Matemática Aplicada a la Criptografía (MAK-UPC)

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	Matemática Aplicada a la Criptografía (MAK-UPC)
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Dept. Matemàtiques
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Universitat Politècnica de Catalunya (UPC)

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Javier Herranz	TELÉFONO	934016015
ROL EN EL EQUIPO	Investigador	MAIL	javier.herranz@upc.edu
WEB DEL EQUIPO	mak.upc.edu		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	C3	CENTRO	
TIPO DE VÍA	calle	NOMBRE DE LA VÍA	Jordi Girona
NÚMERO	1-3	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	8034

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	
MAIL	oficina.oae@upc.edu
TELÉFONO	934016200
WEB	www.upc.edu

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO		CENTRO	
TIPO DE VÍA	calle	NOMBRE DE LA VÍA	Jordi Girona
NÚMERO	31	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	8034

Matemática Aplicada a la Criptografía (MAK-UPC)

Características generales | **Características del Equipo de Investigación** | Características de la Investigación

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Jorge Villar	Doctor en Matemáticas

TRAYECTORIA PROFESIONAL

Más de 20 años de experiencia en ciberseguridad, participación en varios proyectos de investigación nacionales (2 como IP) y europeos, publicaciones en las principales revistas y congresos internacionales en el área de la criptografía. Temas de investigación: criptografía de clave pública, seguridad demostrable

WEB Y REDES SOCIALES

web.mat.upc.edu/jorge.villar/

MIEMBROS DEL EQUIPO

Padró Laimon, Carles	Morillo Bosch, Paz	Herranz Sotoca, Javier
Martín Molleví, Sebastià	Sáez Moreno, Germán	Martínez Pinilla, Ramiro

Matemática Aplicada a la Criptografía (MAK-UPC)		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
PROCESADO DE DATOS	Protección de datos (confidencialidad) Procesado seguro de datos y señales cifrados
GESTIÓN DE LA IDENTIDAD	Autenticación criptográfica Computación verificable Computación segura multiparte Protocolos de autenticación
PRIVACIDAD	Protocolos criptográficos de preservación de la privacidad Sistemas de anonimidad
OTRAS	Protocolos criptográficos para voto electrónico Criptografía basada en lattices Esquemas de compartición de secretos

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2020

O. Farràs, T. Kaced, S. Martín, C. Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. IEEE Transactions on Information Theory, 66 (11), pp. 7088-70100 (2020).

J. Herranz. Attacking pairing-free attribute-based encryption schemes. IEEE Access, 8, pp. 222226-222232 (202).

PUBLICACIONES AÑO 2019

N. Costa, R. Martínez, P. Morillo. Lattice-based proof of a shuffle. Proceedings of VOTING 2019 (4th Workshop on Advances in Secure Electronic Voting Schemes), FINANCIAL CRYPTOGRAPHY WORKSHOPS, Lecture Notes in Computer Science, 11599, pp. 330-346 (2019).

A. Faonio, D. Fiore, J. Herranz, C. Ràfols. Structure-preserving and re-randomizable RCCA-secure public key encryption and its applications. Proceedings of ASIACRYPT 2019, Lecture Notes in Computer Science, 11923, pp. 159-190 (2019).

R. Martínez, P. Morillo. RLWE-based zero-knowledge proofs for linear and multiplicative relations. Proceedings of IMA CC 2019, Lecture Notes in Computer Science, 11929, pp. 252-277 (2019).

PUBLICACIONES AÑO 2018

O. Farràs, T. Kaced, S. Martín, C. Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. Proceedings of EUROCRYPT 2018, Lecture Notes in Computer Science, 10820, pp. 597-621 (2018).

J. Herranz, G. Sáez. Secret sharing schemes for (k,n)-consecutive access structures. Proceedings of CANS'2018, Lecture Notes in Computer Science, 11124, pp. 463-480 (2018).

PUBLICACIONES AÑO 2017

F. Benhamouda, J. Herranz, M. Joye, B. Libert. Efficient cryptosystems from 2k-th power residue symbols. Journal of Cryptology, 30 (2), pp. 519-549 (2017).

N. Costa, R. Martínez, P. Morillo. Proof of a shuffle for lattice-based cryptography. Proceedings of NORDSEC'17, Lecture Notes in Computer Science, 10674, pp. 280-295 (2017).

A. Escala, G. Herold, E. Kiltz, C. Ràfols, J. Villar. An algebraic framework for Diffie-Hellman Assumptions. Journal of Cryptology, 30 (1), pp. 242-288 (2017).

O. Farràs, T.B. Hansen, T. Kaced, C. Padró. On the information ratio of non-perfect secret sharing schemes. Algorithmica, 79 (4), pp. 987-1013 (2017).

J. Herranz. Attribute-based encryption implies identity-based encryption. IET Information Security, 11 (6), pp. 332-337 (2017).

J.L. Villar. Equivalences and Black-Box Separations of Matrix Diffie-Hellman Problems. Proceedings of Public Key Cryptography (PKC 2017), Lecture Notes in Computer Science, 10174, pp. 435-464 (2017).

PUBLICACIONES AÑO 2016

A. Escala, S. Guasch, J. Herranz, P. Morillo. Universal cast-as-intended verifiability. Proceedings of VOTING 2016 (1st Workshop on Advances in Secure Electronic Voting Schemes), Lecture Notes in Computer Science, 9604, pp. 233-250 (2016).

M. Fueyo, J. Herranz. On the efficiency of revocation in RSA-based anonymous systems. IEEE Transactions on Information Forensics & Security, 11 (8), pp. 1771-1779 (2016).

S. Guasch, P. Morillo. How to challenge and cast your e-vote. Proceedings of FC'16 (Financial Cryptography and Data Security), Lecture Notes in Computer Science, 9603, pp. 130-145 (2017).

J. Herranz. Attribute-based versions of Schnorr and ElGamal. Applicable Algebra in Engineering, Communication and Computing, 27 (1), pp. 17-57 (2016).

S. Martín, C. Padró, A. Yang. Secret sharing, rank inequalities and information inequalities. IEEE Transactions on Information Theory, 62 (1), pp. 599-609 (2016).

C. Ràfols, P. Morillo, J. Villar. The Kernel Matrix Diffie-Hellman Assumption. Proceedings of ASIACRYPT'16, Lecture Notes in Computer Science, 10031, pp. 729-758 (2016).

Matemática Aplicada a la Criptografía (MAK-UPC)

Características generales | Características del Equipo de Investigación | Características de la Investigación

PROYECTOS RELEVANTES

RETOS, proyecto PID2019-109379RB-I00: "CREEME: Criptografía para retos digitales emergentes: escenarios multi-usuario y seguridad post-cuántica", IP: Javier Herranz (UPC) y Maribel González-Vasco (URJC), 2020-2023.

RIA (Research and Innovation Action) 780701: PROMETHEUS: PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS. IP: Sébastien Canard. 2018-2022. Por parte del partner UPC, Paz Morillo y Javier Herranz participan como investigadores. Ver https://cordis.europa.eu/project/rcn/213162_en.html

RETOS, proyecto MTM2016-77213-R: "CArSD: Criptografía avanzada para afrontar nuevos retos de la sociedad digital", IP: Javier Herranz, 2017-2020.

RETOS, proyecto MTM2013-41426-R: "eSAMCid: Hacia una sociedad digital segura: Avances matemáticos en criptografía y su impacto en las tecnologías digitales", IP: Jorge Villar, 2014-2017. Ver https://mat-web.upc.edu/people/jorge.villar/esamcid/