WiSeCom

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

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	WiSeCom
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Departamento de Tecnologías de la Información y las Comunicaciones
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Universitat Pompeu Fabra

WiSeCom
Wireless & Secure Communications Research Group

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Vanesa Daza	TELÉFONO	935421858
ROL EN EL EQUIPO	Directora de la línea de investigación de criptografía y ciberseguridad	MAIL	vanesa.daza@upf.edu
WEB DEL EQUIPO	https://www.upf.edu/web/wisecom		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Tánger	CENTRO	DTIC
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Roc Boronat
NÚMERO	138	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	8018

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Vanesa Daza
MAIL	vanesa.daza@upf.edu
TELÉFONO	935421858
WEB	https://www.upf.edu/web/vanesa-daza

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Tánger	CENTRO	DTIC
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Roc Boronat
NÚMERO	138	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	8018

WiSeCom

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

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Vanesa Daza	Doctora en Matemáticas

TRAYECTORIA PROFESIONAL

Vanesa Daza es Profesora Titular de la Universitat Pompeu Fabra desde 2012. Licenciada en Matemáticas por la Universitat de Barcelona y Ph.D. Licenciada en Matemáticas por la Universitat Politècnica de Catalunya. Ha trabajado como investigadora en la industria (Scytl, España) así como en la academia (Universidad Rovira i Virgili). Ha realizado estancias de investigación en la Universidad de Salerno (Italia) y la Universidad de Aarhus (Dinamarca). Ha sido coautora de más de 40 artículos, entre revistas internacionales y importantes conferencias de criptografía y ciberseguridad. También es co-inventora de tres patentes internacionales. Actualmente lidera dos proyectos H2020 relacionados con la ciberseguridad, BAnDIT (MSCA-ITN-EID) y PRESENT (RIA), además de dos proyectos Nacionales. Sus principales intereses de investigación se relacionan con el uso de técnicas criptográficas distribuidas para mejorar la seguridad y la privacidad para proteger las tecnologías emergentes, con especial énfasis en la actualidad en la tecnología blockchain. Es editora asociada de las revistas internacionales IEEE Transactions on Dependable and Secure Computing i IEEE Transactions on Information Forensics and Security, dos de las revistas internacionales más prestigiosas en el ámbito. También ha participado en numerosos comités de programas de congresos internacionales, así como en la organización de eventos de carácter internacional. Entre otros puestos de la UPF, presidió el Departamento de Tecnologías de la Información y las Comunicaciones de la Universidad Pompeu Fabra.

WEB Y REDES SOCIALES

https://www.upf.edu/web/vanesa-daza
https://twitter.com/vdazaf

MIEMBROS DEL EQUIPO

Ràfols Salvador, Carla	Franzoni, Federico	Zacharakis, Alexandros
Zapico, Arantxa	Salleras, Xavier	McMenamin, Conor
Bellés Muñoz, Marta	Pindado Tost, Zaira	Silva Velón, Javier

WiSeCom		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	PRINCIPALES LÍNEAS DE INVESTIGACIÓN
GESTIÓN DE LA IDENTIDAD	Computación segura multiparte
PRIVACIDAD	Protocolos criptográficos de preservación de la privacidad

WiSeCom		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2021

Prastudy Fauzi, Helger Lipmaa, Zaira Pindado, Janno Siim: Somewhere Statistically Binding Commitment Schemes with Applications. Financial Cryptography 2021

PUBLICACIONES AÑO 2020

Federico Franzoni, Vanesa Daza:Improving Bitcoin Transaction Propagation by Leveraging Unreachable Nodes. Blockchain 2020: 196-203

Federico Franzoni, Ivan Abellan, Vanesa Daza: Leveraging Bitcoin Testnet for Bidirectional Botnet Command and Control Systems. Financial Cryptography 2020: 3-19

Vanesa Daza, Carla Ràfols, Alexandros Zacharakis:Updateable Inner Product Argument with Logarithmic Verifier and Applications. Public Key Cryptography (1) 2020: 527-557

Salleras X, Daza V. SANS: self-Sovereign authentication for network slices. Security and Communication Networks. 2020 Nov 24;2020:8823573. DOI: 10.1155/2020/8823573

Carla Ràfols, Javier Silva: QA-NIZK Arguments of Same Opening for Bilateral Commitments. AFRICACRYPT 2020: 3-23

Karim Baghery, Alonso González, Zaira Pindado, Carla Ràfols: Signatures of Knowledge for Boolean Circuits Under Standard Assumptions. AFRICACRYPT 2020: 24-44

Karim Baghery, Zaira Pindado, Carla Ràfols: Simulation Extractable Versions of Groth's zk-SNARK Revisited. CANS 2020: 453-461

PUBLICACIONES AÑO 2019

Vanesa Daza, Xavier Salleras: LASER: Lightweight and Secure Remote Keyless Entry Protocol. ICETE (2) 2019: 372-377

Vanesa Daza, Alonso González, Zaira Pindado, Carla Ràfols, Javier Silva: Shorter Quadratic QA-NIZK Proofs. Public Key Cryptography (1) 2019: 314-343

Mojtaba Khalili, Mohammad Dakhilalian, Carla Ràfols: Short tightly secure signatures for signing a vector of group elements: A new approach. Theor. Comput. Sci. 795: 225-239 (2019)

Antonio Faonio, Dario Fiore, Javier Herranz, Carla Ràfols: Structure-Preserving and Re-randomizable RCCA-Secure Public Key Encryption and Its Applications. ASIACRYPT (3) 2019: 159-190

Alonso González, Carla Ràfols:Shorter Pairing-Based Arguments Under Standard Assumptions. ASIACRYPT (3) 2019: 728-757

PUBLICACIONES AÑO 2018

Josep Domingo-Ferrer, Alberto Blanco-Justicia, Carla Ràfols: Dynamic group size accreditation and group discounts preserving anonymity. Int. J. Inf. Sec. 17(3): 243-260 (2018)

Panagiotis Grontas, Aris Pagourtzis, Alexandros Zacharakis, Bingsheng Zhang: Towards Everlasting Privacy and Efficient Coercion Resistance in Remote Electronic Voting. Financial Cryptography Workshops 2018: 210-231

PUBLICACIONES AÑO 2017

Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, Matteo Signorini: CoLLIDE: CLoud Latency-based IDEntification. EUSPN/ICTH 2017: 81-88

Vanesa Daza, Roberto Di Pietro, Ivan Klimek, Matteo Signorini: CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. ICC 2017: 1-6

Vanesa Daza, Nikolaos Makriyannis: Designing Fully Secure Protocols for Secure Two-Party Computation of Constant-Domain Functions. TCC (1) 2017: 581-611

Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, Jorge Luis Villar: An Algebraic Framework for Diffie-Hellman Assumptions. J. Cryptol. 30(1): 242-288 (2017)

Gottfried Herold, Max Hoffmann, Michael Klooß, Carla Ràfols, Andy Rupp: New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs. CCS 2017: 1547-1564

Steven D. Galbraith, Christophe Petit, Javier Silva: Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. ASIACRYPT (1) 2017: 3-33

Roberto Di Pietro, Federico Franzoni, Flavio Lombardi: HyBIS: Advanced Introspection for Effective Windows Guest Protection. SEC 2017: 189-204

Panagiotis Grontas, Aris Pagourtzis, Alexandros Zacharakis: Coercion Resistance in a Practical Secret Voting Scheme for Large Scale Elections. ISPAN-FCST-ISCC 2017: 514-519

PUBLICACIONES AÑO 2016

Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, Matteo Signorini:FRoDO: Fraud Resilient Device for Off-Line Micro-Payments. IEEE Trans. Dependable Secur. Comput. 13(2): 296-311 (2016)

Alonso González, Carla Ràfols:New Techniques for Non-interactive Shuffle and Range Arguments. ACNS 2016: 427-444

Paz Morillo, Carla Ràfols, Jorge Luis Villar: The Kernel Matrix Diffie-Hellman Assumption. ASIACRYPT (1) 2016: 729-758

PUBLICACIONES 2015

Vanesa Daza, Matteo Signorini: Smart User Authentication for an Improved Data Privacy. Advanced Research in Data Privacy 2015: 345-363

Tzeta Tsao, Roger K. Alexander, Mischa Dohler, Vanesa Daza, Angel Lozano, Michael C. Richardson: A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). RFC 7416: 1-40 (2015)

Alonso González, Alejandro Hevia, Carla Ràfols: QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions. ASIACRYPT (1) 2015: 605-629

Carla Ràfols: Stretching Groth-Sahai: NIZK Proofs of Partial Satisfiability. TCC (2) 2015: 247-27

PUBLICACIONES AÑO 2014

Boris Bellalta, Azadeh Faridi, Jaume Barceló, Vanesa Daza, Miquel Oliver: Performance analysis of a Multiuser Multi-Packet Transmission system for WLANs in non-saturation conditions. Comput. Networks 60: 88-100 (2014)

Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, Matteo Signorini: SOLDI: Secure Off-Line Disposable CredIts to Secure Mobile Micro Payments. ICETE (Selected Papers) 2014: 340-362

Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, Matteo Signorini: FORCE - Fully Off-line secuRe CrEdits for Mobile Micro Payments. SECRYPT 2014: 125-136

Gottfried Herold, Julia Hesse, Dennis Hofheinz, Carla Ràfols, Andy Rupp: Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations. CRYPTO (1) 2014: 261-279

Alex Escala, Javier Herranz, Benoît Libert, Carla Ràfols: Identity-Based Lossy Trapdoor Functions: New Definitions, Hierarchical Extensions, and Implications. Public Key Cryptography 2014: 239-256

PUBLICACIONES AÑO 2013

Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, Jorge L. Villar: An Algebraic Framework for Diffie-Hellman Assumptions. CRYPTO (2) 2013: 129-147

WiSeCom		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2012

Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie de Panafieu, Carla Ràfols: Attribute-based encryption schemes with constant-size ciphertexts. Theor. Comput. Sci. 422: 15-38 (2012)

Javier Herranz, Fabien Laguillaumie, Benoît Libert, Carla Ràfols: Short Attribute-Based Signatures for Threshold Predicates. CT-RSA 2012: 51-67

PUBLICACIONES AÑO 2011

Boris Bellalta, Vanesa Daza, Miquel Oliver: An Approximate Queueing Model for Multi-Rate Multi-User MIMO Systems. IEEE Commun. Lett. 15(4): 392-394 (2011)

Javier Herranz, Fabien Laguillaumie, Carla Ràfols: Relations between semantic security and anonymity in identity-based encryption. Inf. Process. Lett. 111(10): 453-460 (2011)

Boris Bellalta, Vanesa Daza, Jaume Barceló, Miquel Oliver: Buffer Sizing in TxSDMA Systems. MACOM 2011: 241-253

PUBLICACIONES AÑO 2010

Vanesa Daza, Javier Herranz, Paz Morillo, Carla Ràfols: Extensions of access structures and their cryptographic applications. Appl. Algebra Eng. Commun. Comput. 21(4): 257-284 (2010)

Javier Herranz, Fabien Laguillaumie, Carla Ràfols: Constant Size Ciphertexts in Threshold Attribute-Based Encryption. Public Key Cryptography 2010: 19-34

PUBLICACIONES AÑO 2009

Vanesa Daza, Javier Herranz, Germán Sáez: Flaws in some self-healing key distribution schemes with revocation. Inf. Process. Lett. 109(11): 523-526 (2009)

Vanesa Daza, Josep Domingo-Ferrer, Francesc Sebé, Alexandre Viejo: Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks. IEEE Trans. Veh. Technol. 58(4): 1876-1886 (2009)

Paz Morillo, Carla Ràfols: The Security of All Bits Using List Decoding. Public Key Cryptography 2009: 15-33

PUBLICACIONES AÑO 2008

Vanesa Daza, Javier Herranz, Paz Morillo, Carla Ràfols: Ad-Hoc Threshold Broadcast Encryption with Shorter Ciphertexts. Electron. Notes Theor. Comput. Sci. 192(2): 3-15 (2008)

David Galindo, Paz Morillo, Carla Ràfols: Improved certificate-based encryption in the standard model. J. Syst. Softw. 81(7): 1218-1226 (2008

Vanesa Daza, Javier Herranz, Germán Sáez: On the Computational Security of a Distributed Key Distribution Scheme. IEEE Trans. Computers 57(8): 1087-1097 (2008)

Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, Carles Padró: On Codes, Matroids, and Secure Multiparty Computation From Linear Secret-Sharing Schemes. IEEE Trans. Inf. Theory 54(6): 2644-2657 (2008)

PUBLICACIONES AÑO 2007

Vanesa Daza, Javier Herranz, Paz Morillo, Carla Ràfols:Cryptographic techniques for mobile ad-hoc networks. Comput. Networks 51(18): 4938-4950 (2007)

Vanesa Daza, Paz Morillo, Carla Ràfols: On Dynamic Distribution of Private Keys over MANETs. Electron. Notes Theor. Comput. Sci. 171(1): 33-41 (2007)

Vanesa Daza, Javier Herranz, Paz Morillo, Carla Ràfols: CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts. ProvSec 2007: 35-50

Agusti Solanas, Josep Domingo-Ferrer, Antoni Martínez-Ballesté, Vanesa Daza: A distributed architecture for scalable private RFID tag identification. Comput. Networks 51(9): 2268-2279 (2007)

Vanesa Daza, Josep Domingo-Ferrer: On Partial Anonymity in Secret Sharing. EuroPKI 2007: 193-202

Jordi Castellà-Roca, Vanesa Daza, Josep Domingo-Ferrer, Jesús A. Manjón, Francesc Sebé, Alexandre Viejo: An Incentive-Based System for Information Providers over Peer-to-Peer Mobile Ad-Hoc Networks. MDAI 2007: 380-392

PUBLICACIONES AÑO 2006

Jordi Castellà-Roca, Vanesa Daza, Josep Domingo-Ferrer, Francesc Sebé: Privacy homomorphisms for e-gambling and mental poker. GrC 2006: 788-791

David Galindo, Paz Morillo, Carla Ràfols: Breaking Yum and Lee Generic Constructions of Certificate-Less and Certificate-Based Encryption Schemes. EuroPKI 2006: 81-91

PUBLICACIONES AÑO 2005

Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, Carles Padró: On Codes, Matroids and Secure Multi-party Computation from Linear Secret Sharing Schemes. CRYPTO 2005: 327-343

PUBLICACIONES AÑO 2004

Vanesa Daza, Javier Herranz, Germán Sáez: Protocols useful on the Internet from distributed signature schemes. Int. J. Inf. Sec. 3(2): 61-69 (2004)

Carlo Blundo, Paolo D'Arco, Vanesa Daza, Carles Padró: Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures. Theor. Comput. Sci. 320(2-3): 269-291 (2004)

PUBLICACIONES AÑO 2003

Vanesa Daza, Javier Herranz, Germán Sáez: Constructing General Dynamic Group Key Distribution Schemes with Decentralized User Join. ACISP 2003: 464-475

Vanesa Daza, Javier Herranz, Germán Sáez:Some Protocols Useful on the Internet from Threshold Signature Schemes. DEXA Workshops 2003: 359-363

PUBLICACIONES AÑO 2002

Vanesa Daza, Javier Herranz, Carles Padró, Germán Sáez:A Distributed and Computationally Secure Key Distribution Scheme. ISC 2002: 342-356

PUBLICACIONES AÑO 2001

Carlo Blundo, Paolo D'Arco, Vanesa Daza, Carles Padró: Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures. ISC 2001: 1-17

PROYECTOS RELEVANTES

Título: PRESENT: Photoreal Realtime Sentient Entity
Entidad financiadora: Comissió Europea
Referència de la concessió: 856879
Importe: 4,102,070.00€
Duración: desde el 01/09/2019 hasta 31/08/2022.
Investigadores principales: Josep Blat y Vanesa Daza

Título del proyecto: Agrupació de Tecnologies Emergents Fem IoT
Entidad financiadora: Secretaria d'Universitats i Recerca - Fons FEDER
Referencia de la concesión: codi int. coordinada 001-P-001662
Importe concedido: 388.040,38€ (subvención: 194.020,19€)
Duración: desde el 02/05/2019 hasta 30/04/2022
Investigadores principales:Boris Bellalta y Vanesa Daza

Título del proyecto: BAnDIT: Blockchain Attack and Defense Techniques
Entidad financiadora: Comisión Europea
Referencia de la concesión: 814284
Importe concedido: 1,051,413.84€
Duracióna: desde el 01/03/2019 hasta 28/02/2023
Investigador principal: Vanesa Daza

Título del proyecto: ALICE: Técnicas avanzadas de cadenas de bloques para la internet de las cosas
Entidad financiadora: Ministerio de Ciencia, Innovación y Universidades
Referencia de la concesión: RTI2018-102112-B-I00
Importe concedido: 55.902,00€
Duración: desde el 01/01/2019 hasta 31/12/2021
Investigadora principal: Vanesa Daza