CURRÍCULUM VÍTAE NORMALIZADO

David Arroyo Guardeño

Generated from: Editor CVN de FECYT

Date of document: 22/07/2024

v 1.4.3

2c24b6b87804a19a844e1cc689c16193

This electronic file (PDF) has embedded CVN technology (CVN-XML). The CVN technology of this file allows you to export and import curricular data from and to any compatible data base. List of adapted databases available at: http://cvn.fecyt.es/

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT INNOVACIÓN

Summary of CV

This section describes briefly a summary of your career in science, academic and research; the main scientific and technological achievements and goals in your line of research in the medium -and long- term. It also includes other important aspects or peculiarities.

Since July 2018 I am a Senior Scientist at ITEFI, CSIC. Since 2018 my goal has been to create a research group focused on the field of cybersecurity and privacy protection. The group was finally created on 29 March 2023 under the name of Research Group on Cybersecurity and Privacy Protection (GiCP). As principal investigator of the GiCP, I am the only permanent staff member. All other staff are employed on a project basis or receive funding through the JAE-Intro programme of the CSIC. As a CSIC PI I have carried out both the preparation of proposals and their execution, which has involved setting up the computing laboratory from scratch and finding and hiring the working teams for the projects I lead and have led.

Since 2018 I have led two H2020 projects (TRESCA, SPIRS) and one Horizon Europe project (GoIT). I also participate in the Horizon Europe QUBIP project, I am the principal investigator of the CSIC in XAI-Disinfodemics (https://gicp.es/xai-disinfodemics-explainable-ai-for-disinformation-and-conspiracydetection-during-infodemics/) and I have been the principal investigator of the Comunidad de Madrid CYNAMON project. Currently leading the project on digital twins with protection against quantum threat QCDI, as well as a collaboration contract with IMIDRA for the traceability of products in the food chain. As of September 2014, I am coordinating the cyber-attribution activities that CSIC will carry out in the context of the Horizon Europe Safehorizon project (https://gicp.es/introducing-safehorizon-pioneering-the-fight-against-crime-as-a-service-operations/).

For more information, please refer to: https://gicp.es/projects/, https://gicp.es/team/

References:

Billy Bob Brumley (https://scholar.google.com/citations?user=7QX0AQYAAAAJ), Rochester Institute of Technology, billy.brumley@rit.edu.
Constantinos Patsakis (https://scholar.google.com/citations?hl=en&user=wkHmlysAAAAJ), University of Piraeus, kpatsak@imis.athena-innovation.gr

General quality indicators of scientific research

This section describes briefly the main quality indicators of scientific production (periods of research activity, experience in supervising doctoral theses, total citations, articles in journals of the first quartile, H index...). It also includes other important aspects or peculiarities.

I received a M. Sc. degree in Telecommunications Engineering from the University of Seville (Spain), and a PhD in Physics of Complex Systems from the Polytechnic University of Madrid (Spain) in 2009, supervised by Dr. Gonzalo Alvarez Marañón and Dr. Gerardo Pastor Dégano. From October 2001 to July 2002 I was Erasmus Student at the University of Swansea (Wales, UK). During that period I completed my M. Sc. final dissertation in the group of Prof. Jaafar Elmirghani. Once I got my M. Sc. degree in Telecommunications, I worked as software developer of e-learning applications at the CNICE (Spanish Ministry of Education) from January 2003 to April 2005. The next four years I was FPI-MEC predoctoral researcher at the Institute of Applied Physics of the Spanish National Research Council (CSIC). From May 2010 to January 2011 I was JAE-DOC postdoctoral researcher at the Institute of Acoustics of the Spanish National Research Council (CSIC). From January 2011 to July 2018 I was researcher and professor at the Autonomous University of Madrid (Universidad Autónoma de Madrid, UAM). Currently I am Tenured Scientist at the Institute of Physical and Information Technologies (ITEFI), CSIC.

I have WOS h-index of 13, a Google Scholar h-index of 19, and has gained recognition for twelve years (2 sexenios) and for fifteen years (3 quinquenios) of international quality research from the national committee for the assessment of the research action (CNEAI) . I have (co-)authored 37 scientific papers included in the JCR, 2 books, 5 book chapters, and 65 works submitted to national or international conferences. My publications are mainly devoted to inter- and multidisciplinary applications in the areas of cryptography, information security, information theory and coding, signal processing, and nonlinear dynamics. I am member of the Editorial Board of three journals in the JCR, and a regular reviewer for over 15 international journals in the areas of cryptography, information sciences, information security, multimedia processing, signal processing, nonlinear dynamics, and bio-informatics.

Along my research career I proposed and applied computational procedures to improve key enabling technologies in the context of security information, electromechanical devices, and neuroscience. In all cases my focus is on implementing bidirectional protocols to extract information and control nonlinear time-varying dynamical systems. Those procedures are based on information theory, statistics, cybernetics, formal analysis, and machine learning. Indeed, the analysis and classification of time series to identify the main components of a dynamical system is of major importance for mechanics and computational neuroscience, but also for the evaluation of security properties of modern ICT. The quantification of the functional interrelationship among components of a system is essential to design efficient electromechanical devices, to propose activity-dependent stimulation protocols to reveal dynamics in neurophysiology, and to ponder confidentiality and privacy in communication networks.

I have an extensive teaching experience in Computer Science since 2005 (see **http://tinyurl.com/jpzcxqb**). From 2012 I am professor at the master and doctoral programs of the Computer Science and Engineering of the UAM. In addition, I have co-supervised a doctoral thesis. I have supervised 14 undergraduate thesis projects, and 5 master thesis projects (**http://tinyurl.com/gl3ohoz**).

David Arroyo Guardeño

Surname(s): **Arroyo Guardeño**
Name: **David**
ORCID: **0000-0001-8894-9779**
ScopusID: **14828747100**
ResearcherID: **A-5167-2010**
Personal web page: **https://dargcsic.github.io/**

Current professional situation

Employing entity: Consejo Superior de Investigaciones Científicas (CSIC), Spanish National Research Council

Professional category: Tenured Scientist (Científico Titular)

Start date: 09/07/2018

Type of contract: Permanent employment contract **Dedication regime:** Full time

Performed tasks: Design and deployment of computational procedures to improve key enabling technologies in the context of security information, electromechanical devices, and neuroscience. Those procedures are based on information theory, cryptography, statistics, cybernetics, formal analysis, and machine learning.

Identify key words: Systems theory: control; Communication, information; Coding correcting theory; Software; Algorithms; Computation and discrete mathematics; Applications; Multivariate analysis; Sampling theory; Physical application and phisical technologies application; Simulations outside data analysis; Data analysis methods; Statistics and probability; Scientific calculation

Previous positions and activities

	Employing entity	Professional category	Start date
1	Unviversidad Autónoma de Madrid	Lecturer (Profesor Contratado Doctor)	12/12/2017
2	Unviversidad Autónoma de Madrid	Interim Lecturer (Profesor Contratado Doctor Interino)	01/09/2015
3	Unviversidad Autónoma de Madrid	Assistant Professor (Profesor Ayudante Doctor)	22/01/2013
4	Universidad Autónoma de Madrid	Contratado postdoctoral Juan de la Cierva (Juan de la Cierva postdoctoral research felowship)	13/01/2011
5	Consejo Superior de Investigaciones Científicas	Contratado postdoctoral JAE-DOC (JAE-DOC postdoctoral research fellow)	01/05/2010
6	Consejo Superior de Investigaciones Científicas	Becario predoctoral FPI-MEC (FPI-MEC predoctoral research fellow)	01/08/2005
7	ASOCIACION INVESTIGACION Y DESARROLLO INDUSTRIAL DE RECURSOS NATURALES (AITEMIN)	Ayundante de investigación (Research assistant)	01/04/2005
8			01/01/2003

	Employing entity	Professional category	Start date
	Centro Nacional de Información y Comunicación Educativa	Beca para el estudio de la aplicación de TIC en educación (Scholarship holder: development of computer applications for education)	

1 **Employing entity:** Unviversidad Autónoma de Madrid **Type of entity:** University
Professional category: Lecturer (Profesor Contratado Doctor)
Start-End date: 12/12/2017 - 06/07/2018

2 **Employing entity:** Unviversidad Autónoma de Madrid **Type of entity:** University
Professional category: Interim Lecturer (Profesor Contratado Doctor Interino)
Start-End date: 01/09/2015 - 11/12/2017

3 **Employing entity:** Unviversidad Autónoma de Madrid **Type of entity:** University
Professional category: Assistant Professor (Profesor Ayudante Doctor)
Start-End date: 22/01/2013 - 31/08/2015

4 **Employing entity:** Universidad Autónoma de Madrid **Type of entity:** University
Department: Departamento de Ingeniería Informática, Escuela Politécnica Superior de la Universidad Autónoma de Madrid
City employing entity: Madrid, Community of Madrid, Spain
Professional category: Contratado postdoctoral Juan de la Cierva (Juan de la Cierva postdoctoral research felowship)
Start-End date: 13/01/2011 - 21/01/2013
Type of contract: Grant-assisted student (pre or post-doctoral, others)
Dedication regime: Full time
Performed tasks: Desarrollo de observadores y controladores en tiempo real. Diseño de métodos para la clasificación y codificación adecuados para la detección y caracterización de eventos en tiempo real. Implementación de metodologías en lazo cerrado para la observación y control de redes neuronales biológicas.

Development of the Real-Time Dynamical Observer and Controlller. Design classification and codification methods adequate to perform event detection and characterization in real-time, or at least on-line. Implementation of closed-loop methodologies for observing and controlling biological neuronal networks.
Identify key words: Systems theory: control; Communication, information; Coding correcting theory; Physical application and phisical technologies application; Simulations outside data analysis; Nets; Data analysis methods; Statistics and probability; Cryptography

5 **Employing entity:** Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Department: Instituto de Acústica
Professional category: Contratado postdoctoral JAE-DOC (JAE-DOC postdoctoral research fellow)
Start-End date: 01/05/2010 - 11/01/2011
Type of contract: Grant-assisted student (pre or post-doctoral, others)
Performed tasks: Caracterización y control de dispositivos no lineales de ultrasonidos.

Characterization and control of nonlinear ultrasound devices.

Identify key words: Ultrasounds; Physical application and phisical technologies application; Dataprocessing

6 **Employing entity:** Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Department: Instituto de Física Aplicada
Professional category: Becario predoctoral FPI-MEC (FPI-MEC predoctoral research fellow)
Start-End date: 01/08/2005 - 31/07/2009
Performed tasks: Investigación en criptografía caótica, teoría de la información, dinámica no lineal y sistemas complejos.

Research in chaotic cryptography, information theory, nonlinear dynamics and complex systems.
Identify key words: Systems theory: control; Communication, information; Computation and discrete mathematics; Computer network; Dataprocessing

7 **Employing entity:** ASOCIACION INVESTIGACION Y DESARROLLO INDUSTRIAL DE RECURSOS NATURALES (AITEMIN)
Professional category: Ayundante de investigación (Research assistant)
Start-End date: 01/04/2005 - 31/07/2005
Performed tasks: Investigación y desarrollo de software para visión artificial.

Research and software development in artificial vision.

8 **Employing entity:** Centro Nacional de Información y Comunicación Educativa **Type of entity:** Subdirección General integrada en la Dirección General de Evaluación y Cooperación Territorial que, a su vez, forma parte de la Secretaría de Estado de Educación, Formación Profesional y Universidades
Professional category: Beca para el estudio de la aplicación de TIC en educación (Scholarship holder: development of computer applications for education)
Start-End date: 01/01/2003 - 31/03/2005 **Duration:** 2 years - 3 months
Performed tasks: Desarrollo de aplicaciones software (Java, PHP) para e-learning. Administrador de sistemas mysql y servidores Apache.

Software development (Java, PHP) of e-learning applications. Administrator of mysql databases and Apache servers.

Education

University education

1st and 2nd cycle studies and pre-Bologna degrees

1 **University degree:** Higher degree
Name of qualification: Ingeniero de Telecomunicación (Telecommunications Engineer)
Degree awarding entity: Universidad de Sevilla **Type of entity:** University
Date of qualification: 18/10/2002

2 **Name of qualification:** Licenciado en Filosofía (In Progress: 178 credits completed of 316)
Degree awarding entity: Universidad Nacional de Educación a Distancia **Type of entity:** University

Doctorates

Doctorate programme: Programa Oficial de Doctorado en Física de Sistemas Complejos (Physics of Complex Systems)
Degree awarding entity: Universidad Politécnica de Madrid **Type of entity:** University
Date of degree: 28/07/2009
DEA awarding entity: Universidad Politécnica de Madrid
Date DEA was awarded: 09/10/2007
Thesis title: Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems
Thesis director: Gonzalo Álvarez Marañón
Thesis co-director: Gerardo Pastor Dégano
Obtained qualification: Excellent Cum Laude (Sobresaliente "cum laude"); Citations according to Google Scholar: 20
Recognition of quality: Yes

Specialised, lifelong, technical, professional and refresher training (other than formal academic and healthcare studies)

1 **Training title:** Seguridad de la información (Information Security)
Awarding entity: Departamento de Tratamiento de la Información y Codificación del CSIC **Type of entity:** State agency
End date: 01/03/2006 **Duration in hours:** 5 hours

2 **Training title:** Nuevas tecnologías aplicadas al desarrollo de contenidos educativos multimedia interactivos (New ICTs for the development of interactive multimedia applications in education)
Awarding entity: Centro Nacional de información y comunicación educativa (CNICE) **Type of entity:** State agency
End date: 25/11/2004 **Duration in hours:** 21 hours

3 **Training title:** Certificado de Aptitud Pedagógica (Postgraduate certificate in Education)
Awarding entity: Universidad Complutense de Madrid **Type of entity:** University
End date: 28/06/2004 **Duration in hours:** 180 hours

4 **Training title:** First Certificate in English
Awarding entity: University of Cambridge **Type of entity:** University
End date: 01/06/2002

Attended advanced, improvement and innovative teacher training and new technology courses and seminars focused on improving teaching

1 **Title of course/seminar:** Técnicas de "scaffolding" en docencia bilingüe (inglés) a niver universitario (Scaffolding techniques for teachers in a bilingual (english and spanish) CLIL university context)
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
Duration in hours: 8 hours
Start-End date: 03/12/2012 - 10/12/2012

2 **Title of course/seminar:** Moodle para la Docencia: Nivel II (Teaching with Moodle II)
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
Duration in hours: 13 hours
Start-End date: 14/10/2011 - 14/10/2011

3 **Title of course/seminar:** Moodle para la Docencia: Nivel I (Teaching with Moodle I)
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
Duration in hours: 13 hours
Start-End date: 19/09/2011 - 26/09/2011

Language skills

Language	Listening skills	Reading skills	Spoken interaction	Speaking skills	Writing skills
English		C1	C1	C1	C1

Teaching experience

General teaching experience

1 **Type of teaching:** Unofficial teaching
Name of the course: Privacidad, -Seguridad y Aspectos Éticos
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Start date: 01/03/2021 **End date:** 12/05/2021
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 10
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

2 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** Virtual
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 21/09/2020 **End date:** 29/09/2020
Type of hours/ ECTS credits: Hours
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

3 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de análisis de datos: clustering
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 1
Start date: 05/05/2020 **End date:** 06/05/2020
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 8
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

4 **Type of teaching:** Unofficial teaching
Name of the course: Privacidad, -Seguridad y Aspectos Éticos
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 2
Start date: 01/12/2019 **End date:** 12/01/2020
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 10
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

5 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** Virtual
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 21/09/2019 **End date:** 29/09/2019
Type of hours/ ECTS credits: Hours
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

6 **Type of teaching:** Unofficial teaching
Name of the course: Seminario: Blockchain
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 1
Start date: 08/03/2019 **End date:** 08/03/2019
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

7 **Type of teaching:** Unofficial teaching
Name of the course: Disrupción tecnológica: Ciberseguridad
University degree: Máster en Transformación y Consultoría de Negocio
Frequency of the activity: 1
Start date: 13/02/2019 **End date:** 13/02/2019
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 4
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Facultad de Ciencias Económicas y Empresariales

8 **Type of teaching:** Unofficial teaching
Name of the course: Privacidad, -Seguridad y Aspectos Éticos
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 2
Start date: 01/12/2018 **End date:** 12/01/2019
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 10
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

9 **Type of teaching:** Unofficial teaching
Name of the course: Disrupción tecnológica: Blockchain
University degree: Máster en Transformación y Consultoría de Negocio
Frequency of the activity: 1
Start date: 05/12/2018 **End date:** 05/12/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 4
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Facultad de Ciencias Económicas y Empresariales

10 **Type of teaching:** Unofficial teaching
Type of teaching: Virtual
University degree: Curso Superior de Delegado en Protección de Datos
Start date: 15/10/2018 **End date:** 21/10/2018
Entity: Instituto Universitario de Investigación Ortega y Gasset **Type of entity:** Foundation
City of entity: Madrid, Community of Madrid, Spain

11 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** Virtual
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 21/09/2018 **End date:** 29/09/2018
Type of hours/ ECTS credits: Hours
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

12 **Type of teaching:** Unofficial teaching
Name of the course: Hyperledger hands-on
University degree: Curso de verano: Blockchain: de las criptomonedas a las redes de negocio

Course given: https://www.uam.es/UAM/18.-Blockchain/1446761310659.htm?language=es%27A=0&pid=1242687777259&title=18.%20Blockchain:%20de%20las%20criptomonedas%20a%20las%20redes%20de%20negocio
Frequency of the activity: 1
Start date: 18/07/2018 **End date:** 20/07/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

13 **Type of teaching:** Unofficial teaching
Name of the course: Introducción a Blockchain
University degree: Curso de verano: Blockchain: de las criptomonedas a las redes de negocio
Frequency of the activity: 1
Start date: 18/07/2018 **End date:** 20/07/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

14 **Type of teaching:** Unofficial teaching
Name of the course: Moderador de la mesa redonda "Blockchain: mitos, posibilidades y realidades"
University degree: Curso de verano: Blockchain: de las criptomonedas a las redes de negocio
Frequency of the activity: 1
Start date: 18/07/2018 **End date:** 20/07/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

15 **Type of teaching:** Unofficial teaching
Name of the course: Taller de ciberseguridad
University degree: Professional Data Science
Frequency of the activity: 1
Start date: 07/07/2018 **End date:** 07/07/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 5
Entity: MBIT School **Type of entity:** Business
City of entity: Madrid, Community of Madrid, Spain

16 **Type of teaching:** Unofficial teaching
Name of the course: Ciberseguridad y analítica
University degree: Business Inteligence & Big Data
Frequency of the activity: 1
Start date: 06/07/2018 **End date:** 06/07/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 5
Entity: MBIT School **Type of entity:** Business
City of entity: Madrid, Community of Madrid, Spain

17 **Type of teaching:** Official teaching
Name of the course: Proyecto de programación
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Obligatory
University degree: Grado en ingeniería informática
Course given: 1 **Frequency of the activity:** 1
Start date: 13/01/2018 **End date:** 30/06/2018
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: English

18 **Type of teaching:** Official teaching
Name of the course: Internet y Redes Avanzadas
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Obligatory
University degree: Máster Universitario en Ingeniería Informática
Frequency of the activity: 3
Start date: 03/03/2016 **End date:** 16/06/2018
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

19 **Type of teaching:** Official teaching
Name of the course: Programación II
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Obligatory
University degree: Grado en Ingeniería Informática
Course given: 1 **Frequency of the activity:** 1
Start date: 20/01/2018 **End date:** 19/05/2018
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingenería Informática. 2017-18
Subject language: Spanish

20 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de análisis de datos: clustering
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 2
Start date: 05/05/2018 **End date:** 06/05/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 8
Entity: Universidad Autónoma de Madrid **Type of entity:** University

Faculty, institute or centre: Escuela Politécnica Superior

21 **Type of teaching:** Unofficial teaching
Name of the course: Privacidad, -Seguridad y Aspectos Éticos
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 2
Start date: 01/12/2017 **End date:** 12/01/2018
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 10
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

22 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 16/11/2017 **End date:** 14/12/2017
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 15
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

23 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de análisis de datos: clustering
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Frequency of the activity: 2
Start date: 05/05/2017 **End date:** 06/05/2017
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 8
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

24 **Type of teaching:** Unofficial teaching
Name of the course: Clustering
University degree: Master en Bioinformática y Biología Computacional
Start date: 02/03/2017 **End date:** 09/03/2017
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

25 **Type of teaching:** Official teaching
Name of the course: Fundamentos de Criptografía y Seguridad Informática
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Optional
University degree: Grado en ingeniería informática
Course given: 4
Start date: 13/10/2016 **End date:** 13/12/2016
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3

Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

26 **Type of teaching:** Unofficial teaching
Name of the course: Investigación forense en móviles
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 16/09/2016 **End date:** 23/09/2016
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 12
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

27 **Type of teaching:** Official teaching
Name of the course: Biomedical Signal Processing and its applications
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Optional
University degree: Máster Universitario en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones
Frequency of the activity: 3
Start date: 23/11/2015 **End date:** 22/12/2015
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

28 **Type of teaching:** Official teaching
Name of the course: Estructura de datos
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Obligatory
University degree: Grado en Ingeniería Informática
Course given: 2 **Frequency of the activity:** 2
Start date: 21/09/2015 **End date:** 18/12/2015
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingenería Informática. 2015-16, 2 grupos de prácticas
Subject language: Spanish

29 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de análisis de datos: clustering
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Start date: 05/12/2015 **End date:** 12/12/2015
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 6

Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

30 **Type of teaching:** Unofficial teaching
Name of the course: Privacidad, -Seguridad y Aspectos Éticos
University degree: Título de Experto en Big Data y Data Science: Ciencia e Ingeniería de Datos
Start date: 12/09/2015 **End date:** 12/09/2015
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

31 **Type of teaching:** Official teaching
Name of the course: Sistemas Operativos
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Optional
University degree: Grado en ingeniería informática
Course given: 2 **Frequency of the activity:** 3
Start date: 26/01/2014 **End date:** 24/04/2015
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingenería Informática. 2014-15, 2 grupos de prácticas
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

32 **Type of teaching:** Official teaching
Name of the course: Seguridad y auditoría de los sistemas de información
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Obligatory
University degree: Máster Universitario en Ingeniería Informática
Frequency of the activity: 5
Start date: 03/03/2014 **End date:** 10/03/2015
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

33 **Type of teaching:** Unofficial teaching
Name of the course: Mobile devices: security challenges and solutions
Type of teaching: In person theory
University degree: Formación in-company
Frequency of the activity: 1
Start date: 24/07/2014 **End date:** 24/07/2014
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 4
Entity: Centro Nacional de Excelencia en Ciberseguridad
Faculty, institute or centre: Universidad Autónoma de Madrid

34 **Type of teaching:** Official teaching
Name of the course: Proyecto de programación
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Obligatory
University degree: Grado en ingeniería informática
Course given: 1 **Frequency of the activity:** 1
Start date: 13/01/2013 **End date:** 30/06/2013
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: English

35 **Type of teaching:** Official teaching
Name of the course: Desarrollo de Aplicaciones para Dispositivos Móviles
Type of programme: Engineering **Type of teaching:** In person theory
University degree: Grado en Ingeniería Informática
Frequency of the activity: 6
Start date: 21/01/2013 **End date:** 03/05/2013
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior

36 **Type of teaching:** Official teaching
Name of the course: Fundamentos de Criptografía y Seguridad Informática
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Optional
University degree: Grado en ingeniería informática
Course given: 4 **Frequency of the activity:** 2
Start date: 13/10/2012 **End date:** 13/12/2012
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

37 **Type of teaching:** Official teaching
Name of the course: Biomedical Signal Processing and its applications
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Optional
University degree: Máster Universitario en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones
Frequency of the activity: 1
Start date: 29/10/2012 **End date:** 21/11/2012
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2

Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

38 **Type of teaching:** Official teaching
Name of the course: Temas avanzados en Ciencias de la Computación IV
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Optional
University degree: ingeniería informática
Course given: 4 **Frequency of the activity:** 1
Start date: 13/01/2012 **End date:** 28/06/2012
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

39 **Type of teaching:** Official teaching
Name of the course: Proyecto de Programación
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Obligatory
Assessment type: Survey
University degree: Grado en ingeniería informática
Course given: 1 **Frequency of the activity:** 1
Start date: 13/01/2012 **End date:** 13/05/2012
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Assessment type: Survey
Mark obtained: 4.22 **Top mark possible:** 5
Subject language: Spanish

40 **Type of teaching:** Official teaching
Name of the course: Temas Avanzados en Ciencias de la Computación IV
Type of programme: Engineering **Type of teaching:** Laboratory work
Type of subject: Optional
University degree: Ingeniería informática
Course given: 4 **Frequency of the activity:** 1
Start date: 13/01/2011 **End date:** 30/06/2011
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 3
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain

Subject language: Spanish

41 **Type of teaching:** Official teaching
Name of the course: Proyecto de Programación
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
Assessment type: Survey
University degree: Grado en Ingeniería Informática
Course given: 1 **Frequency of the activity:** 1
Start date: 13/01/2011 **End date:** 13/06/2011
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Assessment entity: Universidad Autónoma de Madrid
City assessment entity: Ecuador
Assessment type: Survey
Type of entity: University
Mark obtained: 4.18 **Top mark possible:** 5
Subject language: Spanish

42 **Type of teaching:** Official teaching
Name of the course: criptografía y teoría de códigos
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 20/09/2010 **End date:** 04/02/2011
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

43 **Type of teaching:** Official teaching
Name of the course: criptografía y teoría de códigos
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 14/09/2009 **End date:** 05/02/2010
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain

Subject language: Spanish

44 **Type of teaching:** Official teaching
Name of the course: Criptografía y seguridad informática
Type of programme: Master's degree **Type of teaching:** In person theory
University degree: Máster en Ingeniería Matemática
Start date: 13/05/2009 **End date:** 21/05/2009
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 12
Entity: Universidad Complutense de Madrid **Type of entity:** University
Faculty, institute or centre: Facultad de Ciencias Matemáticas
City of entity: madrid, Community of Madrid, Spain

45 **Type of teaching:** Official teaching
Name of the course: criptografía y teoría de códigos
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 15/09/2008 **End date:** 29/01/2009
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

46 **Type of teaching:** Official teaching
Name of the course: criptografía y teoría de códigos
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 02/10/2007 **End date:** 25/01/2008
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

47 **Type of teaching:** Official teaching
Name of the course: Criptografía y seguridad informática
Type of programme: Master's degree **Type of teaching:** In person theory
University degree: Máster en Ingeniería Matemática
Start date: 23/05/2007 **End date:** 24/05/2007
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 4
Entity: Universidad Complutense de Madrid **Type of entity:** University

Faculty, institute or centre: Facultad de Ciencias Matemáticas

48 **Type of teaching:** Official teaching
Name of the course: Criptografía avanzada
Type of programme: Master's degree **Type of teaching:** In person theory
University degree: Máster/Experto en Seguridad de la Información
Frequency of the activity: 1
Start date: 21/02/2007 **End date:** 23/02/2007
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 8
Entity: Universidad de Deusto **Type of entity:** University
Faculty, institute or centre: Facultad de Ingeniería
City of entity: Bilbao, Basque Country, Spain

49 **Type of teaching:** Official teaching
Name of the course: Seguridad Informática
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 08/02/2006 **End date:** 30/06/2006
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

50 **Type of teaching:** Official teaching
Name of the course: Criptografía y Teoría de Códigos
Type of programme: Engineering **Type of teaching:** In person theory
Type of subject: Optional
University degree: Ingeniería Informática
Course given: 3 **Frequency of the activity:** 1
Start date: 04/10/2005 **End date:** 07/02/2006
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 6
Entity: Universidad Antonio de Nebrija **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior y Arquitectura
Department: Ingeniería Informática
City of entity: madrid, Community of Madrid, Spain
Subject language: Spanish

51 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Start date: 22/12/2016
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 15

Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

52 **Type of teaching:** Official teaching
Name of the course: Biomedical Image Processing
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Optional
University degree: Máster Universitario en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones
Frequency of the activity: 1
Start date: 20/01/2014
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

53 **Type of teaching:** Official teaching
Name of the course: Information systems in biomedicine: Data Integration and knowledge management
Type of programme: Master's degree **Type of teaching:** In person theory
Type of subject: Optional
University degree: Máster Universitario en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones
Frequency of the activity: 1
Start date: 2013
Type of hours/ ECTS credits: Credits
Hours/ECTS credits: 2
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Faculty, institute or centre: Escuela Politécnica Superior
Department: ingeniería informática
City of entity: madrid, Community of Madrid, Spain

54 **Type of teaching:** Official teaching
Name of the course: Criptografía y seguridad informática
Type of programme: Master's degree **Type of teaching:** In person theory
University degree: Máster en Ingeniería Matemática
Start date: 29/05/2008
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 4
Entity: Universidad Complutense de Madrid **Type of entity:** University
Faculty, institute or centre: Facultad de Ciencias Matemáticas

55 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 5
Entity: Universidad Autónoma de Madrid **Type of entity:** University

Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

56 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 5
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

57 **Type of teaching:** Unofficial teaching
Name of the course: Fundamentos de ciberseguridad
Type of programme: Máster **Type of teaching:** In person theory
University degree: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 9
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Department: Instituto de Ciencias Forenses y Seguridad
City of entity: Madrid, Community of Madrid, Spain

58 **Type of teaching:** Unofficial teaching
Name of the course: Análisis forense de dispositivos móviles Android
Type of teaching: In person theory
University degree: Formación in-company: Dirección General de la Policía Nacional de España
Frequency of the activity: 1
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 10
Entity: Centro Nacional de Excelencia en Ciberseguridad
Faculty, institute or centre: Universidad Autónoma de Madrid

59 **Type of teaching:** Unofficial teaching
Name of the course: Introducción a Python
Type of teaching: In person theory
University degree: Formación in-company: Dirección General de la Policía Nacional de España
Frequency of the activity: 1
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 16
Entity: Centro Nacional de Excelencia en Ciberseguridad
Faculty, institute or centre: Universidad Autónoma de Madrid

60 **Name of the course:** Curso de Verano
University degree: Ciberseguridad: vulnerabilidades, amenazas y riesgos
Type of hours/ ECTS credits: Hours
Hours/ECTS credits: 1
Entity: Universidad Rey Juan Carlos **Type of entity:** University

Experience supervising doctoral thesis and/or final year projects

1 **Project title:** Desarrollo de un sistema de trazabilidad en entornos IoT mediante Hyperledger
Type of project: Master's degree final project (TFM, Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
City of entity: Madrid, Community of Madrid, Spain
Student: Jesús Iglesias García
Obtained qualification: 9,5 (Matrícula de Honor)
Date of reading: 25/09/2018
Quality recognition: Yes **Date of award:** 19/12/2018

2 **Project title:** Análisis de metadatos en Bitcoin
Type of project: Master Thesis (Big Data and Data Science)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
City of entity: Madrid, Community of Madrid, Spain
Student: Antonio Vaquerizo Muñoz
Obtained qualification: 5
Date of reading: 09/10/2018

3 **Project title:** Aplicación de los principios de la Ingeniería del Malware al contexto del Pentesting
Type of project: Master thesis
Entity: Universidad Autónoma de Madrid **Type of entity:** University
City of entity: Madrid, Community of Madrid, Spain
Student: Alejandro Villegas López
Obtained qualification: 9
Date of reading: 25/09/2018

4 **Project title:** Seguridad de aplicaciones web basadas en las tecnologías Node.js y Mongodb: estudio y caso de uso
Type of project: Trabajo Fin de Máster en Ingeniería Informática
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Pedro Alberto Ruíz González
Obtained qualification: 9
Date of reading: 03/07/2018

5 **Project title:** Desarrollo de un indexador de contenido para la Deep Web
Type of project: Bachelor Thesis
Entity: Universidad Autónoma de Madrid **Type of entity:** University
City of entity: Marid, Community of Madrid, Spain
Student: Marina Castellanos Nicolás
Date of reading: 18/06/2018

6 **Project title:** Aplicación de geolocalización y aviso en caso de emergencia
Type of project: Master's degree final project (TFM, Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Alberto Martín Manso
Obtained qualification: 8
Date of reading: 15/09/2017

7 **Project title:** Protección de la privacidad en la gestión de eventos de calendario en la nube
Type of project: Master's degree final project (TFM, Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Rodrigo Xavier Pico Paredes
Obtained qualification: 9
Date of reading: 11/07/2017

8 **Project title:** Estudio del ransomware en dispositivos móviles Android análisis y contramedidas
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Albert Soler Colomé
Obtained qualification: 9
Date of reading: 12/06/2017

9 **Project title:** Ransomware: análisis y contramedidas
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Jorge Antonio Ruíz Muñoz
Obtained qualification: 8
Date of reading: 12/06/2017

10 **Project title:** Development of a software infrastructure for the secure distribution of documents using free cloud storage (Awarded as third best student project in the Spanish National Cybersecurity Conference http://2017.jnic.es/wp/?page_id=67)
Type of project: Trabajo Fin de Máster (Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Alejandro Sánchez Gómez
Obtained qualification: 10
Date of reading: 15/06/2016
Quality recognition: Yes **Date of award:** 31/05/2017

11 **Project title:** Desarrollo de una infraestructura para el escaneado y clasificación de documentos mediante dispositivos móviles inteligentes
Type of project: Master's degree final project (TFM, Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Natalia Roales González
Obtained qualification: 7,4
Date of reading: 27/02/2017

12 **Project title:** ROBÓTICA EN DEFENSA Y SEGURIDAD: ANÁLISIS DE SEGURIDAD
Type of project: Master's degree final project (TFM, MÁSTER EN EVIDENCIAS DIGITALES Y LUCHA CONTRA EL CIBERCRIMEN)
Entity: Insituto de Ciencias Forenses y Seguridad **Type of entity:** University
Student: Eva Rosario Martín Ibáñez
Date of reading: 20/12/2016

13 **Project title:** Generación de contraseñas de un sólo uso mediante móviles Android
Type of project: Trabajo Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Alberto Cabello Álvarez
Obtained qualification: 8,4

Date of reading: 18/07/2016

14 **Project title:** Diseño e implementación de un sistema para la recogida de logs en sistemas distribuidos
Type of project: Trabajo Fin de Grado (Doble Grado en Matemáticas e Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Mounaime Mellouk
Obtained qualification: 9
Date of reading: 12/07/2016

15 **Project title:** Diseño de una plataforma para el control de tiempo de acceso a recursos en sistemas distribuidos
Type of project: End of course project
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Javier López Andradas
Obtained qualification: 8
Date of reading: 11/07/2016

16 **Project title:** Desarrollo de un esquema de autenticación basado en la identidad para clientes Android
Type of project: Trabajo Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Juan Manuel Donaire Felipe
Obtained qualification: 9,2
Date of reading: 10/06/2016

17 **Project title:** Diseño de una herramienta para la gestión de pistas deportivas
Type of project: Trabajo Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid
Student: Jorge Yubero Cabronero
Obtained qualification: 9
Date of reading: 07/06/2016

18 **Project title:** Diseño e implementación de una aplicación web para el análisis centralizado de logs de seguridad
Type of project: Trabajo de Fin de Máster (Máster en Ingeniería Informática + Máster en Investigación e Innovación en Tecnologías de la Información y las Comunicaciones))
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Carlos López Cruces
Obtained qualification: 6,5
Date of reading: 19/02/2016

19 **Project title:** Diseño e implementación de un agente móvil Android para medir la Quality of Service de los operadores de telefonía móvil
Type of project: Trabajo Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Christian Ramos Maroto
Obtained qualification: 7,5
Date of reading: 08/02/2016

20 **Project title:** Desarrollo de un sistema MDM para monitorización de dispositivos móviles Android
Type of project: Trabajo Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: José María Pérez Rodríguez-Cadarso
Obtained qualification: 8,5

Date of reading: 13/07/2015

21 **Project title:** Diseño de un sistema de gestión segura de eventos en la nube (Awarded as best student project by itSMF, Spain https://tinyurl.com/ya2qbmbd)
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Rodrigo Xavier Pico Paredes
Obtained qualification: 7,5
Date of reading: 13/07/2015

22 **Project title:** Criptografía basada en emparejamientos: motivación, estudio y aplicaciones prácticas
Type of project: Trabajo de Fin de Grado (Doble Grado en Matemática e Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Laura Ramírez Lapeña
Obtained qualification: 9,3
Date of reading: 17/06/2015

23 **Project title:** Diseño e implementación de un sistema para el escaneado de documentos mediante un cliente Android
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Aristeo Mateos Rodríguez
Obtained qualification: 9
Date of reading: 17/06/2015

24 **Project title:** Estudio del problema de la distribución de claves criptográficas en el contexto de las tecnologías cloud (Awarded as best student project by itSMF, España, 2015, https://tinyurl.com/yckojko8)
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Alejandro Sánchez Gómez
Obtained qualification: 9.3
Date of reading: 17/07/2014
Quality recognition: Yes **Date of award:** 27/05/2015

25 **Project title:** Design and implementation of secure protocols for practical authentication and fair anonymity systems
Type of project: Doctoral thesis
Co-director of thesis: Francisco de Borja Rodríguez Ortiz
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Jesús Díaz Vico
Obtained qualification: Sobresaliente
Identify key words: Software; Computation and discrete mathematics; Computer network; Computer crime; Personal data; Data protection
Date of reading: 12/05/2015
European doctorate: Yes

26 **Project title:** Estudio de procedimientos de autenticación multicanal basados en dispositivos móviles con sistema operativo Android
Type of project: Trabajo de Fin de Máster (Máster en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid
City of entity: Madrid, Community of Madrid, Spain

Student: Nicolás Mertanen Cuní
Obtained qualification: 9.5
Date of reading: 02/10/2014

27 **Project title:** Desarrollo de una política de seguridad para el uso de aplicaciones Android en un contexto empresarial
Type of project: Trabajo de Fin de Grado (Grado en Ingenería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Borja Simancas Ruesgas
Obtained qualification: 7.7
Date of reading: 17/07/2014

28 **Project title:** Estudio de mecanismos de autenticación basados en contraseñas visuales en dispositivos móviles Android
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Mario González Nahón
Obtained qualification: 7.5
Date of reading: 22/05/2014

29 **Project title:** Gestión de documentos en entornos colaborativos mediante un cliente Android
Type of project: Trabajo de Fin de Grado (Grado en Ingeniería Informática)
Entity: Universidad Autónoma de Madrid **Type of entity:** University
Student: Ignacio del Pozo Martínez
Obtained qualification: 9
Date of reading: 07/02/2014

Participation in innovative teaching projects

1 **Project title:** ChalkPy2.0: Extensión de la herramienta ChalkPy para la presentación de contenidos matemáticos mediante dispositivos móviles
Type of participation: Co-ordinator
Funding entity: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 01/09/2015 - 30/06/2016

2 **Project title:** ChalkPy: Una herramienta para mejorar la presentación de contenidos matemáticos en el aula
Type of participation: Others
Name of the main researcher: Luis Fernando Lago Fernández
Funding entity: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 16/07/2014 - 31/12/2014

3 **Project title:** Autenticación mediante smartcard y autenticación anónima en la plataforma interactiva Moodle
Type of participation: Others
Time of working relationship: For a limited time
Funding entity: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 06/05/2013 - 31/12/2013

4 **Project title:** Autenticación avanzada de usuarios en Moodle: autenticación mediante DNIe y autenticación anónima
Type of participation: Others

Time of working relationship: For a limited time
Funding entity: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 14/06/2012 - 31/12/2012

5 **Project title:** Protección de la privacidad y de la información en el sistema de e-learning Moodle
Type of participation: Others
Time of working relationship: For a limited time
Funding entity: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 06/05/2011 - 31/12/2011

Other activities/achievements not included above

1 **Description of the activity:** Coordinador de la asignatura del Máster de Ingeniería Informática "Internet y Redes Avanzadas" en los cursos 2016-17 y 2017-18
Organising entity: Universidad Autónoma de Madrid
End date: 03/07/2018

2 **Description of the activity:** Creación de un MOOC en la plataforma Edx-UAM: https://www.edx.org/course/jugando-con-android-aprende-programar-tu-uamx-android301x. 6 ediciones desde abril de 2015 a diciembre de 2017
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
End date: 12/04/2017

3 **Description of the activity:** Coordinador de Prácticas de Sistemas Operativos, 2º Curso del Grado de Ingenería Informática de la UAM
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
End date: 01/05/2016

4 **Description of the activity:** Coordinador de Prácticas de Sistemas Operativos, 2º Curso del Grado de Ingenería Informática de la UAM
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
End date: 01/05/2015

5 **Description of the activity:** Coordinador de la asignatura Proyecto de Programación (1º, Grado Ingeniería Informática)
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
End date: 13/05/2013

6 **Description of the activity:** Coordinador de la asignatura Proyecto de Programación (1º, Grado Ingeniería Informática)
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
End date: 13/05/2012

Scientific and technological experience

Scientific or technological activities

R&D projects funded through competitive calls of public or private entities

1 **Name of the project:** SafeHorizon: Innovations in Detecting and Disrupting Crime-as-a-Service Operations (101168562)
Geographical area: European Union
Degree of contribution: Scientific coordinator
Entity where project took place: CSIC
Name principal investigator (PI, Co-PI....): David Arroyo Guardeño; Sara Degli Esposti
Name of the programme: HORIZON-CL3-2023-FCT-01-05
Start-End date: 02/09/2024 - 31/08/2026

2 **Name of the project:** Quantum-oriented Update to Browsers and Infrastructures for the PQ Transition (QUBIP)
Entity where project took place: CSIC
Name principal investigator (PI, Co-PI....): Piedad Brox Jiménez; Verónica Fernández Mármol; David Arroyo Guardeño
Funding entity or bodies:
Horizon Europe

Name of the programme: HORIZON-CL3-2022-CS-01-03 - Transition towards Quantum-Resistant Cryptography
Start-End date: 01/09/2023 - 31/08/2026
Total amount: 5.041.091,25 € **Sub-project amount:** 117.273,74 €
Dedication regime: Part time
Applicant's contribution: Standardization of postquantum cryptography and design of hybrid encryption schemes

3 **Name of the project:** GO IT!
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Funding entity or bodies:
Horizon Europe

Start-End date: 01/09/2022 - 31/08/2025
Total amount: 1.993.340 € **Sub-project amount:** 183.380,15 €

4 **Name of the project:** IA explicable para desinformación y detección de conspiración durante infodemias (XAI- DisInfodemics)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Name principal investigator (PI, Co-PI....): David Arroyo Guardeño
Name of the programme: PROYECTOS DE I+D+I EN LÍNEAS ESTRATÉGICAS
Code according to the funding entity: Agencia Estatal de Investigación de España
Start-End date: 01/12/2021 - 30/11/2024

Total amount: 419.876,5 € **Sub-project amount:** 51.578 €
Applicant's contribution: CSIC's PI in the project.

5 **Name of the project:** SPIRS: Secure Platform for ICT systems Rooted at the Silicon manufacturing process
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Piedad Brox Jiménez; David Arroyo
Funding entity or bodies:
Comisión Europea **Type of entity:** H2020

Name of the programme: SU-ICT-02-2020 - Building blocks for resilience in evolving ICT systems
Start-End date: 01/10/2021 - 30/09/2024
Total amount: 5.041.091,25 € **Sub-project amount:** 261.287 €
Applicant's contribution: ITEFI's PI in the project

6 **Name of the project:** Protocolos, Mecanismos y Tecnologías Pre y Postcuánticas para la Ciberseguridad y la Privacidad. P2QProMeTe
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Luis Hernández Encinas; Agustín Martín Muñoz
Nº of researchers: 7
Funding entity or bodies:
Programa Estatal de I+D+i Orientada a los Retos de la Sociedad (AEI)

Start-End date: 01/09/2021 - 31/08/2024
Total amount: 101.640 €

7 **Name of the project:** ORACLE: Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to serve Future Connected Societies
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Luis Hernández Encinas
Nº of researchers: 4
Funding entity or bodies:
EIG CONCERT-Japan 7th Joint Call ICT for Resilient, Safe and Secure Society

Start-End date: 01/04/2021 - 01/03/2024
Total amount: 511.000 € **Sub-project amount:** 120.000 €

8 **Name of the project:** Cybersecurity, Network Analysis and Monitoring for the Next Generation Internet (CYNAMON)
Geographical area: Regional
Degree of contribution: IP del Grupo de Investigación del CSIC
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Nº of researchers: 5
Funding entity or bodies:
Programas operativos del Fondo Social Europeo y del Fondo Europeo deDesarrollo Regional, 2014-2020, de la Comunidad de Madrid

Type of participation: Principal investigator
Start-End date: 01/01/2019 - 31/12/2022
Participating entity/entities: Consejo Superior de Investigaciones Científicas; Universidad Autónoma de Madrid; Universidad Carlos III de Madrid (coordinador); Universidad Rey Juan Carlos
Total amount: 885.500 € **Sub-project amount:** 185.226,46 €

9 **Name of the project:** TRESCA: Trustworthy, Reliable and Engaging Scientific Communication Approaches (Grant agreement ID: 872855)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Name principal investigator (PI, Co-PI....): Sara Degli Esposti; David Arroyo Guardeño
Funding entity or bodies:
Comisión Europea **Type of entity:** H2020-SwafS-2019-1

Start-End date: 01/01/2020 - 30/04/2022
Total amount: 253.218 €
Applicant's contribution: ITEFI'S PI in the project

10 **Name of the project:** Advancing in cybersecurity technologies
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Piedad Brox Jiménez; David Arroyo
Funding entity or bodies:
Programa i-LINK (CSIC)

Start-End date: 01/01/2020 - 31/12/2021
Total amount: 23.738 €

11 **Name of the project:** Criptografía para Optimizar la Privacidad y la CIberSeguridad (COPCIS)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Luis Hernández Encinas; Amparo Fuster Sabater
Funding entity or bodies:
Ministerio de Economía, Industria y Competitividad

Start-End date: 01/01/2018 - 31/12/2020
Total amount: 93.533 €

12 **Name of the project:** New Rules for Assessing Mathematical Competences (RULES_MATH)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Nº of researchers: 4
Name of the programme: Erasmus+
Start-End date: 01/09/2017 - 31/08/2020
Participating entity/entities: Czech Technical University in Prague (República Checa); Dublin Institute of Technology (Irlanda); Gazi University (Turquia); Slovak University of Technology in Bratislava (Slovakia); Technical University of Civil Engineering Bucharest (Rumanía); Universidad de Salamanca; University of Plovdiv (Bulgaria)
Total amount: 33.535 €

13 **Name of the project:** CIBERDINE: ciberseguridad, datos, información y riesgos (Cybersecurity: Data, Information, Risks)

Entity where project took place: Universidad Autónoma de Madrid **Type of entity:** University

Name principal investigator (PI, Co-PI....): Arturo Ribagorda Garnacho; David Camacho Fernández; Luis Hernández Encinas

Funding entity or bodies:

Comunidad de Madrid **Type of entity:** Dirección General de Universidades e Investigación

City funding entity: Madrid, Community of Madrid, Spain

Start-End date: 01/10/2014 - 01/10/2018

Participating entity/entities: Consejo Superior de Investigaciones Científicas; Universidad Autónoma de Madrid; Universidad Carlos III de Madrid

Total amount: 545.100 €

Applicant's contribution: Cyberspace plays a key role in modern societies and economies. Over the last decade Internet has changed the way we interact with Public Administrations, has given rise to new business and entertainment models and influenced the way we communicate. However, as acknowledged by the National Security Strategy, cyberspace is nowadays an open and uncontrolled space. The complexity and globalization of cyberattacks has increased very significantly in the last years, causing an important breach between the capabilities of attackers and defenders. This project aims at strengthening our capabilities to prevent, detect, and respond to cyberattacks by developing techniques that improve situational awareness and cater for a dynamic threat management. To do so, we propose an interdisciplinary research program that tackles three important challenges in cybersecurity research. Firstly, interdependences among networks and information systems are forcing us to adopt cooperative strategies where entities of a very different nature exchange information about vulnerabilities, threats, actors, tactics, ongoing incidents, countermeasures, etc. However, organizations are extremely reluctant to openly share such information. This calls for models and technologies that facilitate sharing by determining what to share, when, with whom, as well as reasoning about the repercussions of sharing confidential data. Secondly, an improved defense capability requires a deeper and more intelligent analysis of all events that take place in the network. This requires to adapt, and develop where necessary, Big Data technologies to analyze massive amounts of security-related information. Finally, an effective threat management system needs to put in context available information, automatically derive dynamic risk levels for all systems, and support decisions about the selection and deployment of optimal countermeasures.

14 **Name of the project:** Computación en ciclo cerrado: de la neurociencia a la tecnología (Closed-loop computating: from neuroscience to technology)

Entity where project took place: Universidad Autónoma de Madrid **Type of entity:** University

Name principal investigator (PI, Co-PI....): Pablo Varona

Nº of researchers: 6

Start-End date: 01/01/2016 - 31/08/2018

Total amount: 137.093 €

Applicant's contribution: Information processing in the nervous system relies to a large extent in closed-loop feedback. These informational loops exist from the molecular level all the way up to the cognitive level in the human brain. Throughout these levels there exists a large diversity of coupled information dynamics. In this project we propose the study, characterization and use as a source of bio-inspiration of closed-loop computing at several spatial and temporal scales in the nervous system. We will focus our study in its transient dynamics addressing the mechanisms for robustness, flexibility, stability and efficacy in information coding, coordination, creation and execution during closed-loop computing. To achieve this goal, we propose to develop theoretical and technical tools, experimental protocols based in the technology of the real time dynamical observer/controller, and methodology for online and offline analysis to reveal fundamental aspects of transient dynamics of closed-loop computing in the experimental models available in our lab. Finally, we propose the knowledge transfer to technology that will employ bio-inspired closed-loop computing in the context of machine olfaction, autonomous locomotion in robotics and human-machine and brain-machine interfaces.

15 **Name of the project:** Ciclos cerrados de estimulación-respuesta para la interacción bidireccional y multiescala con el sistema nervioso (TIN2012-30883) (Stimulus-response closed-loops for bidirectional and multiscale interaction with the nervous system)

Entity where project took place: Universidad Autónoma de Madrid **Type of entity:** University

City of entity: madrid, Community of Madrid, Spain

Name principal investigator (PI, Co-PI....): Pablo Varona Martínez

Nº of researchers: 6

Funding entity or bodies:

MINECO

Type of participation: Investigador colaborador

Start-End date: 01/01/2013 - 31/12/2017

Total amount: 112.409 €

Applicant's contribution: This multidisciplinary proposal aims to continue and extend the research lines opened by the Biological Neurocomputation Group (GNB) at Universidad Autónoma de Madrid in the field of Computational Neuroscience. We propose a theoretical and experimental study of the bidirectional interaction with the nervous system through closed-loop, activity-dependent, stimulus-response protocols. This interaction has a double goal: (i) to extract information to characterize information processing otherwise hidden under traditional stimulation protocols and (ii) to control biological activity or to control a device that uses this activity. Our research will be carried out in different systems and levels of description in order to find general principles and specific aspects within each of them. We will use offline and online event detection tools to characterize and analyze time series, mathematical and computational models of neural activity to build representations of the dynamics and make predictions to drive the closed-loop, tools for adaptive stimulus exploration, and experiments drawn from our theoretical and technical work. For this goal, we will develop a technology called Real Time Dynamical Observer/Controller to implement advanced protocols of neural activity-dependent stimulation. This technology will allow to probe different temporal scales and hierarchies present in transient sequential dynamics in in vitro and in vivo setups to determine its functionality, to control natural and pathological states of these dynamics, and to manage bidirectional interactions between recording/stimulation devices and the nervous system in real time. The results of this research will contribute to the understanding of several mechanisms of complex information processing by the nervous system, with implications in medicine, which will be transferred to the design of new paradigms of artificial neural networks, robotics, biomimetic or neuromorphic devices, prosthetic devices and brain-machine interfaces.

16 **Name of the project:** Monitorización continua y análisis de entornos industriales y habitados con redes de sensores de bajo coste (Continuous monitorization and analysis of industrial and inhabited environ- ments by means of a network of low cost sensors)

Entity where project took place: Universidad Autónoma de Madrid **Type of entity:** University

Funding entity or bodies:

BANCO SANTANDER, S.A.

City funding entity: Spain

Name of the programme: 2ª convocatoria de Proyectos de Cooperación Interuniversitaria UAM-Banco Santander con Estados Unidos

Start-End date: 31/07/2013 - 31/12/2014

Participating entity/entities: Universidad Autónoma de Madrid; Universidad de California en San Diego (Estados Unidos))

17 **Name of the project:** Estudio de los correlatos neurales de la memoria de trabajo emocional y del efecto de la aplicación de un sistema de entrenamiento asistido (Study of neural correlations in emotional working memory and the effect of applying a assisted training system)

Entity where project took place: Universidad Autónoma de Madrid **Type of entity:** University

City of entity: madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Luis Carretié Arangüena
Funding entity or bodies:
Primera Convocatoria Propia de Proyectos de Investigación Multidisciplinares de la Universidad Autónoma de Madrid
Type of entity: University
City funding entity: madrid, Community of Madrid, Spain

Type of participation: Investigador colaborador
Start-End date: 01/05/2012 - 30/04/2013
Participating entity/entities: Universidad Autónoma de Madrid
Applicant's contribution: The present project proposes the cooperation, potentially long-termed, among researches of the Facultad de Psicología, of the Escuela Politécnica Superior, and of the Facultad de Medicina familiarized with different aspects of the Neurosciences, with the general scope of studying emotional working memory. This cooperation, which will mutually enrich all the groups involved in the proposal and will allow a sinergical approach to this psychological process so important in adaptive terms, will involve three phases. In the first one the scope is the characterization of the neural substrates underlying emotional working memory through the recording of electroencephalographic, magnetocencephalographic and haemodynamic activity during an n-back task, which typically activates working memory-related processes. In its emotional modality, the n-back task is directed towards neutral and emotional material (affective pictures). The second phase, based in the characterization provided in the first one, is aimed to design an aided training system regarding the emotional n-back task employing the Real Time Dynamical Observer technology. This system provides online feedback to the individual on the levels which those neural parameters defined in Phase 1 as good indexes of working memory present at each moment, so that he/she receives rapid and simple information on them during the execution of the n-back task. In the third phase, the scope is the validation of the aided training system designed in phase 2 so its efficiency as a potential learning tool is contrasted. Moreover, the application of the aided training to part of the subjects who participated in phase 1 will allow us to observe those change- or plasticity- processes which are a consequence of training. In this same phase we also plan to apply this new training system to Parkinson patients, who show disfunctions affecting working memory and emotion recognition processes. This applied study pretends to open a novel research line within the study of strategies that improve the quality of life on individuals suffering diseases affecting their cognitive and affective processes.

18 **Name of the project:** Observadores dinámicos en tiempo real para el estudio de actividad neuronal transitoria (BFU 2009-08473) (Real-time dynamical observer for studying transient neural activity)
Geographical area: National
Degree of contribution: Researcher
Entity where project took place: Universidad Autónoma de Madrid
Type of entity: University
City of entity: madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Pablo Varona Martínez
Funding entity or bodies:
Ministerio de Ciencia y Tecnología de España
City funding entity: madrid, Community of Madrid, Spain

Start-End date: 01/01/2011 - 31/12/2012
Participating entity/entities: Universidad Autónoma de Madrid
Dedication regime: Full time

19 **Name of the project:** Estudio del procesamiento de información en peces eléctricos mediante protocolos dinámicos de estimulación dependiente de comportamiento (Study of information processing in electric fishes by means of adaptive and activity dependent protocols)
Entity where project took place: Universidad Autónoma de Madrid
Type of entity: University
City of entity: madrid, Community of Madrid, Spain

Name principal investigator (PI, Co-PI....): Francisco de Borja Rodríguez Ortiz
Funding entity or bodies:
7ª Convocatoria de PROYECTOS DE COOPERACIÓNINTERUNIVERSITARIA UAM-SANTANDER con América Latina **Type of entity:** Foundation
City funding entity: madrid, Community of Madrid, Spain

Type of participation: Investigador colaborador
Start-End date: 01/06/2011 - 31/05/2012
Participating entity/entities: São Carlos; Universidad Autónoma de Madrid; Universidade de São Paulo

20 **Name of the project:** Cuántica y Caos (CUCO): algoritmos criptográficos de frontera (MTM2008-02194)??(Quantum information and chaos: frontier cryptographics algorithms)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Gonzalo Álvarez Marañón
Funding entity or bodies:
Ministerio de Ciencia y Tecnología de España

Type of participation: Investigador colaborador
Start date: 2008
Participating entity/entities: Consejo Superior de Investigaciones Científicas

21 **Name of the project:** Nuevos protocolos de seguridad y algoritmos criptográficos para la protección de servicios telemáticos (TSI2007-62657)-(New security protocols and cryptographic algorithm to protect telematic services)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Fausto Montoya Vitini??
Funding entity or bodies:
Ministerio de Industria Turismo y Comercio **Type of entity:** Ministerio
City funding entity: Madrid, Community of Madrid, Spain

Type of participation: Investigador colaborador
Start date: 2007
Participating entity/entities: Consejo Superior de Investigaciones Científicas

22 **Name of the project:** Evaluación de protocolos y algoritmos de seguridad en sistemas de información (SEG2004-02418) (Evaluation of protocols and algorithms for the security of information systems)
Entity where project took place: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City of entity: madrid, Community of Madrid, Spain
Name principal investigator (PI, Co-PI....): Fausto Montoya Vitini
Funding entity or bodies:
Ministerio de Ciencia y Tecnología de España

Type of participation: Investigador colaborador
Start date: 2004 **Duration:** 3 years
Participating entity/entities: CSIC; Politécnica de Madrid y Salamanca; Universidades de Málaga

R&D non-competitive contracts, agreements or projects with public or private entities

1 **Name of the project:** Diseño de una capa blockchain para el registro y supervisión de eventos relacionados con la cadena de producción y distribución agroalimentaria.
Name principal investigator (PI, Co-PI....): David Arroyo Guardeño
Nº of researchers: 1
Funding entity or bodies:
IMIDRA

Start date: 04/03/2024
Total amount: 72.600 €

2 **Name of the project:** Desarrollo de protocolos criptográficos y de blockchain para la gestión de verificación remota y securización de gemelos digitales frente al vector de amenazas asociado a la computación cuántica
Degree of contribution: Coordinator of total project, network or consortium
Funding entity or bodies:
Enzyme S.L.

Start date: 21/12/2022 **Duration:** 3 years
Total amount: 175.619,4 €

3 **Name of the project:** Desarrollo para una capa de la gestión descentralizada de la identidad mediante blockhain en el marco de la aplicación Zerel
Degree of contribution: Coordinator of total project, network or consortium
Funding entity or bodies:
TheBasement S.L.

Start date: 01/03/2022 **Duration:** 1 year
Total amount: 72.600 €

4 **Name of the project:** Auditoría de elementos criptográficos (bibliotecas y funcionalidad) del proyecto NEO
Nº of researchers: 1
Funding entity or bodies:
Red4Sec Cybersecurity

Start date: 04/11/2019 **Duration:** 1 month
Total amount: 4.500 €

5 **Name of the project:** Informe sobre protocolos de conocimiento nulo y sus aplicaciones a los esquemas de voto electrónico y por internet
Nº of researchers: 1
Funding entity or bodies:
Consejo Superior de Investigaciones Científicas **Type of entity:** State agency

Start date: 15/06/2017 **Duration:** 2 months
Total amount: 3.000 €

6 **Name of the project:** Informe sobre las firmas electrónicas no convencionales
Nº of researchers: 1
Funding entity or bodies:
Consejo Superior de Investigaciones Científicas **Type of entity:** State agency

Start date: 15/04/2017 **Duration:** 2 months
Total amount: 3.000 €

7 **Name of the project:** WE NOSE_ Wireless Electronic NOSE (Nariz Artificial Inalámbrica), IPT-2011-0727-020000 (WE NOSE_ Wireless Electronic Nose)
Name principal investigator (PI, Co-PI....): Pablo Varona Martínez (subproyecto UAM; Coordinador ABACCUS)
Nº of researchers: 4
Participating entity/entities: ABACCUS SOLUCIONES E INNOVACIÓN SL; BIOINGENIERIA MEDIOAMBIENTAL; DEUTECNO NOSES; Universidad Autónoma de Madrid; Universidad Rey Juan Carlos
Funding entity or bodies:
MICINN

Start date: 01/06/2011 **Duration:** 1 year

8 **Name of the project:** SEGUR@: Seguridad y Confianza en la Sociedad de la Información (Security and Trust in Information Society)
Degree of contribution: Proyecto CENIT
Name principal investigator (PI, Co-PI....): Luis Hernández Encinas
Participating entity/entities: Alcatel-Lucent en España; Atos Origin; Caja de Ahorros de Navarra; Ericsson; Garrigues Abogados; Instituto de Física Aplicada del CSIC; Isdefe; Panda Software; S21Sec; Safelayer; Secuware y Sermepa??; Telefónica I+D
Funding entity or bodies:
Centro para el Desarrollo Tecnológico Industrial **Type of entity:** Business
City funding entity: Madrid, Community of Madrid, Spain

Ministerio de Industria Turismo y Comercio **Type of entity:** -
City funding entity: Madrid, Community of Madrid, Spain

Start date: 2007 **Duration:** 3 years

9 **Name of the project:** HESPERIA: Homeland sEcurity: tecnologíaS Para la sEguridad integRal en espacIos públicos e infrAestructuras?????
Degree of contribution: Proyecto CENIT
Name principal investigator (PI, Co-PI....): Ámparo Fúster Sabater
Participating entity/entities: BrainStorm; Instituto de Física Aplicada del CSIC; SAC y Technosafe; Soluziona Consultoría y Tecnología; Tecnobit; Unión Fenosa; Visual-Tools
Funding entity or bodies:
Centro para el Desarrollo Tecnológico Industrial: (CDTI) del Ministerio de Turismo

Industria y Comercio de España

Start date: 2006

Scientific and technological activities

Scientific production

H index: 15
Date of application: 11/02/2024

Publications, scientific and technical documents

1 Jesus Diaz; Seung Geol Choi; David Arroyo; Angelos D. Keromytis; Francisco B. Rodriguez; Moti Yung. A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions. Advances in Cyber Security: Principles, Techniques, and Applications. pp. 143 - 183. Springer, 2019. Available on-line at: <https://doi.org/10.1007/978-981-13-1483-4_7>.
Type of production: Book chapter **Format:** Book
Corresponding author: No
Relevant publication: Yes

2 Gonzalo Alvarez; José María Amigó; David Arroyo; Shujun Li. Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers. 354, pp. 257 - 295. Springer Berlin Heidelberg, 2011. Available on-line at: <http://dx.doi.org/10.1007/978-3-642-20542-2_8>. ISBN 978-3-642-20541-5
Type of production: Book chapter **Format:** Book
Source of citations: Google Scholar **Citations:** 37

Relevant results: The authors of this book chapter are shown in alphabetic order. I contributed to this chapter book as author and coordinator of the writing. This book chapter comprises the main conclusions of our research in chaos-based cryptography. According to Google Scholar, it has been referenced 18 times. This book chapter summarizes all our cryptanalysis works, but also presents a set of rules to design chaos-based cryptography according to the general framework of conventional cryptography. Chaos is introduced in cryptography to define new strategies of confusion and diffusion of information. Our work in the field of chaotic cryptography provides a set of procedures to test if chaotic dynamics do really lead to those confusion and diffusion properties. Furthermore, those procedures are of practical nature, since they allow to confirm what cryptography expects and demands from cryptography in a practical environment, i.e., when working with finite precision arithmetic. In our work we proposed a set of mathematical indicators to assess “the distance” between the “factual” chaotic behavior and the requirements of cryptography. In a practical environment chaos cannot be assumed without previous evaluation, but also it cannot be assumed that chaos embodies confusion and diffusion properties unless a careful examination is performed.
Relevant publication: Yes

3 Juha Nurmi; Arttu Paju; Billy Bob Brumley; Tegan Insoll; Anna K. Ovaska; Valeriia Soloveva; Ninna Vaaranen-Valkonen; Mikko Aaltonen; David Arroyo. Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. Scientific Reports. 2024. Available on-line at: <https://www.nature.com/articles/s41598-024-58346-7>.
Type of production: Scientific paper

4 Hanane Azzaoui; Akram Zine Eddine Boukhamla; David Arroyo; Abdallah Bensayah. Developing new deep-learning model to enhance network intrusion classification. Evolving Systems. 18/01/2022. Available on-line at: <https://link.springer.com/article/10.1007/s12530-020-09364-z#citeas>.
Type of production: Scientific paper **Format:** Journal

5 Pablo de Andrés; David Arroyo; Ricardo Correia; Álvaro Rezola. Challenges of the market for initial coin offerings. International Review of Financial Analysis. 09/11/2021. Available on-line at: <https://www.sciencedirect.com/science/article/pii/S1057521921002842?via%3Dihub>.
DOI: 10.1016/j.irfa.2021.101966
Type of production: Scientific paper **Format:** Journal
Corresponding author: No

6 Achieving cybersecurity in blockchain-based systems: A survey. Future Generation Computer Systems. 11/2021. Available on-line at: <https://www.sciencedirect.com/science/article/pii/S0167739X21001576?via%3Dihub>.
Type of production: Scientific paper **Format:** Journal

7 A Compression-Based Method for Detecting Anomalies in Textual Data. Entropy. 16/05/2021. Available on-line at: <https://www.mdpi.com/1099-4300/23/5/618>.
Type of production: Scientific paper **Format:** Journal

8 Paul Kuhle; David Arroyo; Eric Schuster. Building A blockchain-based decentralized digital asset management system for commercial aircraft leasing. Computers in Industry. 126 - 103393, 11/01/2021.
Type of production: Scientific paper
Impact source: ISI **Category:** Computer science-interdisciplinary applications
Impact index in year of publication: 3.954
Position of publication: 21 **No. of journals in the cat.:** 109

9 Andres Marín-López; Sergio Chica-Manjarrez; David Arroyo; Florina Almenares-Mendoza; Daniel Díaz-Sánchez. Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain. Electronics. 9 - 11, pp. 1865. 2020, 06/11/2020. Available on-line at: <https://www.mdpi.com/2079-9292/9/11/1865>.
Type of production: Scientific paper **Format:** Journal

10 Iñigo Querejeta-Azurmendi; David Arroyo Guardeño; Jorge L. Hernández-Ardieta; Luis Hernández Encinas. NetVote: A Strict-Coercion Resistance Re-Voting Based Internet Voting Scheme with Linear Filtering. Mathematics. 8 - 9, pp. 1618. MDPI, 2020.
Type of production: Scientific paper **Format:** Journal
Corresponding author: No

11 Irene Elices; Rafael Levi; David Arroyo; F.B. Rodriguez; Pablo Varona. Robust dynamical invariants in sequential neural activity. Scientific reports. 9 - 1, pp. 9048. Springer Nature, 26/06/2019.
Type of production: Scientific paper **Format:** Journal
Corresponding author: No
Impact source: ISI **Category:** MULTIDISCIPLINARY SCIENCES
Impact index in year of publication: 4,122 **Journal in the top 25%:** Yes
Position of publication: 12 **No. of journals in the cat.:** 64

12 Gonzalo de la Torre; Luis Lago; David Arroyo. On the application of Compression Based Metrics to identifying anomalous behaviour in web traffi. Logic Journal of the IGPL. pp. In Press. 2019.
Type of production: Scientific paper
Corresponding author: No

13 David Arroyo; Fernando Hernandez; Amalia B. Orúe. Cryptanalysis of a Classical chaos-based cryptosystem with some quantum cryptography features. International Journal of Bifurcation and Chaos. 27 - 1, pp. 1750004 - 12 pages. 02/01/2017.
DOI: 10.1142/S0218127417500043

Type of production: Scientific paper
Corresponding author: Yes

Impact source: ISI
Category: MATHEMATICS, INTERDISCIPLINARY APPLICATIONS
Impact index in year of publication: 1.355
Journal in the top 25%: No
Position of publication: 46
No. of journals in the cat.: 101

Source of citations: WOS
Citations: 4

Source of citations: Google Scholar
Citations: 4

14 Víctor Gayoso Martínez; Luis Hernández Encinas; Agustín Martín Muñoz; M.A. Álvarez Mariño; David Arroyo. A comparative study of three Spanish eGoverment smart cards. Logic Jnl IGPL. 25 - 1, pp. 42 - 53. 01/08/2016. Available on-line at: <http://jigpal.oxfordjournals.org/content/early/2016/08/04/jigpal.jzw038.abstract>.
DOI: 10.1093/jigpal/jzw038
Type of production: Scientific paper

Impact source: ISI
Category: Mathematics, Applied
Impact index in year of publication: 0.434
Journal in the top 25%: No
Position of publication: 224
No. of journals in the cat.: 254

15 Jesus Diaz; David Arroyo; Francisco B. Rodríguez. A formal methodology for integral security design and verification of network protocols. Journal of Systems and Software. 89, pp. 87 - 98. 2014. Available on-line at: <http://arxiv.org/abs/1201.5666>.
Type of production: Scientific paper

Impact source: ISI
Category: COMPUTER SCIENCE, THEORY \& METHODS
Impact index in year of publication: 1.352
Journal in the top 25%: No
Position of publication: 31
No. of journals in the cat.: 102

Source of citations: WOS
Citations: 4

Source of citations: Google Scholar
Citations: 12

Relevant results: This paper is part of the Ph.D. research of Jesus Diaz, whose work I am co-supervising with Dr. Francisco Rodriguez. The goal of this paper is to fulfill a solid framework to discern whether the security requirements and assumptions of a communication protocol are valid or not. In the paper we distinguish different stages in the design process of security protocols. First, we perform an informal study of the application context (which determines a basic attack model) and the suitability of the security requirements and assumptions. Afterwards, we implement our protocol using standard (protocols and cryptographic primitives) technologies. Once we have a prototype, we proceed with the procedural analysis of the system. Here we code our protocol using formal languages according to Hoare's theory of Communicating Sequential Processes (CSP), which is applied to perform a formal evaluation of the protocol. This analysis is combined with the classical computational model for the validation of cryptographic primitives, and with the mathematical models for the communication channels associated to the exchange of messages in the protocol. In case the examination is not positive, we reformulate our assumptions and requirements, and after that the security analysis is carried out again. This process is repeated until we reach a successful report from the procedural analysis. The aims and outcomes of this work are aligned with the commitments of security-by-design and privacy-by-design, which are essential component of today information systems

16 David Arroyo; Gonzalo Alvarez. Application of Gray codes to the study of the theory of symbolic dynamics of unimodal maps. Communications in Nonlinear Science and Numerical Simulation. 19 - 7, pp. 2345 - 2353. 2014. Available on-line at: <http://arxiv.org/abs/1204.6514>.
Type of production: Scientific paper

Impact source: ISI
Category: MATHEMATICS, INTERDISCIPLINARY APPLICATIONS

Impact index in year of publication: 2.866 **Journal in the top 25%:** Yes
Position of publication: 6 **No. of journals in the cat.:** 99

Source of citations: WOS **Citations:** 1

Source of citations: Google Scholar **Citations:** 5

Relevant results: This paper provides an exhaustive theoretical conclusion of our previous works in the field of the symbolic dynamics of unimodal maps. We prove in closed mathematical form a series of previous contributions and we solve some inaccuracies in those proposals. Morevoer, we explain the consequences of our theoretical work in the context of chaotic cryptography. As first author and corresponding author I have conceived the theoretical framework, the mathematical proofs, and the writing of the first manuscript. I have also integrated all the comments from the other co-author of this paper.

17 Jesus Diaz; David Arroyo; Francisco B. Rodriguez. New X.509-based mechanisms for fair anonymity management. Computers & Security. 46, pp. 111 - 125. 2014.
Type of production: Scientific paper

Impact source: ISI **Category:** COMPUTER SCIENCE, INFORMATION SYSTEMS
Impact index in year of publication: 1.031 **Journal in the top 25%:** No
Position of publication: 69 **No. of journals in the cat.:** 139

Source of citations: WOS **Citations:** 4

Source of citations: Google Scholar **Citations:** 8

Relevant results: In this paper we show how to adapt X.509 extensions to support fair management of anonymity. The main outcomes of the paper are very relevant in the current context of ICT, where new procedures to get a tradeoff between privacy concerns and security are required. Therefore, this paper contributes to foster easy-to-use methods for the so-called Privacy Enhancing Technologies.

18 Jesus Diaz; David Arroyo; Francisco B. Rodriguez. On securing online registration protocols: formal verification of a new proposal. Knowledge-based systems. 59, pp. 149 - 158. 2014.
Type of production: Scientific paper

Impact source: ISI **Category:** COMPUTER SCIENCE, ARTIFICIAL INTELLIGENCE
Impact index in year of publication: 2.947 **Journal in the top 25%:** Yes
Position of publication: 16 **No. of journals in the cat.:** 123

Source of citations: WOS **Citations:** 0

Source of citations: Google Scholar **Citations:** 2

Relevant results: This paper introduces a registration protocol for distributing digital identities. As an important component of the paper, we analyze the security properties of the proposed protocol using Proverif, i.e., a tool for the formal verification of security protocols. We also highlighted the different steps involved in the design of security protocols, and we take special attention in pointing out the security breaches that we have detected along the protocol implementation and how we have proceeded to solve them. This paper is part of the Ph.D thesis of Jesus Diaz, whose work I am co-supervising with Dr. Rodriguez.

19 David Arroyo; Roberto Latorre; Pablo Varona; Francisco B. Rodriguez. Application of symbolic dynamics to characterize coordinated activity in the context of biological neural networks. Journal of the Franklin Institute. 350 - 10, pp. 2967 - 2981. Elsevier, 2013.
Type of production: Scientific paper

Impact source: ISI **Category:** AUTOMATION \& CONTROL SYSTEMS
Impact index in year of publication: 2.26 **Journal in the top 25%:** Yes
Position of publication: 13 **No. of journals in the cat.:** 59

Source of citations: WOS **Citations:** 1

Source of citations: Google Scholar **Citations:** 2

Relevant results: As first author and corresponding author, I proposed the theoretical framework and the analysis tool, along with the first version of the manuscript. I have also coordinated the simulations, the data analsysis, and the different versions of the paper as result of the contributions/comments of the rest of co-authors. In this work we analyze the coordinated activity of a Central Pattern Generator. The paper uses as main tool the applied theory of symbolic dynamics to study the dynamics of two Central Pattern Generators built upon two different mathematical models for the underlying neurons. By means of the ordinal analysis of time series, we identify the different rhythms sustained by the cooperation among the different neurons of the considered Central Pattern Generators. Along the paper we show the suitability of symbolic dynamics to conduct event detection, which is very relevant for the further construction of procedures to identify hidden information flows and to reconstruct dynamics and states from partial observations.

20 David Arroyo; Jesus Diaz; Francisco de Borja Rodriguez. Cryptanalysis of a one round chaos-based Substitution Permutation Network. Signal Processing. 93 - 5, pp. 1358 - 1364. Elsevier, 2013. Available on-line at: <http://dx.doi.org/10.1016/j.sigpro.2012.11.019>.

Type of production: Scientific paper **Format:** Journal

Corresponding author: Yes

Impact source: ISI **Category:** ENGINEERING, ELECTRICAL & ELECTRONIC

Impact index in year of publication: 2.238 **Journal in the top 25%:** Yes

Position of publication: 51 **No. of journals in the cat.:** 248

Source of citations: WOS **Citations:** 35

Source of citations: Google Scholar **Citations:** 51

Relevant results: Brief summary of my participation in this paper: As first author and corresponding author, I proposed a scheme to analysis a cryptosystem based on the logistic map and one-round Substitution Permutation Network. The first version of the manuscript and the cryptanalasys were further improved according to the suggestions of the co-authors, begin coordinated all the changes by the first author. Along the paper we discussed the link between the topological and metric properties of chaotic maps and the requirements of encryption schemes. We highlighted that a thorough analysis of the properties of chaotic maps (by means of the topological entropy, Lyapunov exponents, statistical distances, etc.) must be performed before being considered as core of a cryptosystem. Furthermore, chaotic systems does not eliminate by themselves security problems of flawed encryption architectures, which is the case of one-round Substitution Permutation Networks. This being the case, we applied a chosen plaintext attack to prove the weaknesses of a chaotic one-round Substitution Permutation Network.

21 David Arroyo; Pablo Chamorro; José María Amigó; Francisco B. Rodriguez; Pablo Varona. Event detection, multimodality and non-stationarity: ordinal patterns, a tool to rule them all?. European Physical Journal Special Topics. 222 - 2, pp. 457 - 472. 2013.

Type of production: Scientific paper

Impact source: ISI **Category:** PHYSICS, MULTIDISCIPLINARY

Impact index in year of publication: 1.796 **Journal in the top 25%:** No

Position of publication: 23 **No. of journals in the cat.:** 83

Source of citations: WOS **Citations:** 5

Source of citations: Google Scholar **Citations:** 6

Relevant results: As first author and corresponding author, I have developed the theoretical framework used in this paper. I performed the analysis of the experimental data, I wrote the first version of the manuscript, and I coordinated all the changes introduced in the first draft by processing the comments and suggestions of all co-authors and reviewers. With respect to the content of the paper, it is centered on the application of ordinal time series analysis to event detection of neurophysiological data. We extend our previous results on the applied theory

of symbolic dynamics in order to analysis intra- and extra-cellular time series. The goal is first the identification of events, and second the detection of correlation between voltage and calicum time series. We underline the limitations of our framework and propose some solutions to overcome them.

22 María José García Martinez; Natalia Denisenko; Diego Soto; David Arroyo; Amalia Beatriz Orue; Agustin Martin; Veronica Fernandez. High-speed free-space quantum key distribution system for urban daylight applications. Applied Optics. 52 - 14, pp. 3311 - 3317. 2013.

Type of production: Scientific paper

Impact source: ISI
Category: Optics
Impact index in year of publication: 1.689
Journal in the top 25%: No
Position of publication: 29
No. of journals in the cat.: 80

Source of citations: WOS
Citations: 12

Source of citations: Google Scholar
Citations: 22

Relevant results: In this paper we introduce a free space channel for quamtum key distribution. My role in this paper has been focused on the data analysis, the study of possible security weaknesses (that were solved during the configuration of the experimental setup), and the design and improvement of the system for the detection of errors in the receiver. I have also contributed in the writting of the different versions of the manuscript.

23 Pablo Chamorro; Carlos Muñiz; Rafael Levi; David Arroyo; Francisco B. Rodriguez; Pablo Varona. Generalization of the Dynamic Clamp Concept in Neurophysiology andBehavior. PLoS ONE. 7 - 7, pp. e40887 - e40887. Public Library of Science, 2012. Available on-line at: <http://dx.doi.org/10.1371%2Fjournal.pone.0040887>.

Type of production: Scientific paper
Format: Journal

Impact source: ISI
Category: Biology
Impact index in year of publication: 4.411
Journal in the top 25%: Yes
Position of publication: 12
No. of journals in the cat.: 86

Source of citations: WOS
Citations: 10

Source of citations: Google Scholar
Citations: 25

Relevant results: Brief summary of my participation in this paper: The goal of this paper is to extend the dynamic clamp concept by means of closed-loop protocols. In this respect, three different experimental setups were discussed as examples of goal-driven real-time closed-loop interactions. The implementation of proper control/observation procedures in the context of complex systems calls for the development of fast and accurate methods for automatic event detection and dynamics characterization. My contribution to this work is on the design, implementation and validation of such analysis tools using symbolic dynamics and information theory, along with the formalization of the (real time/on-line) closed-loop control scheme.

24 David Arroyo; Gonzalo Alvarez; José María Amigó; Shujun Li. Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Communications in Nonlinear Science and Numerical Simulation. 16 - 2, pp. 805 - 813. 2011.

Type of production: Scientific paper
Format: Journal

Impact source: ISI
Category: PHYSICS, MATHEMATICAL
Impact index in year of publication: 2.697
Journal in the top 25%: Yes
Position of publication: 3
No. of journals in the cat.: 54

Source of citations: WOS
Citations: 21

Source of citations: Google Scholar
Citations: 32

Relevant results: Brief summary of my participation in this paper: In this paper we show that the symbolic sequences of unimodal maps can not be used as keystreams. Indeed, if the keystream is given by the symbolic sequence of a unimodal map, then the control parameter and the initial condition of the map can be easily obtained according to some of our previous results. Furthermore, we show that statistical distances can be used to distinguish the symbolic sequences of a unimodal map from another unimodal map. As first author and

corresponding author, I proposed an attack of the cryptosystem based on the theory of symbolic dynamics of unimodal maps, but also in analysis of their order patterns. This first proposal was successful applied with the help of the Wootters' distance, as criterion to distinguish the symbolic sequences of the logistic map from those associated to the skew tent map. The final manuscript was the result of the improvement of the first proposal according to the suggestions and comments of the co-authors, being all of them handled and incorporated by me as first author.

25 Chengqing Li; David Arroyo; Kwok-Tung Lo. Breaking a Chaotic Cryptographic Scheme Based on Composition Maps. International Journal of Bifurcation and Chaos. 20 - 8, pp. 2561 - 2568. 2010.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MULTIDISCIPLINARY SCIENCES
Impact index in year of publication: 0.991
Journal in the top 25%: Yes
Position of publication: 18
No. of journals in the cat.: 50
Source of citations: WOS
Citations: 19
Source of citations: Google Scholar
Citations: 22

Relevant results: As second author of this paper I collaborated in the definition and concretion of the attacks, and I carried out the analysis of the chaoticity of the chaotic system used as base of the considered cryptosystem. The chaoticity was measured by means of the maximum Lyapunov exponent.

26 David Arroyo; Shujun Li; José María Amigó; Gonzalo Alvarez; Rhouma Rhouma. Comments on "Image encryption with chaotically coupled chaotic maps". Physica D. 239 - 12, pp. 1002 - 1006. 2010.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MATHEMATICS, APPLIED
Impact index in year of publication: 1.555
Journal in the top 25%: Yes
Position of publication: 28
No. of journals in the cat.: 236
Source of citations: WOS
Citations: 15
Source of citations: Google Scholar
Citations: 28

Relevant results: Brief summary of my participation in this paper: As first author and corresponding author, I proposed an scheme to analysis a cryptosystem based on the logistic map. This first scheme was further improved according to the suggestions of the co-authors, begin coordinated all the changes by the first author. The final cryptanalysis shows that the cryptosystem has some implementation problems, but it also proves that it is possible to recover part of the secret key using a timing-attack, i.e., by analyzing the complexity of the encryption procedure.

27 Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; David Arroyo; A.B. Orue; Veronica Fernandez; Fausto Montoya. A general view of pseudoharmonics and pseudoantiharmonics to calculate external arguments of Douady and Hubbard. Applied Mathematics and Computation. 213 - 2, pp. 484 - 497. 2009. ISSN 0096-3003

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MATHEMATICS, APPLIED
Impact index in year of publication: 1.124
Position of publication: 61
No. of journals in the cat.: 204
Source of citations: WOS
Citations: 3
Source of citations: Google Scholar
Citations: 6

Relevant results: Brief summary of my participation in this paper: I collaborated in the programming and computer simulations associated to this paper. The work I carried out for this paper led to a set of tools for the analysis of symbolic dynamics and the harmonic structure of the Mandelbrot and logistic maps.

28 Rhouma Rhouma; Ercan Solak; David Arroyo; Shujun Li; Gonzalo Alvarez; Safya Belghith. Comment on ``Modified Baptista type chaotic cryptosystem viamatrix secret key'' [Phys. Lett. A 372 (2008) 5427]. Physics Letters A. 373 - 37, pp. 3398 - 3400. 2009.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: PHYSICS, MULTIDISCIPLINARY
Impact index in year of publication: 2.009
Journal in the top 25%: No
Position of publication: 22
No. of journals in the cat.: 71
Source of citations: WOS
Citations: 13
Source of citations: Google Scholar
Citations: 41

Relevant results: Brief summary of my participation in this paper: I was involved in the definition of the original scheme used in this cryptanalysis paper. My collaboration in this paper is based on the results that I have obtained in the study of the symbolic dynamics of unimodal maps, but also I participated in the analysis of the design problems concerning the encryption scheme under examination.

29 Miguel Romera; Gerardo Pastor; Amalia-Beatriz Orue; David Arroyo; Fausto Montoya. Coupling patterns of external arguments in the multiple-spiral medallions of the Mandelbrot set. Discrete Dynamics in Nature and Society. 2009, pp. Article ID 135637, 14 pages - Article ID 135637, 14 pages. 2009.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MATHEMATICS, INTERDISCIPLINARY APPLICATIONS
Impact index in year of publication: 1.577
Journal in the top 25%: Yes
Position of publication: 18
No. of journals in the cat.: 80
Source of citations: WOS
Citations: 1
Source of citations: Google Scholar
Citations: 4

Relevant results: Brief summary of my participation in this paper: I collaborated in this paper programming and performing some of the simulations used in the concretion of the final manuscript.

30 David Arroyo; Chengqing Li; Shujun Li; Gonzalo Alvarez. Cryptanalysis of a computer cryptography scheme based on a filter bank. Chaos, Solitons and Fractals. 41, pp. 410 - 413. 2009.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MATHEMATICS, INTERDISCIPLINARY APPLICATIONS
Impact index in year of publication: 3.315
Journal in the top 25%: Yes
Position of publication: 2
No. of journals in the cat.: 80
Source of citations: WOS
Citations: 6
Source of citations: Google Scholar
Citations: 15

Relevant results: Brief summary of my participation in this paper: The aim of this paper was the cryptanalysis of a cryptosystem in which the information is encrypted using the orbits of the logistic maps without any transformation. Since the chaotic orbits of the logistic map are accessible, the recovering of the control parameter and the initial condition can be performed straightaway. I participated in this paper as first author and corresponding author, and thus I proposed the first proposal of attack. This first proposal was later improved, being all the changes handled and supervised by me as first author.

31 David Arroyo; Gonzalo Alvarez; Shujun Li; Chengqing Li; Veronica Fernandez. Cryptanalysis of a new chaotic cryptosystem based on ergodicity. International Journal of Modern Physics B. 23 - 5, pp. 651 - 659. 2009.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: PHYSICS, APPLIED
Impact index in year of publication: 0.408
Journal in the top 25%: No

Position of publication: 99 **No. of journals in the cat.:** 180

Source of citations: WOS **Citations:** 12

Source of citations: Google Scholar **Citations:** 20

Relevant results: Brief summary of my participation in this paper: As first author and corresponding author, I designed and coordinated the cryptanalysis of a cryptosystem based on the logistic map. The encryption architecture of this cryptosystem allows the recovering of the symbolic sequences of the logistic map just using a general cryptographic attack. In this paper we show that it is possible to estimate the control parameter and the initial condition of the logistic map from a given symbolic sequence, which means that it is possible to solve the inverse problem associated to the chaotic cryptosystem under examination.

32 David Arroyo; Chengqing Li; Shujun Li; Gonzalo Alvarez; Wolfgang A. Halang. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons and Fractals. 41 - 5, pp. 2613 - 2616. 2009.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** PHYSICS, MATHEMATICAL

Impact index in year of publication: 3.315 **Journal in the top 25%:** Yes

Position of publication: 2 **No. of journals in the cat.:** 80

Source of citations: WOS **Citations:** 37

Source of citations: Google Scholar **Citations:** 90

Relevant results: Brief summary of my participation in this paper: This paper cryptanalysis of a chaotic cryptosystem according to the characteristic attack for permutation-only cryptosystems, along with a keystream recovery attack. In this paper we also show the inadequacy of continuous-time chaotic systems as base of encryption schemes defined in discrete time. My participation in this paper was associated to the generation of the original proposal and the coordination task that led to the writing of the final manuscript.

33 David Arroyo; Gonzalo Alvarez; José María Amigó. Estimation of the control parameter from symbolic sequences: Unimodalmaps with variable critical point. Chaos: An Interdisciplinary Journal of Nonlinear Science. 19, pp. 023125, 9 pages - 023125, 9 pages. 2009.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** MATHEMATICS, APPLIED

Impact index in year of publication: 1.795 **Journal in the top 25%:** Yes

Position of publication: 20 **No. of journals in the cat.:** 204

Source of citations: WOS **Citations:** 13

Source of citations: Google Scholar **Citations:** 20

Relevant results: Brief summary of my participation in this paper: This paper is an extension of the main results of the study of the symbolic dynamics of unimodal maps. As first author and corresponding author, I designed a procedure to overcome the limitations of previous methods for the estimation of the control parameter of unimodal maps using the theory of symbolic dynamics. This new method is based on the concept of order pattern, and it was improved and concreted with the collaboration of two co-authors. As first author I coordinated the final concretion of the method according to the suggestions of the co-authors and referees. Currently we are working on the application of this methodology to other maps and applications.

34 Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; David Arroyo; A.B. Orue; Veronica Fernandez; Fausto Montoya. Algorithm for external arguments calculation of the nodes of a shrub in the Mandelbrot set. Fractals. 16 - 2, pp. 159 - 168. 2008.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** MULTIDISCIPLINARY SCIENCES

Impact index in year of publication: 0.486 **Journal in the top 25%:** No

Position of publication: 28 **No. of journals in the cat.:** 42

Source of citations: WOS **Citations:** 4

Source of citations: Google Scholar **Citations:** 6

Relevant results: Brief summary of my participation in this paper: My collaboration in this paper was focused on the study of the (pseudo)harmonics, (pseudo)antiharmonics of the Mandelbrot set. The results of the computer simulations based on those calculation tools were very helpful for the understanding of the symbolic dynamics of unimodal maps. In this sense, these results were not only the base of my participation in this paper, but also the origin of some applications later developed in other papers.

35 David Arroyo; Gonzalo Alvarez; Shujun Li; Chengqing Li; Juana Nuñez. Cryptanalysis of a discrete-time synchronous chaotic encryption system. Physics Letter A. 372 - 7, pp. 1034 - 1039. 2008.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** PHYSICS, MULTIDISCIPLINARY

Impact index in year of publication: 2.174 **Journal in the top 25%:** Yes

Position of publication: 16 **No. of journals in the cat.:** 68

Source of citations: WOS **Citations:** 20

Source of citations: Google Scholar **Citations:** 30

Relevant results: Brief summary of my participation in this paper: As first author and corresponding author of this paper, I designed the framework that was used in the concretion of the first version of the manuscript. The core of the paper is the resolution of an inverse problem given by a certain encryption architecture based on the Hènon map. The dynamics of the Hènon map were reconstructed using different strategies given by the general cryptanalysis framework. My results on the Lyapunov exponent of the Mandelbrot map were very useful to determine the Lyapunov exponents of the Hénon map and to examine its limitations in the context under consideration. Finally, as first author of the paper I supervised and coordinated the successive revisions, suggestions, and improvements proposed by all the co-authors.

36 Miguel Romera; Gonzalo Alvarez; David Arroyo; A.B. Orue; Veronica Fernandez; Gerardo Pastor. Drawing and computing external rays in the multiple-spiral medallionsof the Mandelbrot set. Computers & Graphics. 32, pp. 597 - 610. 2008.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** COMPUTER SCIENCE, SOFTWARE ENGINEERING

Impact index in year of publication: 0.731 **Journal in the top 25%:** No

Position of publication: 64 **No. of journals in the cat.:** 86

Source of citations: WOS **Citations:** 2

Source of citations: Google Scholar **Citations:** 5

Relevant results: Brief summary of my participation in this paper: I collaborated in the programming and computer simulations associated to this paper. The work I carried out for this paper enabled the definition of a set of tools for the analysis of symbolic dynamics and the harmonic structure of the Mandelbrot and logistic maps.

37 David Arroyo; Rhouma Rhouma; Gonzalo Alvarez; Shujun Li; Veronica Fernandez. On the security of a new image encryption scheme based on chaotic map lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science. 18, pp. 033112, 7 pages - 033112, 7 pages. 2008.

Type of production: Scientific paper **Format:** Journal

Impact source: ISI **Category:** MATHEMATICS, APPLIED

Impact index in year of publication: 2.152 **Journal in the top 25%:** Yes

Position of publication: 9 **No. of journals in the cat.:** 175

Source of citations: WOS **Citations:** 50

Source of citations: Google Scholar **Citations:** 86

Relevant results: Brief summary of my participation in this paper: As first author and corresponding author of this paper, I designed the framework that was used in the concretion of the first version of the manuscript. All my previous results on the study of quadratic unimodal maps were very useful for the goal of this paper. More specifically, this paper is focused on the inverse problem given by data derived from the sampling of orbits of the logistic map. We show how to solve this inverse problem for a certain chaos-based encryption system based on the logistic map. In our cryptanalysis we have also emphasized some serious design problems of the encryption architecture examined in this paper. As first author I coordinated all the different analysis proposed by the rest of co-authors, along with all the different versions of the manuscript until a final version was reached.

38 Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; David Arroyo; Fausto Montoya. On periodic and chaotic regions in the Mandelbrot set. Chaos, Solitons and Fractals. 32 - 1, pp. 15 - 25. 2007.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MATHEMATICS, INTERDISCIPLINARY APPLICATIONS
Impact index in year of publication: 3.025
Journal in the top 25%: Yes
Position of publication: 2
No. of journals in the cat.: 74
Source of citations: WOS
Citations: 9
Source of citations: Google Scholar
Citations: 11

Relevant results: Brief summary of my participation in this paper: The goal of this paper is to improve previous methods on the calculation of the external arguments of the root and Misiurewicz points of the Mandelbrot set. My collaboration in this paper was in the line of experimental analysis of the harmonic structure of quadratic maps.

39 Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; Juana Nunez; David Arroyo; Fausto Montoya. Operating with external arguments of Douady and Hubbard. Discrete Dynamics in Nature and Society. 2007, pp. Article ID 45920, 17 pages - Article ID 45920, 17 pages. 2007.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MULTIDISCIPLINARY SCIENCES
Impact index in year of publication: 0.552
Journal in the top 25%: No
Position of publication: 26
No. of journals in the cat.: 50
Source of citations: WOS
Citations: 3
Source of citations: Google Scholar
Citations: 6

Relevant results: Brief summary of my participation in this paper: This paper was focused on the determination of the external arguments of the hyperbolics components and Misiurewicz points of the Mandelbrot set. My participation in this paper was associated to the set of computer simulations performed to prove the different results.

40 Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; David Arroyo; Fausto Montoya. Equivalence Between Subshrubs and Chaotic Bands in the Mandelbrot Set. Discrete Dynamics in Nature and Society. 2006, pp. Article ID 70471, 25 pages - Article ID 70471, 25 pages. 2006.

Type of production: Scientific paper
Format: Journal
Impact source: ISI
Category: MULTIDISCIPLINARY SCIENCES
Impact index in year of publication: 0.5
Journal in the top 25%: No
Position of publication: 25
No. of journals in the cat.: 50
Source of citations: WOS
Citations: 4
Source of citations: Google Scholar
Citations: 8

Relevant results: Brief summary of my participation in this paper: My collaboration in this paper was focused on the set of simulations related to the study of the inner structure of the Mandelbrot set. My participation in this paper

was motivated by my first results obtained in the study of the dense set of unstable orbits of quadratic maps. Some of those results were useful for the analysis of the one-dimensional route of the Mandelbrot set.

41 En la encrucijada de la “blockchain”: posibilidades, expectativas y retos en la configuración de nuevos espacios de confianza digital. Novatica. 03/04/2020. Available on-line at: <https://www.novatica.es/en-la-encrucijada-de-la-blockchain-posibilidades-expectativas-y-retos-en-la-configuracion-de-nuevos-espacios-de-confianza-digital/>.
Type of production: Popular science article **Format:** Scientific and technical document or report

42 David Arroyo; Javier Valencia; Carlos Galán. From disinformation to cognitive warfare: Russian and Iranian techniques, tactics and procedures in the design and deployment of hybrid threats. Disinformation and fact-checking in contemporary society. Dykinson, 10/10/2023. Available on-line at: <https://www.dykinson.com/libros/disinformation-and-fact-checking-in-contemporary-society/9788411707107/>.
Type of production: Book chapter **Format:** Book
Corresponding author: No

43 Sara Degli Esposti; David Arroyo. Trustworthy humans and machines: Vulnerable trustors and the need for trustees' competence, integrity, and benevolence in digital systems. Trust and Transparency in an Age of Surveillance. pp. 201 - 220. Routledge, 10/11/2021. Available on-line at: <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003120827-15/trustworthy-humans-machines-sara-degli-esposti-david-arroyo>. ISBN 9781003120827
Type of production: Book chapter **Format:** Book
Corresponding author: No

44 Alejandro Sánchez Gómez; Jesus Diaz; Luis Hernández Encinas; David Arroyo. Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers. Computer and Network Security Essentials Book. In Press, Springer, 31/01/2017.
Type of production: Book chapter **Format:** Book
Corresponding author: Yes

45 Pablo Varona; David Arroyo; F.B. Rodríguez; Thomas Nowotny. Online Event Detection Requirements in Closed-Loop Neuroscience. In Closed-Loop Neuroscience. Editor: Ahmed El Hady (Princeton Neuroscience Institute). pp. 81 - 91. Elsevier, Academic Press, 01/10/2016. Available on-line at: <http://store.elsevier.com/Closed-Loop-Neuroscience/Ahmed-El-Hady/isbn-9780128024522/>. ISBN 9780128026410
Type of production: Book chapter
Corresponding author: No

46 David Arroyo Guardeño; Víctor Gayoso Martínez; Luis Hernández Encinas. ¿Qué sabemos de? Ciberseguridad. Colección CSIC "¿Qué sabemos de?". Editorial Catarata, 21/11/2020. Available on-line at: <978-84-9097-684-5>. ISBN 978-8413521190
Type of production: Popular science book **Format:** Book
Position of signature: 1
Total no. authors: 3 **Corresponding author:** Yes

47 David Arroyo Guardeño; Jesús Díaz Vico; Luis Hernández Encinas. ¿Qué sabemos de? Blockchain. Colección CSIC "¿Qué sabemos de?". Editorial Catarata, 06/05/2019. Available on-line at: <978-84-9097-684-5>. ISBN 978-84-9097-684-5
Type of production: Popular science book **Format:** Book
Position of signature: 1
Total no. authors: 3 **Corresponding author:** Yes

48 Javier Valencia; David Arroyo; Borja Díaz-Merry; Carlos Galán; Agustín Valencia; Fernando Valladares; Fernando Villena. TÉCNICAS Y METODOLOGÍAS DE CIBERINTELIGENCIA PARA LA INVESTIGACIÓN DE OPERACIONES DE INFORMACIÓN Y GUERRA COGNITIVA. Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional - Trabajos 2023. Departamento de Seguridad Nacional de España, 12/12/2023. Available on-line at: <https://www.dsn.gob.es/es/documento/foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-trabajos-2023>.
Type of production: Scientific-technical report **Format:** Book

Works submitted to national or international conferences

1 **Title of the work:** Controversy detection and automated characterization of polarized communities by compression distances - Extended Abstract
Name of the conference: MISDOOM
Corresponding author: Yes
Date of event: 21/11/2023
Luis Pérez Miguel; David Arroyo. Available on-line at: <https://event.cwi.nl/misdoom-2023/>.

2 **Title of the work:** WIDISBOT: Widget to analyse disinformation and content spread by bots
Name of the conference: DiTox 2023 : 1st International Workshop on Disinformation and Toxic Content Analysis
Corresponding author: No
City of event: Vienna, Austria
Date of event: 12/09/2023
José Manuel Camacho; Luis Pérez Miguel; David Arroyo. Available on-line at: <https://aclanthology.org/2023.ldk-1.55.pdf>.

3 **Title of the work:** Implementation and Benchmarking of Group Signature Schemes in a RISC-V-based TEE
Corresponding author: No
Date of event: 10/09/2023
Sergio Chica; José Cabrero Holgueras; Alejandro Cabrera Aldaya; Sergio Galán; Nicola Tuveri; David Arroyo. Available on-line at: <https://ches.iacr.org/2023/forum.php>.

4 **Title of the work:** On the Design of a Misinformation Widget (MsW) Against Cloaked Science
Name of the conference: NSS 2023: Network and System Security
Corresponding author: No
Date of event: 07/08/2023
David Arroyo; Sara Degli Esposti; Alberto Gómez Espés; Santiago Palmero Muñoz; Luis Pérez Miguel. Available on-line at: <https://link.springer.com/chapter/10.1007/978-3-031-39828-5_21>.

5 **Title of the work:** Analyzing the Effectiveness of Native Token Airdrop Campaigns in NFT Marketplaces
Name of the conference: International Congress on Blockchain and Applications
Date of event: 12/07/2023
Paul Kuhle; David Arroyo; Pablo de Andrés. Available on-line at: <https://link.springer.com/chapter/10.1007/978-3-031-45155-3_37>.

6 **Title of the work:** A framework for risk management in systems with AI components
Name of the conference: Games & Decisions in Risk & Reliability
Corresponding author: No
City of event: Madrid,
Date of event: 08/05/2023

José Manuel Camacho; David Arroyo. Available on-line at: <https://www.icmat.es/congresos/2023/GDRR/Book_of_Abstracts_GDRR.pdf>.

7 **Title of the work:** Following Negationists on Twitter and Telegram: Application of NCD to the Analysis of Multiplatform Misinformation Dynamics
Name of the conference: UCAmI 2022
Corresponding author: Yes
City of event: Córdoba,
Date of event: 21/11/2022
Alfonso de Paz; Manuel Suárez; Santiago Palmero; Sara Degli-Esposti; David Arroyo.

8 **Title of the work:** Advancing the Use of Information Compression Distances in Authorship Attribution
Name of the conference: MISDOOM 22
Corresponding author: Yes
Date of event: 11/10/2022
End date: 12/10/2022
Santiago Palmero Muñoz; Christian Oliva; Luis Fernando Lago Fenández; David Arroyo.

9 **Title of the work:** Rumor and clickbait detection by combining information divergence measures and deep learning techniques
Name of the conference: ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security
Corresponding author: Yes
City of event: Vienna, Austria
Date of event: 22/08/2022
End date: 26/08/2022
Christian Oliva; Ignacio Palacio Marín; Luis Fernando Fernández Lago; David Arroyo.

10 **Title of the work:** Enhancing the anonymity and auditability of whistleblowers protection
Name of the conference: Blockchain 22
Corresponding author: No
City of event: L'Aquila, Italy
Date of event: 13/07/2022
End date: 14/07/2022
Sergio Chica; Andrés Marín; David Arroyo; Jesús Díaz; Florina Almenares; Daniel Díaz.

11 **Title of the work:** Improving LSTMs' under-performance in Authorship Attribution for short texts
Name of the conference: EICC '22: Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference
Corresponding author: Yes
City of event: Barcelona, Spain
Date of event: 14/06/2022
End date: 14/06/2022
Christian Oliva; Santiago Palmero Muñoz; Luis Fernando Lago Fernández; David Arroyo.

12 **Title of the work:** On the design of a misinformation widget for messaging apps: bridging expert knowledge and automated news classification
Name of the conference: MISDOOM2020
Date of event: 27/10/2020
End date: 27/10/2020
David Arroyo; Sara Degli-Esposti.

13 **Title of the work:** Trustworthy, Reliable and Engaging Scientific Communication Approaches (TRESCA): A Research Agenda
Name of the conference: MISDOOM2020
Date of event: 26/10/2020
End date: 27/10/2020
Marina Tulin; Jason Pridmore; Sara Degli-Esposti; David Arroyo.

14 **Title of the work:** Fake News Detection Do Complex Problems Need Complex Solutions?
Name of the conference: CISIS 2020: 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)
Date of event: 2020
End date: 2020
Ignacio Palacio Marín; David Arroyo. "Advances in Intelligent Systems and Computing". 1267, pp. 229 - 238. Available on-line at: <https://link.springer.com/chapter/10.1007/978-3-030-57805-3_22>.

15 **Title of the work:** Sandbox for Minimal Viable Governance of Blockchain Services and DAOs: CLAUDIA
Name of the conference: International Congress on Blockchain and Applications, BLOCKCHAIN 2020: Blockchain and Applications
Date of event: 2020
End date: 2020
Ismaeil Arribas; David Arroyo; Denisa Reshef Kera. "Advances in Intelligent Systems and Computing". 1238, pp. 24 - 30. Available on-line at: <https://link.springer.com/chapter/10.1007/978-3-030-52535-4_3>.

16 **Title of the work:** Securing Blockchain with Quantum Safe Cryptography: When and How?
Name of the conference: CISIS 2020: 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)
Date of event: 2020
End date: 2020
Veronica Fernandez; Amalia B. Orue; David Arroyo. "Advances in Intelligent Systems and Computing". 1267, pp. 371 - 379. Available on-line at: <https://link.springer.com/chapter/10.1007/978-3-030-57805-3_22>.

17 **Title of the work:** An Internet Voting Proposal Towards Improving Usability and Coercion Resistance
Name of the conference: International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)
City of event: Sevilla, Andalusia, Spain
Date of event: 13/05/2019
End date: 15/05/2019
Publication in conference proceedings: Yes
Inigo Querejeta-Azurmendi; Luis Hernández Encinas; David Arroyo Guardeño; Jorge Hernández Ardieta. pp. 155 - 164. Springer International Publishing, Available on-line at: <https://doi.org/10.1007/978-3-030-20005-3_16>. ISBN 978-3-030-20005-3

18 **Title of the work:** Hyot: Leveraging Hyperledger for Constructing an Event-Based Traceability System in IoT
Name of the conference: International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)
City of event: Sevilla, Andalusia, Spain
Date of event: 13/05/2019

End date: 15/05/2019
Publication in conference proceedings: Yes
Jesús Iglesias García; Jesus Diaz; David Arroyo. pp. 195 - 204. Springer, Cham, Available on-line at: <https://doi.org/10.1007/978-3-030-20005-3_20>. ISBN 978-3-030-20005-3

19 **Title of the work:** El difícil tránsito desde la digitalización a la dataficación: seguridad, privacidad y usabilidad en el contexto tecnológico actual
Name of the conference: Seminario
City of event: Madrid, Community of Madrid, Spain
Date of event: 22/03/2019
End date: 22/03/2019
Organising entity: Instituto de Tecnologías Físicas y de la Información (ITEFI), CSIC

20 **Title of the work:** Principales problemas de seguridad en los smart contracts de Ethereum
Name of the conference: XII JORNADAS STIC CCN-CERT
City of event: Madrid, Community of Madrid, Spain
Date of event: 13/12/2018
End date: 14/12/2018
Organising entity: Centro Criptológico Nacional
David Arroyo Guardeño; Álvaro Rezola Borrego; Luis Hernández Encinas. "https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3422-m22-02-smart-contracts-ethereum/file.html". Available on-line at: <https://www.ccn-cert.cni.es/documentos-publicos/x-jornadas-stic-ccn-cert/1921-m2-05-blockchains-csic/file.html>.

21 **Title of the work:** El cloud computing: una realida ineludible
Name of the conference: Jornandas Fintech
City of event: Madrid, Community of Madrid, Spain
Date of event: 04/12/2018
End date: 04/12/2018
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
David Arroyo Guardeño. "Seminario Invitado".

22 **Title of the work:** El reto de la ciberseguridad
Name of the conference: Jornandas Fintech
City of event: Madrid, Community of Madrid, Spain
Date of event: 29/11/2018
End date: 29/11/2018
Organising entity: Universidad Autónoma de Madrid **Type of entity:** University
David Arroyo Guardeño. "Seminario Invitado".

23 **Title of the work:** A Comprehensive Privacy-Respecting Mechanism for Global E-Commerce
Name of the conference: Invited Seminar, The Applied Security and Information Assurance Group - APSIA, Luxembourg, Luxembourg
City of event: Luxembourg, Luxembourg
Date of event: 10/10/2018
End date: 10/10/2018
Organising entity: The Applied Security and Information Assurance Group - APSIA
David Arroyo.

24 **Title of the work:** Aplicación de técnicas de compresión de información a la identificación de anomalías en fuentes de datos heterogéneas: análisis y limitaciones
Name of the conference: XV Reunión Espñaola de Criptografía y Seguridad de la Información
Corresponding author: No
City of event: Granada, Andalusia, Spain
Date of event: 03/10/2018
End date: 05/10/2018
Organising entity: Universidad de Granada **Type of entity:** University
Gonzalo de la Torre Abaitua; Luis Lago; David Arroyo. Available on-line at: <https://nesg.ugr.es/recsi2018/docs/ActasXVRECSI.pdf>.

25 **Title of the work:** Privacy in e-Shopping Transactions: Exploring and Addressing the Trade-Offs
Name of the conference: CSCML- International Symposium on Cyber Security Cryptography and Machine Learning
Corresponding author: No
City of event: Beer-Sheva, Israel
Date of event: 21/06/2018
End date: 22/06/2018
Jesus Diaz; Seung Geol Choi; David Arroyo; Angelos D. Keromytis; Francisco B. Rodriguez; Moti Yung.

26 **Title of the work:** Desarrollo de un sistema de trazabilidad en entornos IoT mediante Hyperledger
Name of the conference: Jornadas Nacionales de Investigación en Ciberseguridad
City of event: San Sebastián, Basque Country, Spain
Date of event: 13/06/2018
End date: 15/06/2018
Jesús Iglesias García; David Arroyo.

27 **Title of the work:** Desarrollo de una metodología para la caracterización de fuentes de datos heterogéneos e identificación de anomalías en sistemas de información
Name of the conference: Jornadas Nacionales de Investigación en Ciberseguridad
City of event: San Sebastián, Basque Country, Spain
Date of event: 13/06/2018
End date: 15/06/2018
Gonzalo de la Torre; Luis F. Lago; David Arroyo.

28 **Title of the work:** Frente al computador cuántico, Criptografía postcuántica
Name of the conference: XI JORNADAS STIC CCN-CERT
City of event: Madrid, Community of Madrid, Spain
Date of event: 13/12/2017
End date: 14/12/2017
Organising entity: Centro Criptológico Nacional
Luis Hernández Encinas; Víctor Gayoso Martínez; David Arroyo Guardeño. "https://www.ccn-cert.cni.es/pdf/documentos-publicos/xi-jornadas-stic-ccn-cert/2599-m31-02-frente-al-computador-cuantico/file.html". Available on-line at: <https://www.ccn-cert.cni.es/documentos-publicos/x-jornadas-stic-ccn-cert/1921-m2-05-blockchains-csic/file.html>.

29 **Title of the work:** A parameter-free method for the detection of web attacks
Name of the conference: CISIS'17
City of event: León, Castile and León, Spain
Date of event: 06/09/2017
End date: 08/09/2017
Organising entity: Universidad de León **Type of entity:** University

Gonzalo de la Torre Abaitua; Luis F. Lago Fernández; David Arroyo. Accepted,

30 **Title of the work:** Encrypted Cloud: a software solution for the secure use of free-access cloud storage services
Name of the conference: CISIS'17
Corresponding author: Yes
City of event: León, Castile and León, Spain
Date of event: 06/09/2017
End date: 08/09/2017
Organising entity: Universidad de León **Type of entity:** University
Alejandro Sánchez Gómez; Jesus Diaz; David Arroyo. Accepted,

31 **Title of the work:** A coercion-resistant and easy-to-use Internet e-voting protocol based on traceable anonymous certificates"
Name of the conference: III Jornadas Nacionales de Ciberseguridad
City of event: Madrid, Community of Madrid, Spain
Date of event: 31/05/2017
End date: 31/05/2017
Organising entity: Universidad Rey Juan Carlos **Type of entity:** University
Iñigo Querejeta Azurmendi; Jorge López Hernández-Ardieta; Víctor Gayoso Martínez; Luis Hernández Encinas; David Arroyo Guardeño. "https://eciencia.urjc.es/handle/10115/14540".

32 **Title of the work:** Blockchains: usos y abusos
Name of the conference: X JORNADAS STIC CCN-CERT
City of event: Madrid, Community of Madrid, Spain
Date of event: 13/12/2016
End date: 14/12/2016
Organising entity: Centro Criptológico Nacional
Oscar Delgado; David Arroyo; Jesus Diaz; Luis Hernandez. Available on-line at: <https://www.ccn-cert.cni.es/documentos-publicos/x-jornadas-stic-ccn-cert/1921-m2-05-blockchains-csic/file.html>.

33 **Title of the work:** Coordination of irregular bursting rhythms in Central Pattern Generators
Name of the conference: 46th Annual Meeting of the Society For Neuroscience
Type of event: Conference **Geographical area:** Non EU International
Type of participation: 'Participatory - poster
Corresponding author: No
City of event: San Diego, United States of America
Date of event: 12/11/2016
End date: 16/11/2016
Irene Elices; David Arroyo; Rafael Levi; Francisco B. Rodríguez; Pablo Varona. Available on-line at: <https://www.sfn.org/Annual-Meeting/Neuroscience-2016/Sessions-and-Events/Program/Abstract-PDFs-2016>.

34 **Title of the work:** Assessing irregularity and coordination of spiking-bursting rhythms in central pattern generators
Name of the conference: 25th Annual Computational Neuroscience Meeting
Type of event: Conference **Geographical area:** Non EU International
Type of participation: 'Participatory - poster
Corresponding author: No
City of event: Jeju, Republic of Korea
Date of event: 07/07/2016
End date: 07/07/2016

Irene Elices; David Arroyo; Rafael Levi; Francisco B. Rodríguez; Pablo Varona. Available on-line at: <http://www.cnsorg.org/cns-2016-meeting-program>.

35 **Title of the work:** The API Hour: Blockchain Day, BBVA Innovation Center
Type of event: Workshop
Reasons for participation: Upon invitation
Date of event: 21/04/2016
En: Moderador de la mesa redonda sobre la tecnología blockchain. Available on-line at: <https://www.youtube.com/watch?v=aE0IHQ3lTNM>.

36 **Title of the work:** Privacy Threats in E-Shopping (Position Paper)
Name of the conference: 10th Data Privacy Management International Workshop. DPM 2015
Date of event: 21/09/2015
End date: 23/09/2015
Jesus Diaz; Seung Geol Choi; David Arroyo; Angelos D Keromytis; Francisco B. Rodriguez; Moti Yung. En: Data Privacy Management, and Security Assurance. 9481, pp. 217 - 225. Lecture Notes in Computer Science, Available on-line at: <http://link.springer.com/chapter/10.1007%2F978-3-319-29883-2_14>. ISBN 978-3-319-29883-2
DOI: 10.1007/978-3-319-29883-2_14

37 **Title of the work:** Ciberseguridad: vulnerabilidades, amenazas y riesgos
Name of the conference: XII Cursos de Verano, Centro de Altos Estudios Policiales
Date of event: 14/07/2015
Organising entity: Universidad Rey Juan Carlos
Available on-line at: <https://uverano.urjc.es/event_detail/2348/speakers/ciberseguridad_-vulnerabilidades-amenazas-y-riesgos-codigo-uv-s-ciber.html>.

38 **Title of the work:** Non-conventional Digital Signatures and Their Implementations—A Review
Name of the conference: CISIS-ICEUTE 2015
Type of event: Conference
Corresponding author: Yes
City of event: Burgos, Castile and León, Spain
Date of event: 17/06/2015
David Arroyo; Jesus Diaz; Francisco B. Rodriguez. pp. 455 - 462. Available on-line at: <http://link.springer.com/chapter/10.1007/978-3-319-19713-5_39#page-1>.

39 **Title of the work:** On the Difficult Tradeoff Between Security and Privacy: Challenges for the Management of Digital Identities
Name of the conference: CISIS-ICEUTE 2015
Type of event: Conference
Corresponding author: Yes
City of event: Burgos, Castile and León, Spain
Date of event: 17/06/2015
David Arroyo; Jesus Diaz; Victor Gayoso. pp. 455 - 462. Available on-line at: <http://link.springer.com/chapter/10.1007/978-3-319-19713-5_39#page-1>.

40 **Title of the work:** Using Smart Cards for Authenticating in Public Services: A Comparative Study
Name of the conference: CISIS-ICEUTE 2015
Type of event: Conference
Corresponding author: No
City of event: Burgos, Castile and León, Spain
Date of event: 17/06/2015

David Arroyo Guardeño; Víctor Gayoso Martínez; Luis Hernández Encinas; Agustín Martín Muñoz. pp. 455 - 462. Available on-line at: <http://link.springer.com/chapter/10.1007/978-3-319-19713-5_39#page-1>.

41 **Title of the work:** Characterizacion of neural activity by means of the applied theory of symbolic dynamics
Name of the conference: International Workshop on Neurodynamics
City of event: Castro Urdiales, Cantabria, Spain
Date of event: 14/07/2014
End date: 17/07/2014
David Arroyo.

42 **Title of the work:** Applications of symbolic dynamics in the context of cryptography
Name of the conference: The 10th AIMS Conference on Dynamical Systems,Differential Equations and Applications
City of event: Madrid, Community of Madrid, Spain
Date of event: 07/07/2014
End date: 11/07/2014
David Arroyo.

43 **Title of the work:** Automatic event detection and characterization in the context of real-time control of complex time-varying dynamical systems
Name of the conference: The 10th AIMS Conference on Dynamical Systems,Differential Equations and Applications
City of event: Madrid, Community of Madrid, Spain
Date of event: 07/07/2014
End date: 11/07/2014
David Arroyo; Pablo Varona; Francisco B. Rodriguez.

44 **Title of the work:** Closed-loop aproaches to characterize transient neural dynamics
Name of the conference: The 10th AIMS Conference on Dynamical Systems,Differential Equations and Applications
City of event: Madrid, Community of Madrid, Spain
Date of event: 07/07/2014
End date: 11/07/2014
Pablo Varona; David Arroyo; Francisco B. Rodriguez.

45 **Title of the work:** Methodological Security Verification of a Registration Protocol
Name of the conference: CISIS 2014 : 7th International Conference on Computational Intelligence in Security for Information Systems
City of event: Bilbao, Community of Madrid, Spain
Date of event: 25/06/2014
End date: 27/06/2014
Jesus Diaz; David Arroyo; Francisco B. Rodriguez. "International Joint Conference SOCO'14-CISIS'14-ICEUTE'14, Advances in Intelligent Systems and Computing Volume 299, 2014, pp 453-462".

46 **Title of the work:** Coordination of complex dynamics by means of simple neural circuits
Name of the conference: Net-Works 2013
City of event: El Escorial, Community of Madrid, Spain
Date of event: 11/12/2013
End date: 13/02/2014
Roberto Latorre; David Arroyo; Pablo Varona.

47 **Title of the work:** Anonymity revocation through standard infrastructures
Name of the conference: 9th European PKI Workshop: Research and Applications
Type of participation: Participatory - oral communication
Date of event: 13/09/2012
End date: 14/09/2012
City organizing entity: Pisa, Italy
Jesus Diaz; David Arroyo; Francisco Rodriguez. "Anonymity recocation through standard infrastructures. Public Key Infrastructures, Services and Applications. Lecture Notes in Computer Science Volume 7868, 2013, pp 112-127.". (Italy):

48 **Title of the work:** Closing the loop in the context of complex biological systems: Goals, needs and challenges.
Name of the conference: 8th FENS FORUM OF NEUROSCIENCE
Type of participation: 'Participatory - poster
Date of event: 14/07/2012
End date: 18/07/2012
City organizing entity: Barcelona, Spain
D. Arroyo; F. B. Rodriguez; P. Varona. (Spain):

49 **Title of the work:** Extension of the dynamic clamp concept in neurophysiology and behavior
Name of the conference: 8th FENS Forum of Neuroscience
Type of participation: 'Participatory - poster
Date of event: 14/07/2012
End date: 18/07/2012
City organizing entity: Barcelona, Spain
P. Varona; P. Chamorro; C. Muñiz; R. Levi; D. Arroyo; F.B. Rodriguez. (Spain):

50 **Title of the work:** Event detection, multimodality and non-stationarity: order patterns, a tool to rule them all?
Name of the conference: 9th AIMS Conference on Dynamical Systems, Differential equations, and Applications Cidudad: Orlando
Type of participation: Participatory - invited/keynote talk
Date of event: 01/07/2012
End date: 05/07/2012
D. Arroyo; P. Chamorro; J.M. Amigó; F. B. Rodriguez; P. Varona.

51 **Title of the work:** Aplicación de la dinámica simbólica al tratamiento y caracterización de series temporales
Name of the conference: Seminario impartido en el Departamento de Estadística, Matemáticas e Informática de la Universidad de Elche
Type of event: Seminar
Type of participation: Participatory - invited/keynote talk **Reasons for participation:** Upon invitation
City of event: Elche, Valencian Community, Spain
Date of event: 23/04/2012
Organising entity: Universidad Miguel Hernández de Elche **Type of entity:** University

52 **Title of the work:** On-line characterization of transient neuronal activity Nombrel del congreso: IV International Conference Net-Works 2011 Complex Networks: Structure, Applications and Related Topics
Name of the conference: IV International Conference Net-Works 2011 Complex Networks: Structure, Applications and Related Topic
Type of event: Conference **Geographical area:** Non EU International
Type of participation: 'Participatory - poster

City of event: El Escorial, Community of Madrid, Spain
Date of event: 26/10/2011
End date: 28/10/2011
City organizing entity: El Escorial, Spain
With external admission assessment committee: Yes
Type of contribution: Scientific paper
David Arroyo; Pablo Chamorro; J.M. Amigó; F. B. Rodriguez; P. Varona. En: International Journal of Complex Systems in Science. (Spain): Available on-line at: <http://www.ij-css.org/volume-01_02/ijcss01_02-146.pdf>. ISSN 2174-6036

53 **Title of the work:** Herramientas para la caracterización de actividad neuronal transitoria
Name of the conference: XIV Congreso Nacional de la Sociedad Española de Neurociencia
Geographical area: National
Type of participation: 'Participatory - poster
Date of event: 28/09/2011
End date: 30/09/2011
City organizing entity: Salamanca, Spain
David Arroyo; Pablo Chamorro; F.B. Rodriguez; Pablo Varona. (Spain):

54 **Title of the work:** An approach for adapting moodle into a secure infrastructure Editores: A. Herrero and E. Corchado
Name of the conference: CISIS 2011
Geographical area: Non EU International
Type of participation: Participatory - oral communication
Date of event: 08/06/2011
End date: 10/06/2011
City organizing entity: Torremolinos, Spain
With external admission assessment committee: Yes
J. Diaz; D. Arroyo; F. B. Rodriguez. En: Computational Intelligence in Security for Information Systems. Lecture Notes in Computer Science.. 6694, Springer Berlin Heidelberg, Available on-line at: <http://dx.doi.org/10.1007/978-3-642-21323-6_27>. ISBN 978-3-642-21322-9

55 **Title of the work:** Estudio del comportamiento vibracional nolineal de los sistemas ultrasónicos de potencia con radiadores de placa para aplicaciones industriales
Name of the conference: 41º Congreso Nacional de Acústica, 6º Congreso Ibérico de Acústica
Geographical area: National
Type of participation: Participatory - oral communication
Date of event: 13/10/2010
End date: 15/10/2010
City organizing entity: León, Spain
Andrea Cardoni; Enrique Riera; Alfonso Blanco; Víctor Acosta; David Arroyo; Juan A. Gallego Juárez."Estudio del comportamiento vibracional nolineal de los sistemas ultrasónicos de potencia con radiadores de placa para aplicaciones industriales". En: Revista de Acústica. 41, (Spain): ISBN 978-84-87985-19-5

56 **Title of the work:** Metodología para la caracterización del comportamiento no lineal de una familia de transductores de ultrasonidos de potencia
Name of the conference: 41º Congreso Nacional de Acústica, 6º Congreso Ibérico de Acústica
Geographical area: National
Type of participation: Participatory - oral communication
Date of event: 13/10/2010
End date: 15/10/2010

City organizing entity: León, Spain
David Arroyo; Alfonso Blanco; Enrique Riera; Andrea Cardoni. "Metodología para la caracterización del comportamiento no lineal de una familia de transductores de ultrasonidos de potencia". En: Revista de Acústica. 41, ISBN 978-84-87985-19-5

57 **Title of the work:** Resultados en I+D y aplicaciones recientes del IA-CSIC en sistemas y tecnologías ultrasónicas
Name of the conference: 41º Congreso Nacional de Acústica, 6º Congreso Ibérico de Acústica
Geographical area: National
Type of participation: Participatory - oral communication
Date of event: 13/10/2010
End date: 15/10/2010
City organizing entity: León, Spain
A. Ramos; J. A. Gallego; E. Riera; J.L. San Emeterio; T. Gómez; I. González; C. Campos; H. Calás; P.T. Sanz; G. Rodríguez; L. Castellanos; V. Acosta; A. Ruiz; E. Pardo; I. Bazán; D. Arroyo. "Resultados en I+D y aplicaciones recientes del IA-CSIC en sistemas y tecnologías ultrasónicas". En: Revista de Acústica. 41, (Spain): ISBN 978-84-87985-19-5

58 **Title of the work:** High-speed free-space quantum key distribution system for urban applications
Name of the conference: XI Reunión Española sobre Criptología y Seguridad de la Información (XI RECSI)
Type of event: Conference **Geographical area:** National
Type of participation: Participatory - oral communication
City of event: Tarragona, Catalonia, Spain
Date of event: 07/09/2010
End date: 10/09/2010
Organising entity: Universitat Rovira i Virgili **Type of entity:** University
City organizing entity: Tarragona, Catalonia, Spain
María José Garcia; Diego Soto; Natalia Denisenko; David Arroyo; A. B. Orue; Verónica Fernandez. "High-speed free-space quantum key distribution system for urban applications". En: Josep Domingo Ferrer, Antoni Martínez Ballesté, Jordi Castellá Roca, and Agustí Solanas Gómez, editors, XI Reunión Española sobre Criptología y Seguridad de la Información (XI RECSI). pp. 333 - 336. (Spain): ISBN 978-84-693-3304-4

59 **Title of the work:** On the inadequacy of unimodal maps for cryptographic applications
Name of the conference: XI Reunión Española sobre Criptología y Seguridad de la Información (XI RECSI)
Type of event: Conference **Geographical area:** National
Type of participation: Participatory - oral communication
City of event: Tarragona, Catalonia, Spain
Date of event: 07/09/2010
End date: 10/09/2010
Organising entity: Universitat Rovira i Virgili
City organizing entity: Tarragona, Spain
David Arroyo; José María Amigó; Shujun Li; Gonzalo Alvarez. "On the inadequacy of unimodal maps for cryptographic applications". En: Josep Domingo Ferrer, Antoni Martínez Ballesté, Jordi Castellá Roca, and Agustí Solanas Gómez, editors, XI Reunión Española sobre Criptología y Seguridad de la Información (XI RECSI). pp. 37 - 42. ISBN 978-84-693-3304-4

60 **Title of the work:** High-speed free-space quantum key distribution system for urban applications
Name of the conference: Photon10
Type of participation: 'Participatory - poster
Date of event: 23/08/2010
End date: 26/08/2010

City organizing entity: Southampton, United Kingdom
María José Garcia; David Arroyo; Natalia Denisenko; Diego Soto; Verónica Fernandez.(United Kingdom):

61 **Title of the work:** Estimation of the control parameter of a map through the analysis of its order patterns
Name of the conference: ICCSA 2009
Type of event: Conference **Geographical area:** Non EU International
Type of participation: Participatory - invited/keynote talk
Date of event: 29/06/2009
End date: 02/07/2009
Organising entity: Université du havre
City organizing entity: Le Havre, France
David Arroyo; Gonzalo Alvarez; José María Amigó. pp. 198.

62 **Title of the work:** Some hints for the design of digital chaos-based cryptosystems: lessons learned from cryptanalysis
Name of the conference: Second IFAC Conference on Analysis and Control of Chaotic Systems
Type of participation: Participatory - oral communication
Date of event: 22/06/2009
End date: 24/06/2009
Organising entity: Queen Mary, University of London
City organizing entity: London, United Kingdom
With external admission assessment committee: Yes
David Arroyo; Gonzalo Alvarez; Shujun Li. "Some hints for the design of digital chaos-based cryptosystems: lessons learned from cryptanalysis". En: Analysis and Control of Chaotic Systems (Proceedings of IFAC CHAOS 2009, the 2nd IFAC Meeting on Analysis and Control of Chaotic Systems, Queen Mary, University of London, UK). 2, (United Kingdom): Available on-line at: <http://dx.doi.org/10.3182/20090622-3-UK-3004.00034>.

63 **Title of the work:** A basic framework for the cryptanalysis of digital chaos-based cryptography
Name of the conference: Sixth International Multi-Conference on Systems, Signals and Devices Pagínas:
Geographical area: Non EU International
Type of participation: Participatory - oral communication
Date of event: 23/03/2009
End date: 26/03/2009
City organizing entity: Djerba, Tunisia
With external admission assessment committee: Yes
David Arroyo; Gonzalo Alvarez; Veronica Fernandez. "A basic framework for the cryptanalysis of digital chaos-based cryptography". En: Sixth International Multi-Conference on Systems, Signals and Devices. 1 - 2, pp. 58 - 63. (Tunisia): Available on-line at: <http://dx.doi.org/10.1109/SSD.2009.4956652>. ISBN 978-1-4244-4346-8

64 **Title of the work:** A new color image cryptosystem based on a piecewise linear chaotic map
Name of the conference: International Multi-Conference on Systems, Signals & Devices, Conference on Power Electrical Systems
Type of participation: Participatory - oral communication
Date of event: 23/03/2009
End date: 26/03/2009
City organizing entity: Djerba, Tunisia
With external admission assessment committee: Yes
Rhouma Rhouma; David Arroyo; Safya Belghith. "A new color image cryptosystem based on a piecewise linear chaotic map". En: International Multi-Conference on Systems, Signals & Devices,

Conference on Power Electrical Systems. 1 - 2, pages 377–382, (Tunisia): Available on-line at: <http://dx.doi.org/10.1109/SSD.2009.4956666>. ISBN 978-1-4244-4346-8

65 **Title of the work:** On the skew tent map as base of a new image chaos-based encryption scheme
Name of the conference: Second Workshop on Mathematical Cryptology
Type of participation: 'Participatory - poster
Date of event: 23/10/2008
End date: 25/10/2008
Organising entity: Universidad de Cantabria
City organizing entity: Santander, Spain
David Arroyo; Rhouma Rhouma; Gonzalo Alvarez; Veronica Fernandez; Safya Belghith. "On the skew tent map as base of a new image chaos-based encryption scheme". En: Álvar Ibeas and Jaime Gutiérrez, editors, Second Workshop on Mathematical Cryptology. pp. 113 - 117.

66 **Title of the work:** Free-space quantum key distribution link at gigahertz clock rates
Name of the conference: QKD Network Demonstration and Conference
Type of participation: 'Participatory - poster
Date of event: 08/10/2008
End date: 10/10/2008
City organizing entity: Viena,
V. Fernandez; D. Arroyo; M. J. Garcia; AB. Orue.

67 **Title of the work:** Experimental quantum key distribution at a wavelength of ? ~ 850nm
Name of the conference: X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI)
Geographical area: National
Type of participation: Participatory - oral communication
Date of event: 02/09/2008
End date: 05/09/2008
Organising entity: Universidad de Salamanca
City organizing entity: Salamanca, Spain
V. Fernandez; D. Arroyo; M.J. Garcia; P.A. Hiskett; R.J. Collins; G.S. Buller; A.B. Orue. "Experimental quantum key distribution at a wavelength of ? ~ 850nm". pp. 157 - 161. (Spain): A. Martin L. Hernandez, editor, X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI), ISBN 978-84-691-5158-7

68 **Title of the work:** On the inadequacy of the logistic map for cryptographic applications
Name of the conference: X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI)
Geographical area: National
Type of participation: Participatory - oral communication
Date of event: 02/09/2008
End date: 05/09/2008
Organising entity: Universidad de Salamanca **Type of entity:** University
City organizing entity: Salamanca, Spain
D. Arroyo; G. Alvarez; V. Fernandez. "On the inadequacy of the logistic map for cryptographic applications". En: L. Hernandez and A. Martin, editors, X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI). pp. 77 - 82. (Spain): ISBN 978-84-691-5158-7

69 **Title of the work:** Conjuntos de Julia alternados
Name of the conference: Nolineal 2008
Geographical area: National
Type of participation: 'Participatory - poster

Date of event: 06/2008
Organising entity: Universitat Politècnica de Catalunya
City organizing entity: Barcelona, Spain
G. Pastor; G. Alvarez; A. Orúe; V. Fernandez; D. Arroyo; M. Romera. "Conjuntos de Julia alternados". En: F. Marqués y A. Delshams, editor, Nolineal 2008. pp. 192. (Spain):

70 **Title of the work:** Emparejamiento de patrones en medallones de espiral múltiple
Name of the conference: Nolineal 2008
Geographical area: National
Type of participation: 'Participatory - poster
Date of event: 06/2008
Organising entity: Universitat Politècnica de Catalunya
City organizing entity: Barcelona, Spain
G. Pastor; G. Alvarez; A. Orúe; V. Fernandez; D. Arroyo; M. Romera."Emparejamiento de patrones en medallones de espiral múltiple". En: F. Marqués y A. Delshams, editor, Nolineal 2008. pp. 198. (Spain):

71 **Title of the work:** Pseudoharmonics and pseudoantiharmonics: a new tool to calculate external arguments of Douady and Hubbard
Name of the conference: International Conference on Dynamical methods and Mathematical modelling
Type of event: Conference **Geographical area:** Non EU International
Type of participation: 'Participatory - poster
Date of event: 18/09/2007
End date: 22/09/2007
Organising entity: Universidad de Valladolid **Type of entity:** University
City organizing entity: Valladolid, Spain
With external admission assessment committee: Yes
Gerardo Pastor; Miguel Romera; Gonzalo Alvarez; Juana Nunez; David Arroyo; Amalia Beatriz Orue; Fausto Montoya. "Pseudoharmonics and pseudoantiharmonics: a new tool to calculate external arguments of Douady and Hubbard". En: International Conference on Dynamical methods and Mathematical modelling. pp. 27.

72 **Title of the work:** Application of Gray code to the cryptanalysis of chaotic cryptosystems
Name of the conference: 3rd International IEEE Scientific Conference on Physics and Control (PhysCon'2007, 3rd - 7th, September 2007, Potsdam, Germany)
Type of event: Conference **Geographical area:** Non EU International
Type of participation: Participatory - oral communication
Date of event: 03/09/2007
End date: 07/09/2007
Organising entity: IEEE IPACS.
City organizing entity: Potsdam,
Gonzalo Alvarez; David Arroyo; Juana Nuñez. "Application of Gray code to the cryptanalysis of chaotic cryptosystems". En: 3rd International IEEE Scientific Conference on Physics and Control (PhysCon'2007, 3rd - 7th, September 2007, Potsdam, Germany). pp. 87. Available on-line at: <http://lib.physcon.ru/doc?id=f90b427a07e5>.

73 **Title of the work:** Aplicaciones de los códigos de Gray a la criptografía caótica
Name of the conference: NoLineal 2007
Geographical area: National
Type of participation: Participatory - invited/keynote talk
Date of event: 08/06/2007
Organising entity: Escuela Universitaria de Magisterio Padre Poveda
Gonzalo Álvarez Marañón; David Arroyo Guardeño; Juana Núñez García.

74 **Title of the work:** Algoritmo para el cálculo de los argumentos externos de los nodos de un shrub en el conjunto de Mandelbrot
Name of the conference: NoLineal 2007
Geographical area: National
Type of participation: 'Participatory - poster
Date of event: 06/2007
Organising entity: Escuela Universitaria de Magisterio Padre Poveda
Gerardo Pastor; M. Romera; G. Alvarez; J. Nunez; D. Arroyo; A.B. Orue; F. Montoya.

75 **Title of the work:** Determinación del valor de los parámetros del sistema de Lorenz y aplicación al criptoanálisis de criptosistemas caóticos
Name of the conference: NoLineal 2007
Geographical area: National
Date of event: 06/2007
Organising entity: Escuela Universitaria de Magisterio de Ciudad Real Tipo de comunicación: Poster
A.B. Orue; G. Alvarez; D. Arroyo; J. Nunez; F. Montoya. pp. 85.

76 **Title of the work:** Medallones de espiral múltiple en el conjunto de Mandelbrot
Name of the conference: NoLineal 2007
Geographical area: National
Type of participation: 'Participatory - poster
Date of event: 06/2007
Organising entity: Escuela Universitaria de Magisterio Padre Poveda
Gerardo Pastor; M. Romera; G. Alvarez; J. Nunez; D. Arroyo; A.B. Orue; F. Montoya.pp. 77.

R&D management and participation in scientific committees

Scientific, technical and/or assessment committees

1 **Committee title:** Experto asesor en el informe sobre Desinformación en la era digital de la Oficina C del Congreso de los Diputados de España (https://oficinac.es/es/informes-c/desinformacion-era-digital)
Start date: 14/12/2023

2 **Committee title:** Vocal en el Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional en representación de centros de investigación en el campo de la inteligencia artificial
Start date: 15/12/2022

3 **Committee title:** Experto asesor en el informe sobre ciberseguridad de la Oficina C del Congreso de los Diputados de España (https://oficinac.es/es/informes-c/ciberseguridad))
Start date: 14/11/2022

4 **Committee title:** Coordinator of chapter 8, smart cybersecurity in
CSIC's White Paper on Artificial Intelligence, Robotics and Data Science
(http://libros.csic.es/product_info.php?cPath=164&products_id=1493)
Affiliation entity: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Start date: 2021

5 **Committee title:** El papel de la estadística oficial en la administración y gestión de datos (https://www.ine.es/normativa/leyes/cse/papel_estadistica_oficial.pdf))
Affiliation entity: Consejo Superior de Estadística de España
City affiliation entity: Madrid, Spain
Start date: 02/07/2020

6 **Committee title:** CTN 71/SC 42 - INTELIGENCIA ARTIFICIAL Y BIG DATA
Geographical area: National
City: Madrid, Community of Madrid, Spain
Affiliation entity: UNE Asociación Española de Normalización
Start date: 2019

7 **Committee title:** CTN 320 Cybersecurity and Protection of Personal Data, Member of the committee in behalf of the Spanish National Research Council (CSIC)
Geographical area: National
City: Madrid, Community of Madrid, Spain
Affiliation entity: UNE Asociación Española de Normalización
Start date: 12/11/2018

8 **Committee title:** CTN 71/SC 307 Blockchain and distributed ledger technologies, Member of the committee in behalf of the Spanish National Research Council (CSIC)
Geographical area: National
City: Madrid, Community of Madrid, Spain
Affiliation entity: UNE Asociación Española de Normalización
Start date: 12/09/2018

Evaluation and revision of R&D projects and articles

1 **Performed tasks:** independent expert in the evaluation of proposals for the European Commission's HORIZON-CL3-2022-CS-01-02
Entity where activity was carried out: REA Safeguarding Secure Society **Type of entity:** State agency
City of entity: Brussels, Belgium
Start-End date: 12/12/2022 - 12/01/2023

2 **Name of the activity:** Evaluation of call for Industry Driven Research
Performed tasks: Project evaluator
Entity where activity was carried out: The Central Finance and Contracting Agency (CFCA **Type of entity:** State agency
City of entity: Riga, Latvija, Latvia
Start-End date: 05/11/2018 - 23/11/2018

3 **Name of the activity:** Certification of R&D projects (Certificación de Proyectos de I+D+I)
Performed tasks: Project evaluator
Entity where activity was carried out: UNE **Type of entity:** State agency
City of entity: Madrid, Community of Madrid, Spain
Start-End date: 02/02/2018 - 28/02/2018

4 **Performed tasks:** independent expert in the evaluation of proposals for the European Commission's H2020-DS-2016-2017
Entity where activity was carried out: REA Safeguarding Secure Society **Type of entity:** State agency
City of entity: Brussels, Belgium
Start-End date: 22/09/2017 - 06/10/2017

5 **Name of the activity:** RIS3 projects
Performed tasks: Project Evaluator
Entity where activity was carried out: Universidad Autónoma de Madrid **Type of entity:** University
Start-End date: 23/02/2017 - 10/03/2017

6 **Name of the activity:** Associate Editor
Performed tasks: International Journal of Bifurcation and Chaos
Start date: 01/01/2017

7 **Name of the activity:** Editor
Performed tasks: Complexity
Entity where activity was carried out: https://www.hindawi.com/journals/complexity/editors/
Start date: 04/04/2016

8 **Name of the activity:** Editor
Performed tasks: Discrete Dynamics in Nature and Society
Entity where activity was carried out: https://www.hindawi.com/journals/ddns/editors/
Geographical area: Non EU International
Start date: 06/04/2015

9 **Name of the activity:** Reviewer
Performed tasks: Computer Methods and Programs in Biomedicine
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 18/11/2013

10 **Name of the activity:** Reviewer
Performed tasks: PLosOne
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 7
Start date: 08/08/2013

11 **Name of the activity:** Reviewer
Performed tasks: Entropy
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 26/07/2013

12 **Name of the activity:** reviewer
Performed tasks: ieee journal of biomedical and health informatics
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 19/07/2013

13 **Name of the activity:** Reviewer
Performed tasks: Journal of Information Security and Applications
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 4
Start date: 15/01/2013

14 **Name of the activity:** Reviewer
Performed tasks: Nonlinear dynamics
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 2
Start date: 21/11/2012

15 **Name of the activity:** Revisor
Performed tasks: Information Security Technical Report
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 4
Start date: 06/11/2012

16 **Performed tasks:** journal of visual communication and image representation
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 8
Start date: 23/07/2012

17 **Name of the activity:** Reviewer
Performed tasks: Signal Processing: Image Communication
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 3
Start date: 28/04/2012

18 **Name of the activity:** Revisor
Performed tasks: Communications in Nonlinear Science and Numerical Simulation
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 15/04/2012

19 **Name of the activity:** Revisor
Performed tasks: Mathematical problems in engineering
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 2
Start date: 14/11/2011

20 **Name of the activity:** Revisor
Performed tasks: Journal of Systems and Software
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 6
Start date: 20/10/2011

21 **Name of the activity:** Revisor
Performed tasks: Physica A
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 3

Start date: 21/09/2011

22 **Name of the activity:** Revisor
Performed tasks: KSII Transactions on Internet and Information Systems
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 2
Start date: 28/08/2011

23 **Name of the activity:** Revisor
Performed tasks: The computer journal
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 8
Start date: 04/08/2011

24 **Name of the activity:** Revisor
Performed tasks: Proyectos postdoctorales de la Czech Science Foundation
Frequency of the activity: 1
Start date: 12/07/2011

25 **Name of the activity:** Revisor
Performed tasks: Journal of Cryptographic Engineering (JCEN)
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 26/06/2011

26 **Name of the activity:** Revisor
Performed tasks: Optics Communications
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 02/06/2011

27 **Name of the activity:** Revisor
Performed tasks: Information Sciences
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 14
Start date: 13/05/2011

28 **Name of the activity:** Revisor
Performed tasks: Mathematical & Computer Modelling
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 4
Start date: 12/04/2011

29 **Name of the activity:** Revisor
Performed tasks: Journal of the Franklin Insitute
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 3
Start date: 08/04/2011

30 **Performed tasks:** International Journal of Bifurcation and Chaos
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 24
Start date: 15/01/2010

31 **Name of the activity:** Revisor
Performed tasks: Inverse Problems and Imaging
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 28/12/2009

32 **Name of the activity:** Revisor
Performed tasks: Signal Processing
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 4
Start date: 18/08/2009

33 **Name of the activity:** Revisor
Performed tasks: CHAOS: AN INTERDISCIPLINARY JOURNAL OF NONLINEAR SCIENCE
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 3
Start date: 27/06/2009

34 **Performed tasks:** International Journal of Computer Mathematics
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 2
Start date: 17/06/2009

35 **Name of the activity:** Revisor
Performed tasks: IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-Part II
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 6
Start date: 21/04/2009

36 **Name of the activity:** Revisor
Performed tasks: International Journal of Computers and Applications
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 1
Start date: 17/04/2009

37 **Performed tasks:** International Journal of Modern Physics B
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 13
Start date: 26/02/2009

38 **Name of the activity:** Reviewer
Performed tasks: Physics Letters A
Type of activity: Review of articles in scientific or technological journals **Frequency of the activity:** 2
Start date: 27/11/2008

Other achievements

Stays in public or private R&D centres

1 **Entity:** FernUniversität in Hagen **Type of entity:** University
Faculty, institute or centre: Lehrgebiet Informationstechnik
City of entity: Hagen, Germany
Start-End date: 23/07/2007 - 21/09/2007
Goals of the stay: Doctorate
Provable tasks: Study and analysis of recent proposals in chaos-based cryptography. F.P.I. short stay.
Narrative explanation: Short stay associated to the PhD grant of the Programa Nacional de Formación de Personal Investigador. The host supervisor was Prof. Dr. Dr. Wolfgang A. Halang. This stay was part of the active collaboration with Dr. Shujun Li (Present address: Fachbereich Informatik und Informationswissenschaft , Department of Computer and Information Science, Universität Konstanz, Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany. email: Shujun.Li@uni.-konstanz.de, hooklee@gmail.com), and the main goal was the analysis of inverse problems in the context of the cryptanalysis of chaos-based cryptosystems. The core of the work was the dynamic reconstruction of chaotic systems from time series. Different statistical and system identification tools were used in the analysis of recent chaotic cryptosystems, and some of the results lead to three ISI papers. As a part of the stay, a discussion about symbolic dynamics was given in the Seminar “Applied symbolic dynamics of Unimodal Maps” (September 2007). After this stay the collaboration with Dr. Shujun Li has been very active and fluent, as it has allowed the concretion of eight peer-review papers and a book chapter.
Identify key words: Cryptography; Data protection; Disclosure of information

2 **Entity:** Universidad de Swansea **Type of entity:** University
Faculty, institute or centre: Institute of Advanced Telecommunications
City of entity: Swansea, West Wales and The Valleys, United Kingdom
Start-End date: 10/07/2006 - 08/09/2006 **Duration:** 2 months
Funding entity: Ministerio de Ciencia e Innovación. Investigación **Type of entity:** Organismo público
Goals of the stay: Doctorate
Narrative explanation: Short stay associated to the PhD grant of the Programa Nacional de Formación de Personal Investigador. The host supervisor was Professor Jaafar M. H. Elmirghani (Present address: Chair in Communication Networks and Systems, School of Electronic & Electrical Engineering, University of Leeds, Email: J.M.H.Elmirghani@leeds.ac.uk). The aim of this visit was to extend the results obtained from the previous stay at the group of Professor Elmirghani. This being the case, chaotic dynamics was applied to the concretion of a multi-user and multi-level spread spectrum communication system. The definition of this kind of communication systems requires first the selection of a set of chaotic sequences from a given group of chaotic systems, and second the coding of the selected chaotic sequences. The selection of chaotic sequences was carried out by different clustering methods and using the relative wavelet entropy between sequences. The codification of the selected chaotic sequences was done using Artificial Neural Networks, Self-Organizing Maps, and Support Vector Machines.
Identify key words: Cryptography; Data protection; Disclosure of information

3 **Entity:** Universidad de Swansea **Type of entity:** University
Faculty, institute or centre: Escuela de Ingenieros
City of entity: Swansea, West Wales and The Valleys, United Kingdom
Start-End date: 24/09/2001 - 26/06/2002 **Duration:** 9 months
Goals of the stay: Beca Erasmus
Provable tasks: Proyecto fin de carrera. Nota obtenida: Matrícula de honor

Narrative explanation: M. Sc. final dissertation under the supervision of Professor Jaafar M. H. Elmirghani (Present address: Chair in Communication Networks and Systems, School of Electronic & Electrical Engineering, University of Leeds, Email: J.M.H.Elmirghani@leeds.ac.uk). The work was focused on the application of chaotic dynamics and adaptive filtering to the identification of the communication channel, and on the design of a multi-level chaos-based communication system. Chaotic dynamics was used to design Wiener filters upon the Least Mean Squares (LMS) and Dynamic Based Deconvolution (DBD) formalisms, being the goal to solve the inverse problem related to the characterization of the communication channel. On the other hand, a spread spectrum communication system was designed using Artificial Neural Networks (ANN), Self-Organizing Maps (SOM), and different clustering techniques. The expectation-maximization (EM) algorithm, the Kohonen maps, and the neural-gas algorithm were used to select a subgroup of chaotic sequences from the set of chaotic sequences associated to a group of chaotic dynamical systems. ANN and SOM were trained to classify the selected chaotic sequences in order to codify them and to construct the communication system.
Identify key words: Data protection; Disclosure of information

Obtained grants and scholarships

1 **Name of the grant:** Contrato Juan de la Cierva
Aims: Post-doctoral
Awarding entity: Ministerio de Ciencia e Innovación **Type of entity:** Organismo público
Conferral date: 17/01/2011 **Duration:** 3 years
End date: 16/01/2014
Entity where activity was carried out: Universidad Autónoma de Madrid
Faculty, institute or centre: Escuela Politécnica Superior

2 **Name of the grant:** Contrato JAE-DOC
Aims: Post-doctoral
Awarding entity: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
Conferral date: 01/05/2010 **Duration:** 8 months
End date: 10/01/2011
Entity where activity was carried out: Consejo Superior de Investigaciones Científicas
Faculty, institute or centre: Instituto de Acústica

3 **Name of the grant:** Beca de Formación de Personal Investigador
Aims: Pre-doctoral
Awarding entity: Ministerio de Educación y Ciencia de España **Type of entity:** State agency
Conferral date: 01/08/2005 **Duration:** 4 years
End date: 31/07/2009
Entity where activity was carried out: Consejo Superior de Investigaciones Científicas
Faculty, institute or centre: Instituto de Física Aplicada

4 **Name of the grant:** Beca de Formación en Tecnologías de la Información
Aims: Formación en Tecnologías de la Información
Awarding entity: Centro Nacional de Información y Comunicación Educativa **Type of entity:** Centro adscrito al Ministerio de Educación y Ciencia
Conferral date: 01/01/2003 **Duration:** 2 years - 3 months
End date: 31/03/2005

5 **Name of the grant:** Beca ERASMUS
Aims: Beca ERASMUS
Awarding entity: Universidad de Sevilla **Type of entity:** University
Conferral date: 24/09/2001 **Duration:** 9 months
End date: 26/06/2002

Obtained accreditations/recognitions

1 **Description:** Valoración positiva del sexenio de investigación 01/01/2018 - 31/12/2023
Accrediting entity: Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI) **Type of entity:** State agency
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 20/05/2024

2 **Description:** Valoración positiva de los méritos investigadores (quinquenios) 01/01/2016 - 31/12/2020
Accrediting entity: COMISIÓN EVALUADORA DEL DESEMPEÑO DE LA ACTIVIDAD CIENTÍFICO-TECNOLÓGICA
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 2021

3 **Description:** Valoración positiva del sexenio de investigación 01/01/2006 - 31/12/2011
Accrediting entity: Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI) **Type of entity:** State agency
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 26/06/2018

4 **Description:** Valoración positiva del sexenio de investigación 01/01/2012 - 31/12/2017
Accrediting entity: Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI) **Type of entity:** State agency
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 26/06/2018

5 **Description:** Valoración positiva de los méritos investigadores (quinquenios) 01/01/2006 - 31/12/2010
Accrediting entity: COMISIÓN EVALUADORA DEL DESEMPEÑO DE LA ACTIVIDAD CIENTÍFICO-TECNOLÓGICA
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 2018

6 **Description:** Valoración positiva de los méritos investigadores (quinquenios) 01/01/2011 - 31/12/2015
Accrediting entity: COMISIÓN EVALUADORA DEL DESEMPEÑO DE LA ACTIVIDAD CIENTÍFICO-TECNOLÓGICA
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 2018

7 **Description:** Mejor artículo de investigación en la Jornadas Nacionales de Ciberseguridad, JNIC 2017: A coercion-resistant and easy-to-use Internet e-voting protocol based on traceable anonymous certificates
Accrediting entity: IIII Jornadas Nacionales de Inves- tigación en Ciberseguridad
City accrediting entity: Madrid,
Date of recognition: 2017

8 **Description:** Evaluación positiva en la figura de Profesor Contratado Doctor
Accrediting entity: Agencia Nacional de Evaluación de la Calidad y Acreditación **Type of entity:** Organismo público
Date of recognition: 17/07/2012

9 **Description:** Evaluación positiva en la figura de Profesor de Universidad Privada
Accrediting entity: Agencia Nacional de Evaluación de la Calidad y Acreditación **Type of entity:** Organismo público
Date of recognition: 17/07/2012

10 **Description:** Evaluación positiva en la figura de Profesor Contratado Doctor
Accrediting entity: ACAP **Type of entity:** Organismo público
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 03/10/2011

11 **Description:** Evaluación positiva en la figura de Profesor de Universidad Privada
Accrediting entity: ACAP **Type of entity:** Organismo público
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 03/10/2011

12 **Description:** Evaluación positiva en la figura de Profesor Ayudante Doctor
Accrediting entity: ACAP **Type of entity:** Organismo público
City accrediting entity: Madrid, Community of Madrid, Spain
Date of recognition: 19/11/2010

13 **Description:** Evaluación positiva en la figura de Profesor Ayudante Doctor
Accrediting entity: Agencia Nacional de Evaluación de la Calidad y Acreditación **Type of entity:** Organismo público
Date of recognition: 15/02/2010

Summary of other achievements

1 **Description of the achievement:** Co-organizer of the workshop "Blockchain: mitos, realidades y posibilidades" (http://catedrauamibm.com/jornada-blockchain/)
Accrediting entity: IBM-UAM Chair **Type of entity:** University
City accrediting entity: Madrid, Community of Madrid, Spain
Conferral date: 19/10/2107

2 **Description of the achievement:** Organizador del workshop Workshop on Beyond the promises of web3.0: foundations and challenges of trust decentralization (WEB3-TRUST) en el congreso Blockchain
Conferral date: 01/05/2023

3 **Description of the achievement:** Organizador del workshop Workshop on Beyond the promises of web3.0: foundations and challenges of trust decentralization (WEB3-TRUST) en el congreso Blockchain
Conferral date: 01/05/2022

4 **Description of the achievement:** Co-organizer of the Special Session "Identification, simulation and prevention of security and privacy threats in modern communication networks"
Accrediting entity: CISIS'17, Universidad de León
City accrediting entity: León, Castile and León, Spain

Conferral date: 06/09/2017

5 **Description of the achievement:** Technical Report on non-conventional digital signatures
Accrediting entity: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City accrediting entity: Madrid, Community of Madrid, Spain
Conferral date: 10/07/2017

6 **Description of the achievement:** Technical Assistance (No de Proyecto: WNN15SOF01. Realización de Servicios Tecnológicos a través de profesores e investigadores (Expertos) de la Escuela Politécnica Superior de la UAM)
Accrediting entity: Acker & Partners
City accrediting entity: Madrid, Community of Madrid, Spain
Conferral date: 01/06/2017

7 **Description of the achievement:** Technical Report on cryptographic zero-knoledge proofs in e-voting platforms
Accrediting entity: Consejo Superior de Investigaciones Científicas **Type of entity:** State agency
City accrediting entity: Madrid, Community of Madrid, Spain
Conferral date: 10/03/2017

8 **Description of the achievement:** Co-organizer of the Special Session "Digital Identities Management by means of non-standard digital signatures schemes" at CISIS'15
City accrediting entity: Burgos, Castile and León, Spain
Conferral date: 17/06/2015

9 **Description of the achievement:** Member of the working group "Aesthetics and politics of the pro-common" ("Estética y política del procomún")
Accrediting entity: Medialab Prado **Type of entity:** Centro cultural
City accrediting entity: Madrid, Community of Madrid, Spain
Conferral date: 29/04/2010

10 **Description of the achievement:** Co-organizer of the Special Session "Theoretical, Technical, and Experimental Challenges in Closed-Loop Approaches in Biology" at the 10th AIMS Conference on Dynamical Systems,Differential Equations and Applications.
City accrediting entity: Madrid, Community of Madrid, Spain

11 **Description of the achievement:** Member of the Scientific Program committee of the 2009 IEEE International Symposium on Circuits and Systems, 6th International Multi-Conference on Systems, Signals and Devices

12 **Description of the achievement:** Member of the Scientific Program committee of the 8th International Multi-Conference on Systems, Signals and Devices-SSD'11

13 **Description of the achievement:** Member of the International Program Committee of the Third IFAC CHAOS http://www.ipicyt.edu.mx/Chaos12/corganizador.html

14 **Description of the achievement:** Miembro del Comité de programa del Segundo Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS 2012): http://www.utpl.edu.ec/tibets/?q=node/10

15 **Description of the achievement:** Reviewer fo the ISIEA 2012, 2012 IEEE Symposium on Industrial Electronics and Applications

16 **Description of the achievement:** Reviewer for the ICCES'2012, The Eight International Conference on Computer Engineering and Systems