryption with Cyclo-Multiquadratic Fields and maximal totally real cyclotomic* |
| 11:30 – 12:00 | Rodrigo Martín Sánchez-Ledesma (Universidad Complutense de Madrid, Indra Sistemas de Comunicaciones Seguras)<br>*Ataques a instancias PLWE totalmente factorizables vía isomorfismos explícitos* |
| 12:00 – 12:30 | Antonio Falcó (Universidad CEU Cardenal Herrera)<br>*A computational approach to the Regev Quantum Factorization Algorithm* |

# Estándares de la Criptografía Postcuántica y más

Luis Hernández Encinas, Luis Hernández-Álvarez, Agustín Martín Muñoz

Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)

luis.h.encinas@csic.es

***Resumen.*** En la bienal de la RSME de 2024 [1] presentamos la convocatoria del NIST para la criptografía postcuántica (PQC) y la publicación de los borradores considerados. Nos detuvimos en los problemas definidos sobre retículos dado que cuatro de los borradores basaban su seguridad en ellos.
A día de hoy tenemos más noticias, que abordaremos en esta charla, y algunos aspectos más:
1. Se han publicado tres de los cuatro estándares aprobados por el NIST: ML-KEM [2] y ML-DSA [3], basados en retículos y SLH-DSA [4], basada en hashes. Falta por publicarse FALCON [5] o FN-DSA.
2. Todo apunta a que uno de los KEM rechazados por el NIST puede ser estandarizado por ISO/IEC; se trata de FrodoKEM [6].
3. Se ha aprobado un nuevo KEM estándar: HQC [7], que basa su seguridad en códigos correctores de errores. Hecho previsible, para evitar la dependencia exclusiva de los retículos.
4. Además, continúa la nueva convocatoria del NIST para firmas digitales, ya en la Ronda 2, donde se vuelven a considerar problemas descartados anteriormente: los sistemas de ecuaciones multivariantes cuadráticas y las isogenias entre curvas elípticas.

## Referencias

[1] L. Hernández Encinas, Futuros Estándares de la Criptografía Postcuántica, Congreso Bienal de la Real Sociedad Matemática Española (RSME), Sesión especial de Criptografía. Pamplona, 23 de enero 2024.

[2] NIST (2024). *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, FIPS 203. `https://doi.org/10.6028/NIST.FIPS.203`

[3] NIST (2024). *Module-Lattice-Based Digital Signature Standard*, FIPS 204. `https://doi.org/10.6028/NIST.FIPS.204`.

[4] NIST (2024), *Stateless Hash-Based Digital Signature Standard*, FIPS 205. `https://doi.org/10.6028/NIST.FIPS.205`.

[5] T. Prest, P.-A. Fouque, J. Hoffstein et al. (2020). FALCON, `https://falcon-sign.info/`.

[6] E. Alkim, J.W. Bos, L. Ducas et al. (2021). FrodoKEM learning with errors key encapsulation, `https://frodokem.org/`

[7] C. Aguilar Melchor, N. Aragon, S. Bettaieb et al. (2020). HQC (Hamming Quasi-Cyclic), `http://pqc-hqc.org/index.html`

**Agradecimientos.** Trabajo parcialmente financiado por el CSIC, a través del proyecto *Seguridad Algebraica y Aplicaciones de la Inteligencia Artificial en la Criptología Actual y Postcuántica* (SAIACAP), Nº. Ref.: 202450E017.

# Ataques por canal lateral usando inteligencia artificial

Luis Hernández-Álvarez, Luis Hernández Encinas, Agustín Martín Muñoz

Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)

agustin.martin@csic.es

***Resumen.*** Los ataques a las implementaciones de los criptosistemas en dispositivos físicos, comúnmente conocidos como ataques por canal lateral, suponen desde 1996 una importante amenaza a la seguridad de dichos criptosistemas. A lo largo de los años se han propuesto numerosos tipos de ataque, utilizando por ejemplo técnicas diferenciales (DPA, *Differential Power Analysis*), correlación (CPA, *Correlation Power Analysis*), información mutua (MIA, *Mutual Information Analysis*) o plantillas (TA, *Template Attacks*). Más recientemente, los ataques basados en técnicas de aprendizaje automático (ML, *Machine Learning*) han tenido un gran impulso. El continuo desarrollo de esta tecnología motivó que el BSI, la oficina federal alemana de seguridad de la información, publicase en 2024 una guía para evaluar la resistencia de los criptosistemas a los ataques por canal lateral utilizando machine learning [1].
En los últimos años, la evolución de los ataques ha llevado a la utilización de técnicas de aprendizaje profundo (*deep learning*) [2], [3], [4], empleando diversos métodos (como redes neuronales convolucionales, *autoencoders*, redes neuronales recurrentes, etc.) para analizar la información que puede ser obtenida a través de los canales laterales. En esta comunicación se describirán los fundamentos de los ataques por canal lateral utilizando *deep learning*, así como los últimos avances en el campo.

## Referencias

[1] BSI, German Federal Office for Information Security (2024) *Guidelines for Evaluating Machine-Learning based Side-Channel Attack Resistance. Part of AIS 46.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_AI_guide.pdf.

[2] H. Maghrebi, T. Portigliatti, and E. Prouff (2016), Breaking cryptographic implementations using deep learning techniques, in C. Carlet et al., editores, *Security, Privacy, and Applied Cryptography Engineering* Lect. Notes in Comput. Sci., vol. 10076. Springer, 3—26.

[3] S. Picek, G. Perin, L. Mariot, L. Wu, L. Batina (2023). SoK: Deep Learning-based Physical Side-channel Analysis. *ACM Comput. Surv.*, 55, 11, Article 227, 1–35.

[4] S. Karayalçin, M. Krček, S. Picek (2025). A Practical Tutorial on Deep Learning-based Side-channel Analysis. *Cryptology ePrint Archive, Paper 2025/471*, 1–17.

**Agradecimientos.** Trabajo parcialmente financiado por el CSIC, a través del proyecto *Seguridad Algebraica y Aplicaciones de la Inteligencia Artificial en la Criptología Actual y Postcuántica* (SAIACAP), Nº. Ref.: 202450E017.

# Cyclotomic Mappings and Plateau Functions: Exploring Generalizations of APN Structures in Finite Fields

Ana I. Gómez, Domingo Gómez-Pérez

Departamento MATESCO, Universidad de Cantabria

gomezd@unicanes

***Resumen.*** Cyclotomic mappings, rooted in the partitioning of finite fields into multiplicative cosets, provide a powerful framework for constructing and analyzing nonlinear functions with desirable cryptographic properties. In this talk, we investigate the algebraic and combinatorial properties of cyclotomic mappings, with a focus on their role in generating plateau functions—functions whose Walsh spectra take on a small number of values. These functions generalize the concept of Almost Perfect Nonlinear (APN) functions, which are optimal against differential attacks in even characteristic fields. We explore how cyclotomic structures can be leveraged to construct new classes of plateau and generalized APN functions, analyze their spectral and differential properties, and discuss their implications in cryptography and coding theory. The talk will highlight recent advances, open problems, and the interplay between algebraic structure and cryptographic strength.

## Referencias

[1] Y. Li, H. Kan, S. Mesnager, J. Peng, L. Zheng (2024). Direct Approaches for Generic Constructions of Plateaued Functions and Bent Functions Outside M. *IEEE Trans. Inf. Theory.*

[2] X. Xie, N. Li, Q. Wang, X. Zeng (2024). On constructing bent functions from cyclotomic mappings. *IEEE Trans. Inf. Theory.*

[3] C. Carlet (2025). On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero. *Des. Codes Cryptogr.*, 93(4), 1237–1254.

**Agradecimientos.** This result is part of the project CÁTEDRA UNIVERSIDAD DE CANTABRIA-INCIBE DE NUEVOS RETOS EN CIBERSEGURIDAD, financed by European Union NextGeneration-EU, the Recovery Plan, Transformation and Resilience, through INCIBE.

# El diseño de cifrados en flujo en el entorno no binario

Slobodan Petrović

Norwegian University of Science and Technology (NTNU)

slobodan.petrović@ntnu.no

***Resumen.*** El desarrollo de los circuitos no-binarios ha hecho posible la realización en la práctica de varios algoritmos complejos de cifrado con menos transistores y el consumo reducido de energía. Eso es muy importante en algunos entornos, típicamente en el entorno IoT. En esta charla nos enfocamos en la generalización de varios teoremas conocidos que valen en los cuerpos finitos de característica 2 y sus aplicaciones en el diseño de cifrados en flujo que generan secuencias pseudoaleatorias no binarias. Estos cifrados tienen algunas ventajas teóricas sobre los cifrados binarios. Por ejemplo, es más fácil alcanzar las propiedades de resistencia contra loa ataques por correlación en los cuerpos con las características mayores que 3. Explicamos cómo se generan los polinomios adecuados de realimentación de los registros de desplazamiento realimentados linealmente (LFSR) y cómo se encuentran las funciones Booleanas no-lineales y equilibradas para combinar de una manera no-lineal las secuencias de salida de varios LFSRs no binarios. Al final se consideran algunas medidas de complejidad de las secuencias pseudoaleatorias no binarias.

## Referencias

[1] Potapov V.N. (2020). On $q$-ary bent and plateaued functions. *Designs, Codes, and Cryptography*, 88, 2037–2049.

[2] Bos S. (2024) *Beyond 0 and 1: A mixed radix design and verification workflow for modern ternary computers.* PhD thesis, University of South-Eastern Norway, Kongsberg.

[3] Stanković R., Astola J., Moraga C. (2022) *Representation of multiple-valued logic functions.* Springer Nature, Switzerland.

# Propuesta de Algoritmo de Cifrado de Imágenes Usando Caos y Autómatas Celulares

Ander Chueca Rodríguez, Adriana Suárez Corona

Departamento de Matemáticas, Universidad de León

achur@unileon.es

***Resumen.*** El crecimiento exponencial en la generación, transmisión y almacenamiento de imágenes digitales ha convertido la protección de información visual en un área relevante dentro de la ciberseguridad. A diferencia de otros tipos de datos, como el texto o los datos binarios, los gráficos presentan altas tasas de correlación entre píxeles adyacentes, valores redundantes y, cada vez, un mayor tamaño. Estas propiedades reducen la efectividad de cifrados clásicos como AES y limitan su uso en dispositivos de poca potencia.
Los modelos caóticos, caracterizados por su alta sensibilidad a las condiciones iniciales y su capacidad para generar secuencias aparentemente aleatorias, son una alternativa para el cifrado de imágenes. Este trabajo presenta un algoritmo de cifrado basado en la combinación de un modelo caótico y autómatas celulares, centrado en la eficiencia y la paralelización, para mejorar la seguridad en dispositivos con limitaciones de potencia, como cámaras de vigilancia.

## Referencias

[1] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 21(4), 917-935.

[2] Kocarev, L., Lian, S. (Eds.). (2011). *Chaos-based cryptography: Theory, algorithms and applications* (Vol. 354). Springer Science & Business Media.

**Agradecimientos.** Trabajo parcialmente financiado por el proyecto de investigación PID2021-123461NB-C22, del MCINN.

# Nonlinear Approximations in Linear Cryptanalysis using Hadamard Matrices

José Andrés Armario

Departamento de Matemática Aplicada I, Universidad de Sevilla

armario@us.es

***Resumen.*** The aim of this talk is to show a link between linear cryptanalysis and some types of nonlinear approximations [1]. The novelty of our approach relies on the use of Hadamard matrices to construct these nonlinear approximations. Focusing on Ascon's 5-bit S-box (see [2]), we will make some comments on our ongoing work.

## Referencias

[1] C. Beierle, A. Canteaut, G. Leander (2018). Nonlinear Approximations in Cryptanalysis Revisited. *IACR Transactions on Symmetric Cryptology*, 4, 80–101.

[2] C. Dobraunig, M. Eichlseder, F. Mendel, M. Schlaffer (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing, *Journal of Cryptology*, 34, n. 3, 33.

**Agradecimientos.** Trabajo en colaboración con Delfín Santana Rubio. Proyecto parcialmente financiado por FQM016 (JJAA).

# Exceptional cliques of integer matrices and applications to secret sharing and zero-knowledge proofs

Ignacio Cascudo

IMDEA Software Institute

ignacio.cascudo@imdea.org

***Resumen.*** Given a ring $R$, a subset $S \subset R$ is exceptional if $x-y$ is invertible in $R$ for every $x, y \in S$ with $x \neq y$. Recent applications to black-box secret sharing [1, 2, 3, 4] and zero-knowledge proofs for hidden order groups [4] have motivated the following question: *given $n > 0$, what is the size of the largest exceptional subset $S$ of the ring of $n \times n$ matrices over the integers $R = \mathrm{Mat}_n(\mathbb{Z})$?* For non-commutative rings like these, this question is very little explored, as opposed to the case of commutative rings, where H. Lenstra [5], already in 1976, introduced this concept in the context of rings of integers of algebraic number fields, in a celebrated result with important consequences to study which of these fields are Euclidean. In this talk, some of the recent results that the speaker has obtained together with other authors will be presented, and the aforementioned applications to cryptography will be explained.

## Referencias

[1] Y. Desmedt and Y. Frankel (1994). Perfect homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM J. Discret. Math.*, 7(4), 667–679.

[2] R. Cramer, S. Fehr (2002). Optimal black-box secret sharing over arbitrary abelian groups. *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, Lect. Notes Comput. Sci., vol. 2442, Springer-Verlag, 272–287.

[3] R. Cramer, S. Fehr, and M. Stam (2005). Black-box secret sharing from primitive sets in algebraic number fields. *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, Lect. Notes Comput. Sci., vol. 3621, Springer-Verlag, 344–360.

[4] C. Bartoli, I. Cascudo (2024). On sigma-protocols and (packed) black-box secret sharing schemes. *Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part II*, Lect. Notes Comput. Sci., vol. 14602, Springer-Verlag, 426–457.

[5] H. W. Lenstra Jr. (1976) Euclidean number fields of large degree. *Inventiones mathematicae*, 38, 1432–1297, 1976.

**Agradecimientos.** Based on joint works with Claudia Bartoli, and with Milan Boutros, Ronald Cramer and Daniel van Gent.

# Construcciones criptográficas basadas en grupos lineales de matrices

Irene Urrutia Calvo, María Isabel González Vasco

Departamento de Matemáticas, Universidad Carlos III de Madrid

urrutiacalvoirene@gmail.com

***Resumen.*** Con la aparición de la computación cuántica, los esquemas criptográficos convencionales se han visto amenazados, lo que ha impulsado la búsqueda de nuevas herramientas matemáticas. Entre ellas, las construcciones basadas en teoría de grupos han surgido como alternativas prometedoras. En esta charla nos centramos en construcciones criptográficas que emplean grupos lineales de matrices, como $SL_n(\mathbb{F}_p)$. En particular en funciones hash de Cayley definidas sobre dichos grupos. Este enfoque tiene sus orígenes en la propuesta de Tillich y Zémor (1994) [1], que ha dado lugar a un área activa de investigación que combina álgebra, teoría de grafos y criptografía. El objetivo principal de esta charla es analizar la seguridad de dos propuestas recientes basadas en la función hash de Tillich y Zémor: la propuesta por Le Coz et al. [3] y la de Shpilrain y Sosnovski [2]. Concretamente, estudiaremos su resistencia frente a ataques basados en la longitud, una clase de ataques probabilísticos originalmente desarrollados en grupos de trenzas y adaptados aquí al contexto de grupos de matrices.

## Referencias

[1] J. P. Tillich, G. Zémor (1994). Hashing with $SL_2$. *Advances in cryptography, Eurocrypt 1994*, 40–49.

[2] V. Shpilrain, B. Sosnovski (2025). Cayley Hashing with Cookies. *Advances in Information and Communication*, 706–718.

[3] C. Le Coz, C. Battarbee, Ramón Flores, T. Koberda, D. Kahrobaei (2024). Post-quantum hash functions using $SL_n(\mathbb{F}_p)$. *Advances in Mathematics of Communications*, 19(3), 996-–1009.

**Agradecimientos.** Este trabajo esta financiado el proyecto Vital-IoT de INCIBE. Se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiadas por la Unión Europea (Next Generation), el proyecto del Gobierno de España que traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID19, y para responder a los retos de la próxima década.

# Using mutually orthogonal local permutation polynomials in image symmetric encryption

Raúl M. Falcón, Jaime Gutiérrez, Jorge Jiménez Urroz

Departamento de Matemática Aplicada I, Universidad de Sevilla

rafalgan@us.es

***Resumen.*** Permutation polynomials (PPs) over finite fields have may applications in Cryptography, with particular relevance in the symmetric-key algorithm described by the Advanced Encryption Standard. This talk focuses on local permutation polynomials (LPPs) [5], which constitute a natural generalization of PPs to several variables. More specifically, an LPP in the polynomial ring $\mathbb{F}_q[x_1,\ldots,x_n]$, with $q$ a prime power, is a polynomial $f(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$ such that $f(a_1,\ldots,a_{k-1},x_k,a_{k+1},\ldots,a_n)$ is a permutation polynomial in $\mathbb{F}_q[x_k]$ for all $a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n \in \mathbb{F}_q$, and every $k \leq n$. Every LPP is equivalent to a Latin hypercube, so that there is a natural translation of notions and results between both theories. This fact has particular relevance in Cryptography, because Latin hypercubes are used to design error-correcting codes, cryptographic primitives, pseudorandom sequences or image encryption algorithm, among others. Despite this, and unlike PPs, there are very few papers in the literature dealing with LPPs [2, 3, 4]. This talk delves into this topic by showing how the superposition operator described by the so-called Hadamard multiary quasigroup product [1] can be used to construct mutually orthogonal LPPs. As an illustrative example, we show how this construction may be used in symmetric image encryption.

## Referencias

[1] R. M. Falcón, L. Mella, P. Vojtechovský (2025). The Hadamard multiary quasigroup product. *Banach Center Publications*, 129, 85–101.

[2] J. Gutiérrez, J. Jiménez Urroz (2023). Local permutation polynomials and the action of e-Klenian groups. Finite Fields Their Appl., 91, paper 102261, 22 pp.

[3] J. Gutiérrez, J. Jiménez Urroz (2025). Local permutation polynomials of maximum degree over prime finite fields. Bull. Malays. Math. Sci. Soc., 48, paper 40, 10 pp.

[4] J. Gutiérrez, J. Jiménez Urroz (2025). Permutation and local permutation polynomials of maximum degree. Afr. Mat., 36, paper 45, 11 pp.

[5] G. L. Mullen (1980). Local permutation polynomials over $\mathbb{Z}_p$. *Fibonacci Q.* 18, 104–108.

**Agradecimientos.** This research is partially s upported by the Research and Innovation Project PPIT-FEDER 2023 “Modeling small-world, scale-free networks from combinatorial designs based on quasigroup digraphs”, co-financed by the EU - Ministry of Finance and Public Administration - European Funds - Andalusian Regional Government - Ministry of University, Research and Innovation.

# Criptografía basada en acciones con polinomios skew

D. Camazón Portela, J. A. López Ramos

Departamento de Matemáticas, Universidad de Almería

jlopez@ual.es

***Resumen.***
En este trabajo, definimos la acción de un anillo de polinomios skew $\mathbb{F}_q[X;\sigma,\delta]$ sobre $\mathbb{F}_q$ basada en la evaluación polinomial y el producto skew a izquierda de funciones. Esta acción nos permite definir un subconjunto de $\mathbb{F}_q[x;\sigma,\delta]$ sobre el que somos capaces de controlar de algún modo la no-conmutatividad del producto y, sobre tal conjunto y haciendo uso de tal acción somos capaces de definir un intercambio de clave del tipo Diffie-Hellman como los introducidos en [1] basados en la acción de un semigrupo conmutativo sobre un conjunto. El protocolo es seguro en el modelo de Canetti y Krawczyk, [2], y permite otras aplicaciones criptográficas derivadas del mismo.

El cálculo del conjunto anteriormente referenciado sobre el que somos capaces de controlar la no conmutatividad y que sirve para escoger las claves privadas de cada entidad requiere, por otro lado, el estudio de ciertas variedades tóricas, además de una cierta simplifiación que permita un uso real del protocolo, permitiendo su implementación en dispositivos hardware y con un uso de ancho de banda mínimo en las comunicaciones.

## Referencias

[1] G. Maze, C. Monico, J. Rosenthal (2007). Public key cryptography based on semigroup actions. *Adv. Math. Commun.*, 1(4), 489–507.

[2] R. Canetti and H. Krawczyk (2001). Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, en *Advances in Cryptology-EUROCRYPT 2001*, Lect. Notes. Comp. Sci. vol. 2045. Springer, 2001, 453–474.

**Agradecimientos.** Este trabajo ha sido parcialmente financiado por los proyectos PID2022-138906NB-C21 MICIU/AEI/ 10.13039/501100011033 y PID2022-140934OB-I00 y por ERDF/EU.

# Fast Polynomial Arithmetic in Homomorphic Encryption with Cyclo-Multiquadratic Fields and maximal totally real cyclotomic subFields

Iván Blanco Chacón

Universidad de Alcalá

ivan.blancoc@uah.es

***Resumen.*** In this talk we will discuss the advantages and limitations of cyclotomic fields to have fast polynomial arithmetic within homomorphic encryption, and show how these limitations can be overcome by replacing cyclotomic fields by maximal totally real cyclotomic subfields and cyclomultiquadratic fields. This family is of particular interest due to its arithmetic efficiency properties and to the fact that the Polynomial Learning with Errors (PLWE) and Ring Learning with Errors (RLWE) problems are equivalent for it. We will also provide exact expressions for the condition number for any cyclotomic field, but under what we call the twisted power basis and will show that for this family, swapping between NTT (Number Theoretic Transform) and coefficient representations can be achieved at least twice faster than for the usual cyclotomic family. This talk is based on the recently published works [1] and [2].

## Referencias

[1] Blanco-Chacón, I., Pedrouzo-Ulloa, A., Njah Nchiwo, R.Y. et al. Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields. Cryptogr. Commun. (2025). https://doi.org/10.1007/s12095-024-00771-6

[2] Ahola, J., Blanco-Chacón, I., Bolaños, W. et al. Fast multiplication and the PLWE–RLWE equivalence for an infinite family of maximal real subfields of cyclotomic fields. Des. Codes Cryptogr. (2025). https://doi.org/10.1007/s10623-025-01601-3

# Ataques a instancias PLWE totalmente factorizables vía isomorfismos explícitos

Rodrigo Martín Sánchez-Ledesma, Raúl Durán Díaz

Departamento de Álgebra, Universidad Complutense de Madrid, España,
Indra Sistemas de Comunicaciones Seguras, España

rodrma01@ucm.es

***Resumen.*** En esta charla avanzamos algunos resultados concernientes a la generalización de ataques al problema PLWE (Polynomial Learning With Errors) que ofrecimos provisionalmente en [1]. En dichos ataques se usa el conocimiento de una raíz del polinomio generador del anillo de polinomios sobre cierto cuerpo base (finito) para obtener algoritmos que pueden resolver bajo ciertas condiciones el problema PLWE en su variante decisional.
Ahora el objetivo que nos proponemos es extender esos ataques por medio de la construcción de morfismos partiendo de instancias vulnerables a los ataques anteriormente descritos. Los primeros resultados indican que si el polinomio generador es totalmente factorizable sobre el cuerpo base no es posible encontrar nuevas vulnerabilidades.
Para demostrarlo la idea clave es construir isomorfismos explícitos entre polinomios totalmente factorizables y mostrar que tales isomorfismos siempre distorsionan las muestras en tal manera que las muestras transformadas no pueden ser utilizadas como una ventaja para el ataque decisional. Dicho con otras palabras, no permiten distinguir si tales muestras proceden de una distribución de tipo PLWE o bien de una distribución puramente uniforme, de modo que el ataque resulta ineficaz.

## Referencias

[1] I. Blanco Chacón, R. Durán Díaz, R. Martín Sánchez-Ledesma, *A Generalized Approach to Root-based Attacks against PLWE*, arXiv (2024). arXiv:2410.01017,doi:10.48550/arXiv.2410.01017.

# A computational approach to the Regev Quantum Factorization Algorithm

Antonio Falcó, Daniela Falcó-Pomares

Departamento de Matemáticas, Física y Ciencias Tecnológicas, Universidad CEU Cardenal Herrera

afalco@uchceu.es

***Resumen.*** This talk focuses on the cryptographic implications of the Regev Quantum Factorization Algorithm, analyzing its computational complexity and potential to challenge current cryptosystems. Regev's method [4] provides an alternative to Shor's algorithm [1], reducing quantum circuit complexity to $\widetilde{O}(n^{3/2})$ gates per subroutine call, balanced by $O(\sqrt{n})$ independent quantum runs and efficient classical post-processing based on lattice reduction. We interpret this structure within probabilistic proof systems, where quantum samples act as probabilistic certificates revealing hidden periodicities in lattice structures associated with integer factorization. We discuss how the algorithm could impact the hardness assumptions underlying RSA and lattice-based cryptography, particularly if combined with classical breakthroughs in lattice problem algorithms. In particular, recent extensions by Pilatte [2] and improvements in space complexity by Ragavan and Vaikuntanathan [3] could further influence the practicality of such quantum attacks. Furthermore, we examine conditions where Regev's approach may offer advantages in the NISQ regime or in hybrid quantum-classical cryptanalytic settings, and highlight open questions regarding the long-term security of post-quantum cryptosystems.

## Referencias

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2010.

[2] C. Pilatte, Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms, arXiv:2404.16450v1 [math.NT] 25 Apr 2024.

[3] S. Ragavan and V. Vaikuntanathan, Space-Efficient and Noise-Robust Quantum Factoring, arXiv:2310.00899v5 [quant-ph] 30 Apr 2025.

[4] O. Regev, An Efficient Quantum Factoring Algorithm, Journal of the ACM, 2024. `https://doi.org/10.1145/3708471`.

**Agradecimientos.** Proyecto parcialmente financiado por Generalitat Valenciana COMCUANTICA/007.