institute imdea software

science
and technology
for developing
better software

annual report 2021

software.imdea.org

software

foreword

Manuel Carro
Director, IMDEA Software Institute
October 10, 2022

Computers have a prominent role in our lives. Many, if not most, of us work primarily with a computer or use computers to get our daily job done. We use them to communicate with our friends, to shop, and to spend some leisure time watching movies or playing games. We continuously tap on the screen of smartphones, which are sophisticated computers equipped with a SIM reader, a phone app, and a camera. But few people realize up to which point computers, and therefore computer science, play an essential role in our society. It is not too bold to state that computer science has become the foundation on which the fabric of our society is built. Let us imagine, for a moment, that a magical spell causes all the software in the world to stop. Everything else is just right: screens are on, communication lines are up... but, for some reason, programs just do not run. What would happen, then?

Of course, our laptops stop working, as well as our smartphones. TV sets also cease to function: these days, a TV is a small computer with a big screen. Cars will be hit hard: a modern car is mainly a set of many small computers and controllers linked together and executing sophisticated software that receives signals and commands from the environment and reacts to them acting on the physical components of the car: brakes, lights, engine, wheels,...

The power grid will also suffer. The transmission of power in the electricity lines is governed by programs that monitor consumption, production, and prices and try to match them. Without this control, mismatches can cause problems in the production and distribution plants and, eventually, blackouts. Hospitals, which keep the information on their patients in databases, will see their ability to function normally seriously impaired when the access to this data is lost.

This list can go on and on: in a modern society, there are computing devices behind the scenes doing a silent job practically everywhere. Remaining unnoticed and eventually blending with the background is what one would expect of a truly useful technology: be at our service without being a hurdle. This, however, is easier said than done. We expect that when we touch a smartphone screen, a bank transfer is made across the globe within milliseconds. This simple act invokes an immense amount of technology whose creation required huge doses of ingenuity, and is based on rigorous mathematical and logical foundations. All of this, and more, falls within what we call computer science and information technologies – two disciplines so wide that describing them in a short and meaningful way is a daunting, if at all possible, task.

At this point it should be intuitively clear that ensuring that a system of this complexity works seamlessly while being reliable and scalable, and keeping the economic costs of developing and maintaining it within reasonable bounds, is extremely challenging. There is a wide variety of functionality that we expect from such a computer system. Is my data safe, or can it be stolen? Are my communications really private, or is it possible for a malicious third party to be aware of my conversations? How much energy does a given program need to run, and therefore for how long can it run with a given energy storage? Can we have reasonable guarantees that the programs in a car will not halt to a freeze or start malfunctioning due to a hacker attack?

These are some of the questions that the research at the IMDEA Software Institute tries to answer. The IMDEA Software Institute is an advanced research institution created under the umbrella of the Regional Government of Madrid, as part of a series of seven Institutes performing world-class research in several areas of high practical relevance for the society. These advances are made available both to the scientific community through the usual academic channels and to the industrial ecosystem through research contracts and joint projects, and they eventually trickle down to the society as improvements in the products that we use, perhaps without noticing, every day.

Among the work that the Institute does, we can cite research and advances in computer security, privacy, cryptography, secure computation, analysis of energy consumption, safety of mobile and aerospace software, distributed systems, blockchain, advanced programming languages, techniques to prove programs correctness, execution optimization, and the use of machine learning as a support of these areas. The way in which our work impacts society is not by directly creating or improving the programs, apps, and devices that we use every day, but by discovering the science and technology that makes it possible to develop better tools with which software engineers can generate in an easier and faster way applications that are safer and more efficient.

The relevance and timeliness of this research is witnessed by academic recognitions at several levels and the industrial interest it has generated. At the moment of writing, four researchers of the Institute are recipients of two Starting and two Consolidator ERC grants, the most prestigious scientific grants awarded in Europe by a public body. In relative terms, the IMDEA Software Institute holds 27% of all the ERC Starting + Consolidator grants that are, at this moment, active in Spain in the area of Information Technologies. For an institution the size and age of IMDEA Software, this is a truly remarkable achievement.

The Institute has been awarded close to 150 grants, fellowships, and contracts since its inception, which brought to the Institute close to 30MC in funds (roughly, an average of 30% of its budget during this period, being smaller at the beginning and reaching close to a 50% in the last years) from Regional, National, European, and International agencies, and from private companies. Among the latter, the Institute has had contracts with well-known companies such as Google, Amazon, Facebook, GMV, INDRA, BBVA, Microsoft Resarch, and Intel, and also with other more specialized companies which work on products that sustain the software infrastructure, such as Nomadic Labs, Nextel, LogicBlox, RedBorder, and Zemsania. In addition to that, the Institute has collaborated in joint projects with a very large number of companies which include most, if not all, the "usual suspects" in the IT world.

Undoubtedly, the most precious asset of the Institute is its staff, from administration and support to the researchers. In this last category, the Institute has managed to attract a selected team coming from some of the most renowned universities and research centers in the world – among them some Spaniards who, after spending some years abroad, found an attracting opportunity to return to their country. Our researchers routinely publish in the highest-ranked venues and receive prizes for their work, such as best paper and best thesis awards. In addition to that, they contribute to strengthening the education work of local universities by advising students through agreements with these universities. At the moment of writing, IMDEA Software researchers have been advisors of 48 PhD, 50 MSc, and 23 BSc theses.

Besides the research activities, the IMDEA Software Institute also takes care of managing REDIMadrid, the regional telecommunications network for research and higher-education, giving 24/7 service to more than 330,000 users.

More than 90 people work currently at the Institute, 75 of which are focused on research. Those with a PhD obtained it from top-level institutions such as Stanford, Carnegie Mellon, the University of Cambridge, ETH Zürich, Purdue University, the University of California at San Diego, the Università of the Svizzera Italiana... The Institute is a truly international place where right now a 65% of its research personnel is originally from abroad.

All of them, regardless of their position or mission, share a common trait: the passion and dedication that they show every day in their tasks and in the overarching objective of improving the society through science and technology.

We hope that the rest of this annual report can show a meaningful and useful snapshot of the Institute and its activities. Up-to-date news can always be found at our website, **www.software.imdea.org.**

I would like to once more thank all who have contributed to the achievements of the Institute so far, including of course the Madrid Regional Government and Assembly for their vision and support, and very specially all the staff of the Institute at all levels. It is their enthusiasm, dedication, and passion that has allowed the Institute reach this level in a so short amount of time.

annual report 2021

software.imdea.org

editor
IMDEA Software Institute

graphic design
loveodesign.es

contents

contents

about us

methods

languages

tools

The IMDEA Software Institute is a non-profit, independent research institute promoted by the Madrid Regional Government to perform research of excellence and technology transfer in the methods, languages, and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., software which is **safe**, **reliable**, and **efficient**. The attraction and retention of talent has been identified since the beginnings of the Institute as the main mechanism to achieve these goals.

The IMDEA Software Institute is part of the Madrid Institutes for Advanced Studies (IMDEA), an institutional framework created to foster **social and economic growth** in the region of Madrid by promoting research of excellence and technology transfer in a number of strategic areas with high potential impact.

Since 2013, the IMDEA Software Institute is located in its headquarters building, at the **Montegancedo Science and Technology Park**. The campus has the "International Campus of Excellence" label, and the "Campus of Excellence in Research and Technology Transfer" award from the Spanish government. It is an ideal environment for fulfilling the mission of **attraction of talent, research, and technology transfer**. It is highly energy-efficient, through energy-conscious design, co-generation, and full automation.

The building also provides ample space for strategic activities such as the **Madrid Co-location Center of the EIT Digital KIC** and collaboration activities with industry.

The location of the IMDEA Software building provides excellent access to the UPM School of Computer Science, with which we maintain excellent and fruitful ties, as well as to the other research centers within the Campus and convenient access to the other Madrid universities and IMDEA Institutes.

about us

the institute at a glance

2021 in figures

71 Researchers

31 Interns

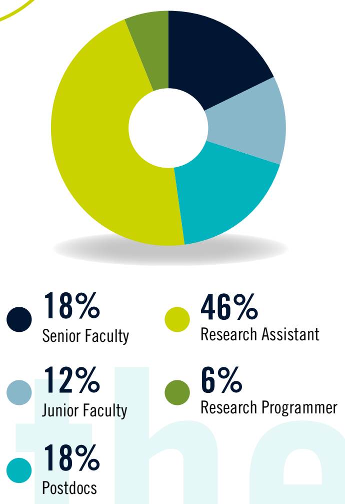
29 Nationalities

5 Ph.D. thesis

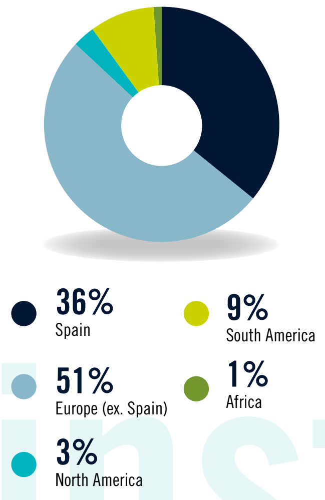
15 Active fellowships

25 Active projects

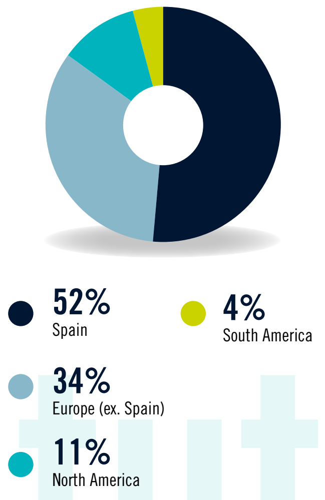
Researchers



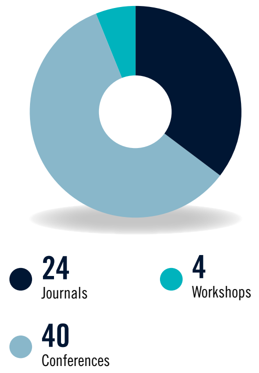
Nationalities



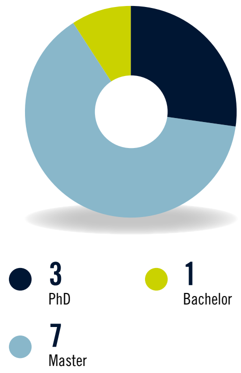
Where Ph.D.was obtained



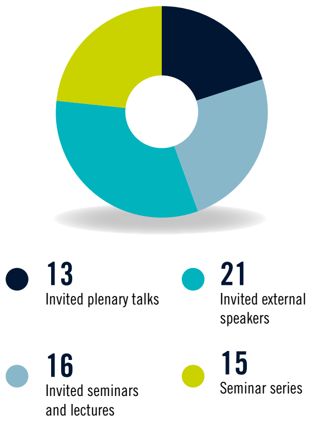
Publications



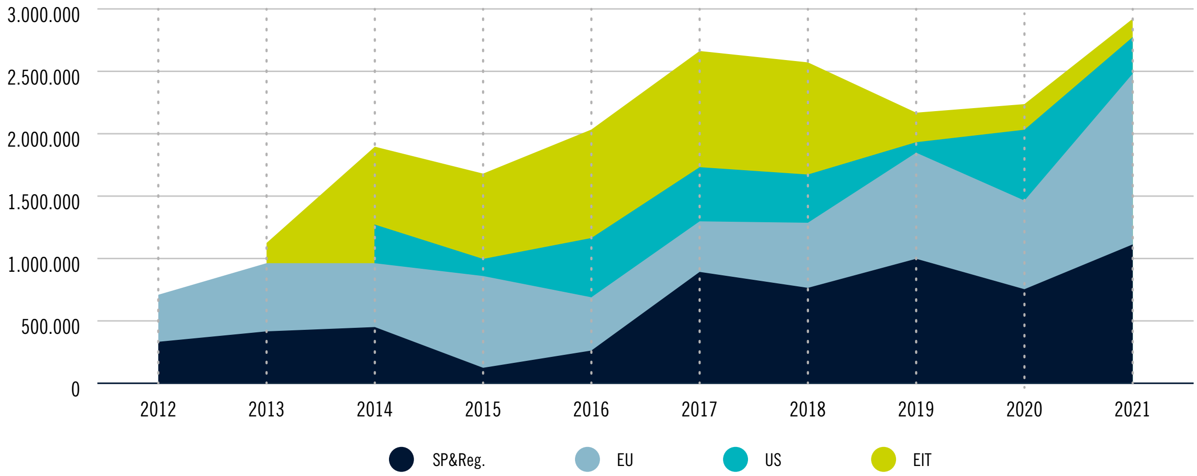
Thesis



Invited talks



R&I External Income



Accumulated projects & fellowships

105

Projects since 2008

36

Fellowships since 2008

motivation and goals:

the economic landscape of software production

It is difficult to overstate the importance of software in both our daily lives and in the industrial processes that, running behind the scenes, sustain the modern world. Software is the enabling technology behind many devices and services that are now essential components of our society, ranging from large critical infrastructures on which our lives depend (cars, planes, air-traffic control, medical devices, banking, the stock market, etc.) to all the devices that are now part of our lives such as cell phones, tablets, computers, digital televisions, and the Internet itself. Software has not only facilitated improved solutions to existing problems, but has also started modern revolutions like social networks that change the way we interact with our environment and communicate with each other.

This pervasiveness explains the global figures around software: studies and macroeconomic simulations reported in *The EU Sector its R&D Performance*, predict an increase in the value added for the ICT sector from e642 bn in 2019 to e666 bn in 2022 and an increase in productivity per person employed in ICT from e105 thousand/person in 2019 to e107 thousand/person on 2021. Moreover, according to the report *Shaping the Digital Transformation in Europe*, the cumulative additional GDP contribution of new digital technologies by 2030 could amount to e2.2 trillion in the EU, which is a 14.1% increase from 2017.

This increase cannot however materialize without a corresponding investment to nurture the ecosystem in which digital technologies are created and to facilitate the conditions in which these technologies can be effectively adopted and put to work. It is estimated that European institutions and governments may need to contribute approximately e75 billion per year in ICT in the next ten years to narrow the digital gap between European Member states. In this line, education and re-skilling labor force to take advantage of the digital transition may require investments of up to e42 billion per year. At the same time, the estimated amount of personnel working in ICT during the period 2019-2021 was stable, which means that the sector was resilient enough to fight off the effects of the 2019 COVID-19 pandemic.

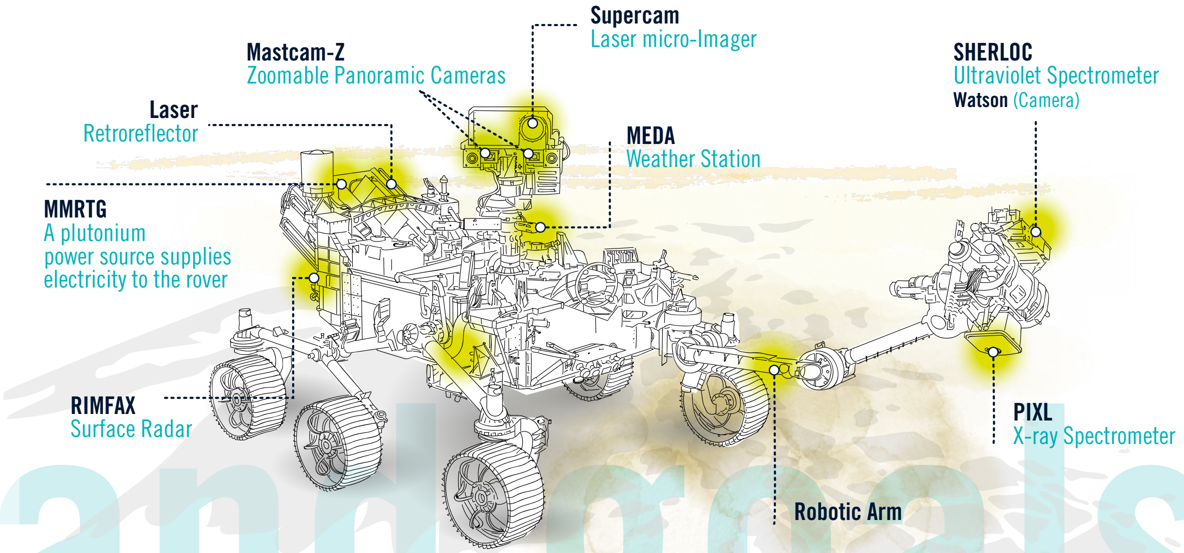
A relevant aspect revealed by this simulation is the positive effect in all Member States, independently of the point where they start. But proactive convergence measures are needed to avoid an uneven distribution of effects of digital innovation and to bypass the differences in the capacity of absorption of their industrial fabric and capability to adopt new technologies.

This study underlines once more the relevance of ICT, and how it can contribute to shape the future economy and society — as it has done so far. That reinforces our belief that the mission of the Institute is fully aligned with advances that are expected to bring deep changes to the society and to the work landscape. For this interrelationship to take place, we need a continuous layer of research that feeds the innovation process and eventually produces new solutions. In order for this pipeline not to stall, investments in all sectors have to be adequately balanced. There is, therefore, a need not to stop investing in basic research in the post-pandemic world. Earmarking funds for other, more pressing needs to achieve a quick fix for a troubling situation is a temptation, but that should not get in the way of taking strategic steps towards a better future.

On the other hand, the growing relevance and pervasiveness of software makes failures and vulnerabilities in software have a social and economic cost that his higher as time passes. The results of malfunctioning apps go from being annoying to posing serious social and legal problems (such as the ever more common issues caused by systems labeled as having Artificial Intelligence inside that take decisions on behalf of humans and which directly impact people) to having high economic cost or even threats to human lives (e.g., a malfunctioning airplane or medical device). A 2018 report from the *Consortium for IT Software Quality (CISQ)* reckons that poor-quality software products (including legacy systems that could not be substituted by more advanced versions and need delicate maintenance, cancelled projects, and the estimated value of technical debt) incurs a global extra cost of $2.4 trillion *in the US alone*. If we restrict ourselves only to massive bug-related failures, the figure is reduced to $1.2 trillion — still a staggering amount.

The main mission of the IMDEA Software Institute is to tackle these and other related challenges by performing research of excellence in methods and tools to develop software products with sophisticated functionality and high quality while keeping the software development cost-effective and making it less error-prone. We do that by focusing on approaches that are rigorous and with solid foundations, but which at the same time allow building practical tools. The research focus includes all phases of the development cycle (analysis, design, implementation, verification, validation, maintenance, and evolution).

In order to achieve its mission, the IMDEA Software Institute gathers a critical mass of top-class researchers world-wide, and at the same time develops synergies between them and the significant research base and industrial capabilities existing in the region.



Perseverance ROVER Instruments – NASA Mars Mission

legal status, governance, and management

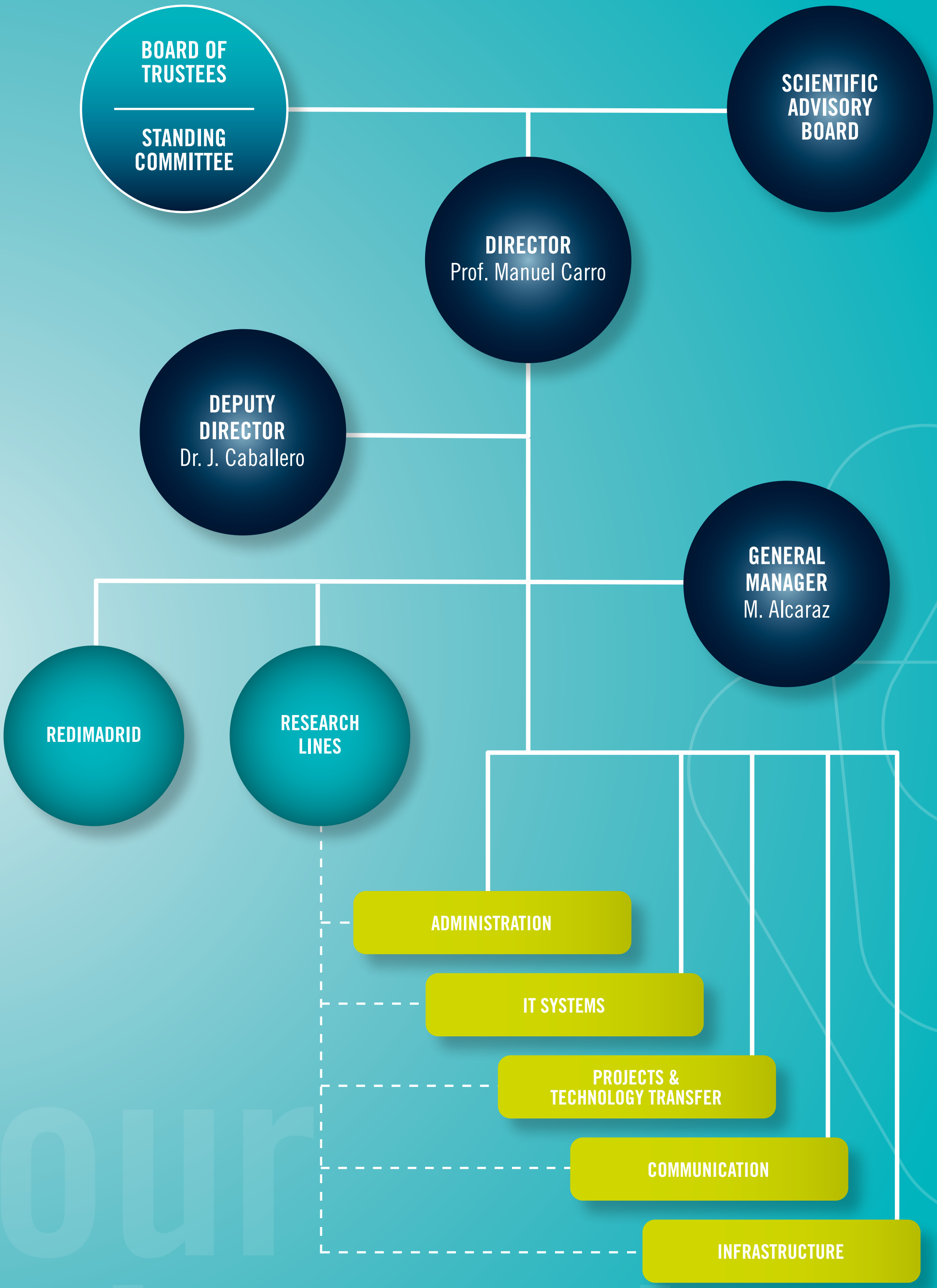
The IMDEA Software Institute is a foundation, which brings together the advantages and guarantees associated with that structure with the flexible and dynamic management more typical of a private body. This combination is deemed necessary to attain the goals of excellence in research, cooperation with industry, and attraction of talented researchers from all over the world, while managing a combination of public and private funds. The Institute was created officially on November 23, 2006 at the initiative of the Madrid Regional Government, following a design that was the result of a collaborative effort between industry and academia, and started its activities during 2007.

The main governing body of the Institute is the **Board of Trustees**. The Board includes representatives of the Madrid Regional Government, universities and research centers of Madrid, scientists with high international reputation in software development science and technology, and representatives of companies, together with independent experts.

The Board is in charge of guaranteeing the fulfillment of the foundational purpose and the correct administration of the funds and rights that make up the assets of the Institute, maintaining their appropriate returns and utility. It normally meets twice a year. In the interim, Board-level decisions are delegated to the **Standing Committee** of the Board. The **Director**, who is the CEO of the Institute, is appointed by the board among scientists with a well-established international reputation in software development science and technology. The Director fosters and supervises the activities of the Institute, and establishes the distribution and application of the available funds among the goals of the Institute, within the patterns and limits decided by the Board of Trustees. The Director is assisted by the **Deputy Director** and the **General Manager**, who take care of the legal, administrative, and financial activities of the Institute. Together, they supervise the different units in the Institute (administration, IT support, project management, communication, infrastructure, and REDIMadrid) which work closely with and support the **Research** units of the Institute.

The Board of Trustees and the Director are assisted in their functions by the **Scientific Advisory Board**, composed of high-level external scientists of international reputation with expertise in different areas of research covered by the Institute. The tasks of this advisory board include: to provide advice on and approve the selection of researchers; to provide advice and supervision in the preparation of yearly and longer-term strategic plans; to evaluate the performance with respect to those plans; and to give general advice on matters of relevance to the Institute.

our structure



BOARD OF TRUSTEES

STANDING COMMITTEE

SCIENTIFIC ADVISORY BOARD

DIRECTOR
Prof. Manuel Carro

DEPUTY DIRECTOR
Dr. J. Caballero

GENERAL MANAGER
M. Alcaraz

REDIMADRID

RESEARCH LINES

ADMINISTRATION

IT SYSTEMS

PROJECTS & TECHNOLOGY TRANSFER

COMMUNICATION

INFRASTRUCTURE

members of the governing bodies

Members of the Board of Trustees
and the Scientific Advisory Board as of Dec. 31st, 2020.

BOARD OF TRUSTEES

SCIENTIFIC ADVISORY BOARD

our structure

CHAIRMAN OF THE FOUNDATION

PROF. ROBERTO DI COSMO
Université Paris Diderot and INRIA, France.

VICE-CHAIRMAN OF THE FOUNDATION

ILMO. SR. D. ENRIQUE OSSORIO CRESPO
Councilor for Education, Universities, Science, and Office of Spokesperson, Madrid Regional Government, Spain.

REGIONAL GOVERNMENT AND PUBLIC ENTITIES

JOSÉ ANTONIO SÁNCHEZ SERRANO
Vice-Councilor for Local Administration and Digitization, Regional Ministry of Local Administration and Digitization.

FIDEL RODRÍGUEZ BATALLA
Vice-Councilor for Universities, Science, and Innovation, Regional Ministry of Education, Universities, and Science.

ANA ISABEL CREMADES RODRÍGUEZ
Director-General for Research and Technological Inovation, Regional Ministry of Education, Universities, and Science.

RICARDO DÍAZ MARTÍN
Director-General for Universities and Higher Art Studies, Regional Ministry of Education, Universities, and Science.

BÁRBARA FERNÁNDEZ-REVUELTA FERNÁNDEZ-DURÁN
Deputy Director-General for Research and Technological Inovation, Regional Ministry of Education, Universities, and Science.

JOSÉ DE LA SOTA RIUS
General Coordinator, Fundación para el Conocimiento madri+d, Madrid, Spain.

UNIVERSITIES AND PUBLIC RESEARCH BODIES

PROF. NARCISO MARTÍ OLIET
Universidad Complutense de Madrid, Spain.

PROF. JUAN JOSÉ VAQUERO LÓPEZ
Universidad Carlos III de Madrid, Spain.

PROF. FRANCISCO JAVIER SORIANO CAMINO
Universidad Politécnica de Madrid, Spain.

PROF. JESÚS M. GONZÁLEZ BARAHONA
Universidad Rey Juan Carlos, Madrid, Spain.

SCIENTIFIC TRUSTEES

PROF. PATRICK COUSOT
Courant Institute, New York University, USA.

PROF. JOSÉ MESEGUER
University of Illinois at Urbana Champaign, USA.

PROF. LUÍS MONIZ PEREIRA
Universidade Nova de Lisboa, Portugal.

PROF. MARTIN WIRSING
Ludwig-Maximilians-Universität München.

INDEPENDENT EXPERT

JESÚS CONTRERAS CINO
Fundación EIT Digital Spain, Director.

SECRETARY

ALEJANDRO BLÁZQUEZ LIDOY

PROF. ROBERTO DI COSMO
Universitè Paris Diderot and INRIA, France. Chairman of the Board.

PROF. MARÍA ALPUENTE
Universidad Politécnica de Valencia, Spain.

PROF. PATRICK COUSOT
Courant Institute of Mathematical Sciences, New York University, USA.

PROF. VERONICA DAHL
Simon Fraser University, Vancouver, Canada.

PROF. JOSÉ MESEGUER
University of Illinois at Urbana Champaign, USA.

CATUSCIA PALAMIDESSI
INRIA Saclay and LIX, France.

PROF. LUIS MONIZ PEREIRA
Universidade Nova de Lisboa, Portugal.

PROF. MARTIN WIRSING
Ludwig-Maximilians-Universität, München, Germany.

cooperation

Companies with which IMDEA Software Cooperated during 2021

SENER Aeroespacial

Mellanox TECHNOLOGIES

NOKIA

BT

Microsoft Research

iXblue

IDQ

Telefónica Investigación y Desarrollo

galois

fragmentiX QUANTUM SAFE STORAGE SOLUTIONS

ENERGIE AG Oberösterreich

ferrovial

ADVA Optical Networking

the REUSE company

nomadic labs

GENERA TECNOLOGIAS

CITYCOM www.citycom-austria.com

TOSHIBA Leading Innovation

gmv INNOVATING SOLUTIONS

centum tech&motion

Stellar

NOKIA Bell Labs

intel

ROHDE&SCHWARZ Cybersecurity

Atos

Mt Pelerin

Protocol Labs

orange

NEC

NPL

VISA

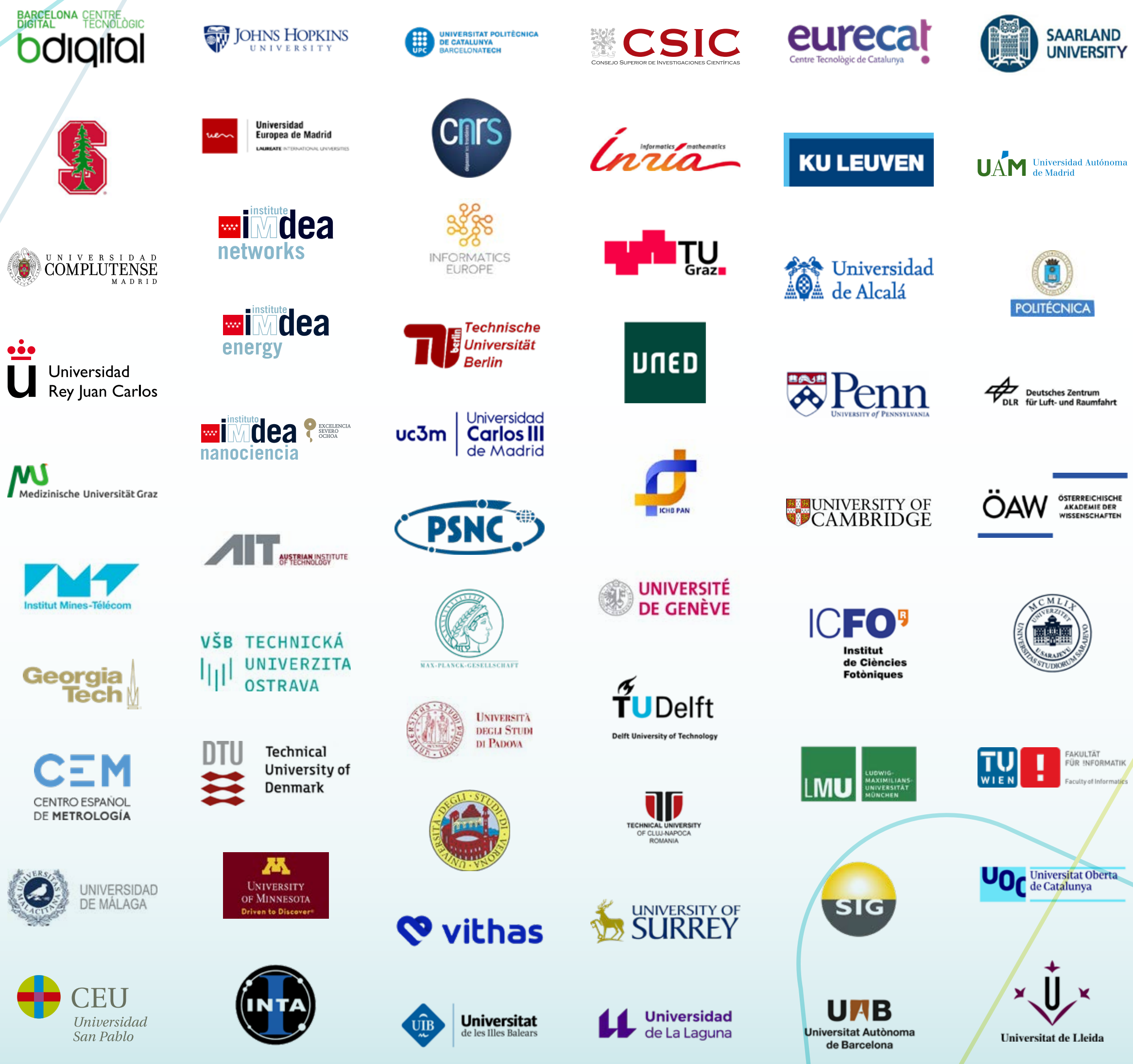
MARM Sistemas

indra

Deutsche Telekom

DEVELOPAIR

Academic Institutions with which IMDEA Software Cooperated during 2021


BARCELONA DIGITAL CENTRE TECNOLÒGIC bdigital
JOHNS HOPKINS UNIVERSITY
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH UPC
CSIC Consejo Superior de Investigaciones Científicas
eurecat Centre Tecnològic de Catalunya
SAARLAND UNIVERSITY
Universidad Europea de Madrid LAUREATE INTERNATIONAL UNIVERSITIES
cnrs
Inria informatics mathematics
KU LEUVEN
UAM Universidad Autónoma de Madrid
institute imdea networks
INFORMATICS EUROPE
TU Graz
Universidad de Alcalá
POLITÉCNICA
UNIVERSIDAD COMPLUTENSE MADRID
institute imdea energy
Universidad Rey Juan Carlos
Technische Universität Berlin
UNED
Penn UNIVERSITY of PENNSYLVANIA
DLR Deutsches Zentrum für Luft- und Raumfahrt
instituto imdea nanociencia EXCELENCIA SEVERO OCHOA
uc3m Universidad Carlos III de Madrid
MU Medizinische Universität Graz
ICHB PAN
UNIVERSITY OF CAMBRIDGE
ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
PSNC
Institut Mines-Télécom
MAX-PLANCK-GESELLSCHAFT
UNIVERSITÉ DE GENÈVE
ICFO Institut de Ciències Fotòniques
MCMLIX UNIVERSITAS STUDIORUM SARAJEVENSIS
VŠB TECHNICKÁ UNIVERZITA OSTRAVA
Georgia Tech
UNIVERSITÀ DEGLI STUDI DI PADOVA
TU Delft Delft University of Technology
CEM CENTRO ESPAÑOL DE METROLOGÍA
DTU Technical University of Denmark
UNIVERSITAS DEGLI STUDI DI VERONA
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
TU WIEN FAKULTÄT FÜR INFORMATIK Faculty of Informatics
UNIVERSIDAD DE MÁLAGA
UNIVERSITY OF MINNESOTA Driven to Discover
vithas
UNIVERSITY OF SURREY
SIG
UOC Universitat Oberta de Catalunya
CEU Universidad San Pablo
INTA
UIB Universitat de les Illes Balears
Universidad de La Laguna
UAB Universitat Autònoma de Barcelona
Universitat de Lleida

Other Publicly-Funded Institutions with which IMDEA Software Cooperated during 2021

Comunidad de Madrid
fundación para el conocimiento madri+d
eit Digital
RedIRIS
red.es

Industrial Partnerships

Incorporating scientific results and technologies into processes and products is key to increase the competitiveness of industry. It also contributes to sustainable growth and creates jobs. As a generator of new knowledge in the ICT area, IMDEA Software is committed to the transfer of innovation to industry. *Collaborative projects* (funded through competitive public calls) and *direct industrial contracts* are the key instruments through which collaboration with industry is conducted. Through both, the Institute has established *strategic partnerships* with the main stakeholders in the sector to enable long-term collaboration.

In particular, the Institute has established close ties with Telefónica, Indra, NEC Labs Europe, Nomadic Labs, Tezos Foundation, GMV, Sener, and Atos, among others, which have led to a number of strategic cooperation initiatives.

An important instance of these initiatives was the creation of the Spanish Associate Partner Group of EIT Digital with Telefónica, Indra, Atos, and UPM that eventually, under the leadership of IMDEA Software, evolved towards the status of Full Node in January 2017. Another instance is the participation of the Institute in the Spanish Network of Excellence on Research on Cybersecurity (RENIC) and the European Cybersecurity Organization (ECSO) that implements the Cyber Security Public-Private Partnership (cPPP) of the European Commission.

Finally, as a result of these industry-joint initiatives, we want to highlight the joint application with NEC Labs of several PCT patent requests that currently are under revision.

The Institute also has a strong presence in national and international bodies. It is a member of *Informatics Europe*, the organization of all deans, chairs, and directors of the leading Departments and Institutes of Computer Science in Europe, whose mission is to study issues of common interest and design solutions to shared problems. Manuel Hermenegildo, Director of the Institute until mid-2017, was Vice-President of Informatics Europe.

All these activities contribute towards aligning research agendas and promote joint participation in projects. Good examples of this are the *MadridFlightOnChip* project, awarded by the Madrid Regional Government, in which IMDEA Software collaborates with companies of the Madrid region working in the aerospace sector, and the *OPENQKD* project, funded by the European Union and in which the Institute collaborates with 16 of the principal european telecomunication companies to develop the future quantum european network.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

RENIC
Red de Excelencia Nacional de Investigación en Ciberseguridad

eit Digital

The currently active projects and contracts are described elsewhere in this report, including a table with the list of companies the Institute has collaborated so far.

Commercialization of Technology

Commercialization of technology is another important form of technology transfer. Given the global controversy around software patents and their legal status in Europe, the Institute combines intellectual property protection with other exploitation models based on licensing. As an example of the former, the Institute routinely performs software registrations of the prototypes developed (e.g., ActionGUI — jointly developed by IMDEA Software and ETH Zürich—, MIST, LEAP, CacheAudit, GGA, and EasyCrypt, ZooCrypt and Masking, these last three developed jointly with INRIA). As an example of the latter, the technology generated through Cadence, an EIT Digital project, was licensed to Communication Valley Reply.

Other Industrial Funding and Collaborations

Other forms of collaboration with industry include the *industrial funding of research assistants* working at the Institute, (e.g., Protocol Labs funds research students working on cryptography), *research stays of Institute researchers at company premises* (e.g., Institute researchers have made industrially-funded extended stays at Microsoft Redmond in the US, Microsoft Cambridge in the UK, Facebook in the UK, Protocol Labs, and elsewhere), *access to the Institute's technology and scientific results* (e.g., researchers of the Institute frequently meet with representatives from the most relevant companies in the IT sector to present research results). In addition, the Institute is open to giving access to the Institute's researchers as consultants and to the participation of company staff in Institute activities.

Academic Partnerships

An important way to cooperate with other academic institutions is through *collaborative projects* funded through competitive calls or industrial contracts. The Institute has also established *longer-term*, *strategic partnerships* with a number of research institutions in the Madrid region and elsewhere to reach objectives that go beyond those of individual projects. At present the Institute has active long-term agreements with several universities and research and innovation centers and associations, among which we can count:

- Universidad Politécnica de Madrid.
- Universidad Complutense de Madrid.
- Universidad Rey Juan Carlos.
- Universidad Autónoma de Madrid.

- University of Verona, Italy.
- Sapienza University of Rome, Italy.
- Roskilde University, Denmark.
- Fundación madri+d para el Conocimiento, Madrid.
- EIT Digital Spain, Madrid.

These agreements establish a framework to develop collaborations that go beyond research projects and include, e.g., the joint development of graduate programs, shared use of resources, equipment, and infrastructure, the association of researchers and research groups with the Institute, or joint commercialization of technology.

As examples that illustrate the importance of these agreements, the agreements with the Universidad Politécnica de Madrid (UPM) included hosting the Institute building in its Montegancedo Science and Technology Park and paves the way for teaching activities at different levels at the School of CS of the UPM, including the supervision of research assistants registered as PhD students at UPM. Similar agreements with other Universities, both in Spain and abroad, make it possible for the Institute to participate in student training activities by hosting interns who earn credits for their degrees while performing research and development under the advising of our researchers. Under the agreement with Roskilde University, one of its full professors —John Gallagher— is also part-time senior researcher at the Institute. The contracts withe NEC Labs Europe also include the agreement to host researchers in the Institute facilities to facilitate collaboration.

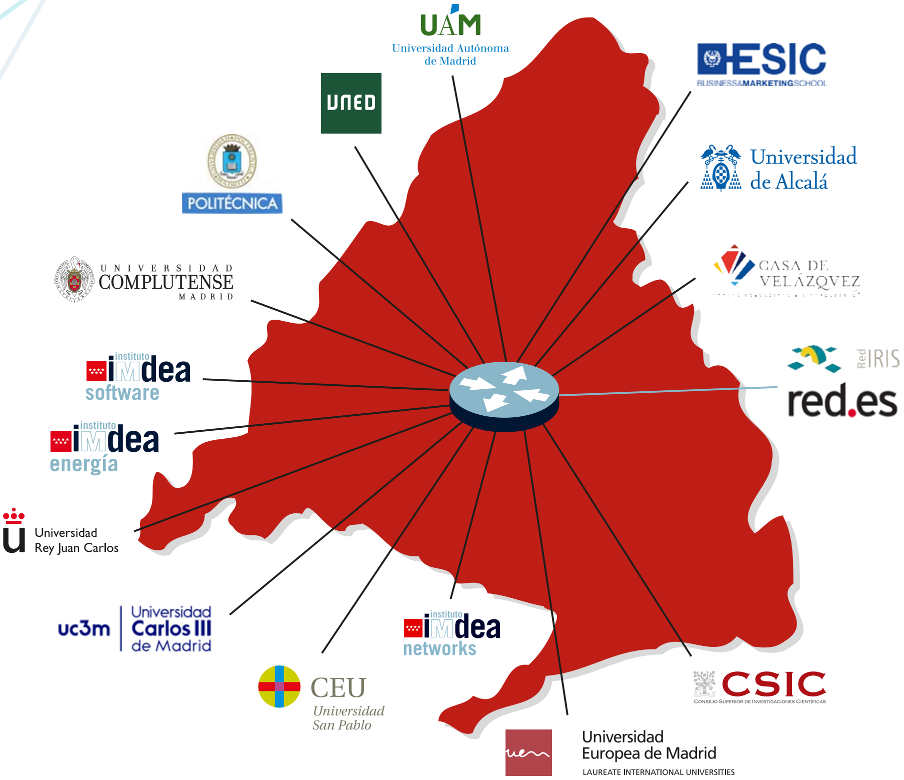
REDIMadrid

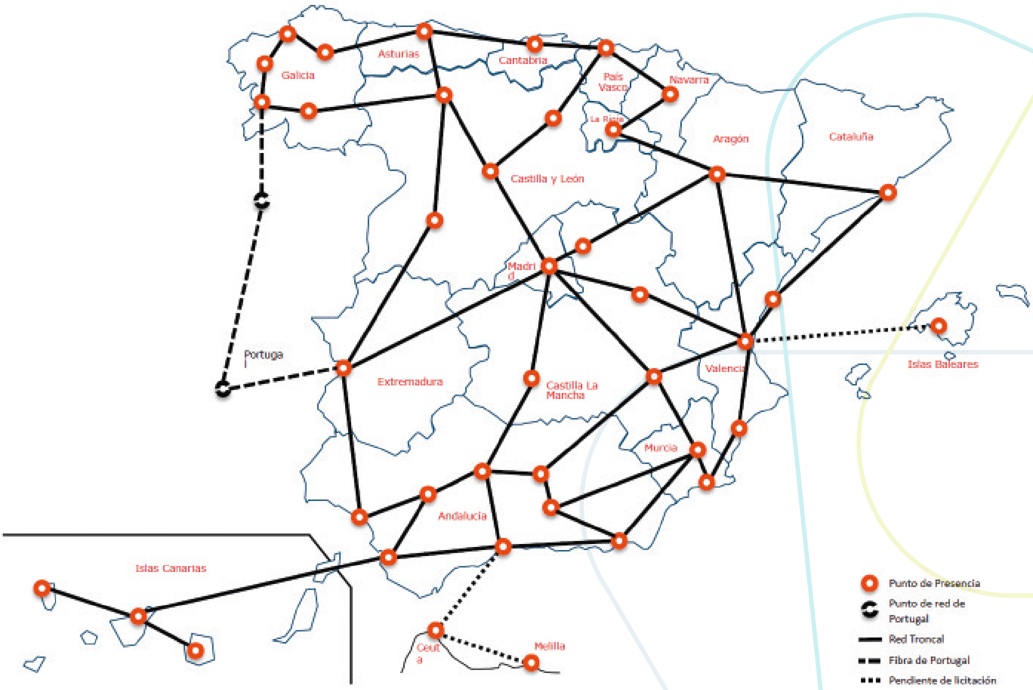
REDIMadrid is the high-speed network for research and higher education that provides advanced connectivity to universities and research centers within the region of Madrid. REDIMadrid is funded and supported by the Madrid Regional Government and managed by the IMDEA Software Institute. REDIMadrid provides the connected institutions with a highly-reliable, high-speed connection. The connected institutions include all public universities in the area of Madrid and the IMDEA research Institutes. The communication infrastructure provided by REDIMadrid allows these institutions to communicate among themselves and to access the national research network (RedIRIS), the European research network Géant, and the rest of the Internet. Public universities in the area of Madrid are provided diversified connections at a speed of 10Gbps-100Gbps using a physical deployment of metropolitan optic fiber rings, which provides a highly reliable infrastructure that can be easily updated to new optical and communication technologies. REDIMadrid provides service to more than 330 thousand users (more than 52% of them female) and enables numerous research projects.

redi madrid

Red IRIS

red.es


UAM
Universidad Autónoma de Madrid
UNED
ESIC
BUSINESS&MARKETINGSCHOOL
POLITÉCNICA
Universidad de Alcalá
UNIVERSIDAD COMPLUTENSE MADRID
CASA DE VELAZQVEZ
instituto imdea software
RedIRIS
red.es
instituto imdea energía
Universidad Rey Juan Carlos
uc3m Universidad Carlos III de Madrid
instituto imdea networks
CEU Universidad San Pablo
CSIC
Consejo Superior de Investigaciones Científicas
Universidad Europea de Madrid
LAUREATE INTERNATIONAL UNIVERSITIES


Galicia
Asturias
Cantabria
País Vasco
Navarra
La Rioja
Aragón
Cataluña
Castilla y León
Madrid
Portugal
Extremadura
Castilla La Mancha
Valencia
Islas Baleares
Murcia
Andalucía
Islas Canarias
Ceuta
Melilla
Punto de Presencia
Punto de red de Portugal
Red Troncal
Fibra de Portugal
Pendiente de licitación

In 2021, REDIMadrid continued its expansion to a deployment of dark fiber whose complete deployment is scheduled for 2022. All new connections are fully diversified and provide links at 100Gbps. Also in 2021, REDIMadrid served as a testbed of Quantum Communication Infrastructures equipment in the context of the EU OpenQKD project.

EIT Digital

EIT Digital (formerly known as EIT ICT Labs) is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT). EIT Digital includes some of the leading educational, research, and industrial actors in the ICT innovation ecosystem in Europe, and its mission is to combine educational, research, and industrial tools and activities to drive and foster ICT innovation on the European scale in the following strategic areas: Digital Industry, Digital Cities, Digital Wellbeing, Digital Tech, and Digital Finance. These areas are complemented by integrated and innovation-driven Master and Doctoral Schools, the EIT Digital acceleration programs, and a Professional School.

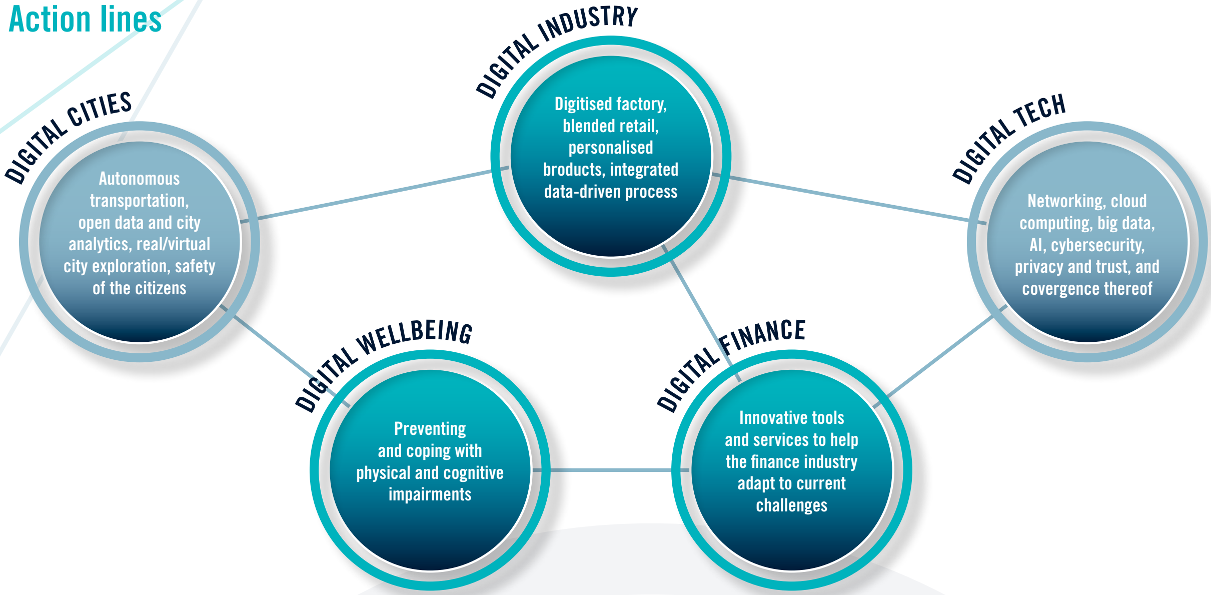
The participation of Spain in EIT Digital started when IMDEA Software officially became an Associate Partner of EIT Digital in 2013, with the goal of organizing the presence of EIT Digital in Spain and driving the evolution of the then-created Spanish Associate Partner Group (APG) towards a fully operational node of EIT Digital. The initial group included Atos, Indra, Telefónica, and the Technical University of Madrid (UPM). The APG became a full node in September 2016, still under the leadership of IMDEA Software, and an independent foundation (EIT Digital Spain) at the end of 2019. IMDEA Software is a member of EIT Digital and collaborates with it in training activities. It also provides IT infrastructure and physical spaces for the Co-Location Center.

The Co-Location Center of EIT Digital Spain is the main meeting point for the members of the node and its joint activities. Its presence is supported by a specific agreement aimed at funding the usage and maintenance of the facilities (offices, A/V, meeting spaces, etc.) that are made available to EIT Digital Spain. Having the CLC in the headquarters of the Institute makes it possible for PhD and Master students registered at the EIT-labeled degrees to interact with Institute researchers. Likewise, the startups hosted at the CLC can interact with the Institute researchers and attend activities at the Institute (technical talks, workshops, etc).

EIT Digital partners

- ALTRNATIV
- ATOS
- BarcelonaBeta Brain Research Center
- BGI S.A.
- Car Sharing Mobility Services S.L.
- Comet Global Innovation, S.L.
- Consultora de Telecomunicaciones Optiva Media S.L.
- Creando Redes
- DTx Colab
- EIDOLON S.L.
- Ferrovial
- Ferrovial Aeropuertos España S.A.
- Ferrovial Construccion S.A.
- Ferrovial Mobility S.L.U.
- Foodintech, Lda.
- Fundación 29 de Febrero
- Fundación Centro de Innovación de Infraestructuras Inteligentes (Ci3)
- Fundación de la C.Valenciana para la investigación, promoción y estudios comerciales de Valenciaport
- GENESIS Biomed
- GEOMOTION GAMES S.L.
- HOP Ubiquitous, S.L.
- Indra Business Consulting, S.L.U.
- Indra Producción Software, S.L.U.
- INDRA SISTEMAS, S.A.
- Indra Soluciones Tecnológías de la Información, S.L.U.
- INFOPORT VALENCIA S.A.
- Innovalia Association (Asociacion de Empresas Tecnológicas Innovalia)
- Insomnia Consulting Sociedad Limitada
- Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)
- Integrated Systems Design and Development S.L.
- Lurtis Rules S.L.
- Quantitative Risk Research S.L.
- Robotnik Automation S.L.L.
- Technical University of Madrid (UPM)
- Technologies SA
- Telefónica Investigación y Desarrollo S.A.U.
- Unicaja Banco S.A.
- Universidade do Minho
- University of Barcelona

Action lines



DIGITAL CITIES

Autonomous transportation, open data and city analytics, real/virtual city exploration, safety of the citizens

DIGITAL INDUSTRY

Digitised factory, blended retail, personalised broducts, integrated data-driven process

DIGITAL TECH

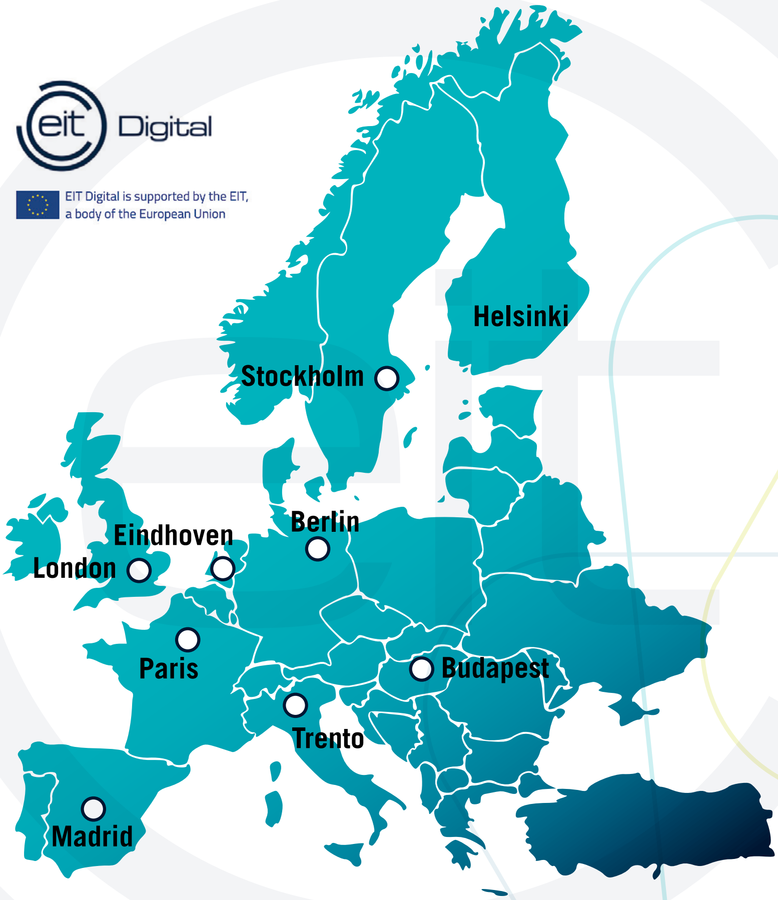
Networking, cloud computing, big data, AI, cybersecurity, privacy and trust, and covergence thereof

DIGITAL WELLBEING

Preventing and coping with physical and cognitive impairments

DIGITAL FINANCE

Innovative tools and services to help the finance industry adapt to current challenges



EIT Digital is supported by the EIT, a body of the European Union

research areas

The research activities carried out by the IMDEA Software Institute address directly its core mission: to advance the technology and the scientific foundations that enable the cost-efficient development of software for tomorrow's computing platforms. That is, software with sophisticated functionality and high quality in terms of reliability, security, and efficiency. We pursue our mission by focusing on three strategic areas, namely *Program Analysis and Verification, Languages, Compilers, and Systems,* and *Security and Privacy*.

PROGRAM ANALYSIS AND VERIFICATION
SECURITY AND PRIVACY
LANGUAGES, COMPILERS, AND SYSTEMS

Program Analysis and Verification

Our research on *Program Analysis and Verification* advances the theoretical underpinnings and the practical tools that help programmers show, by means of a mathematical proof, that their software executes as intended in terms of functionality, efficiency, and resource consumption.

Establishing program correctness is essential in many existing and emerging industrial domains where malfunctions may have serious negative consequences. Examples include safety-critical avionics and automotive software, embedded and mobile software that must perform within given resource bounds, and electronic currencies and smart contracts, which are essentially a form of programmable money.

In addition to being practically important, proving that software is correct is a source of some of the deepest, most challenging, but also most beautiful scientific and mathematical questions. Here are some of the topics on which IMDEA researchers currently work, and are worldwide leaders.

Verification of concurrent and distributed systems.

- Spatial, temporal, and relational program logics (Hoare logics, separation logic, logics for temporal hyperproperties, logics for information flow security, LTL, CTL).
- Consistency criteria (linearizability, serializability, quiescent linearizability, eventual consistency).
- Weak memory models.
- Consensus algorithms.
- Blockchain and smart contracts.
- Runtime Verification.
- Efficient and correct implementations of blockchain systems.

Formal languages and systems for specification, interactive, and automated proofs.

- Expressive, dependent and higher-order type systems (liquid types, type theories, proof assistants, Coq, Agda).
- Behavioral types (monads, comonads, Hoare types, session types) .
- SAT and SMT solvers.

Algorithms and efficent deductive methods for software verification.

- Sofware model checking, parametrized model checking.
- Decision procedures for complex data-types.
- Automata theory and formal languages.
- System minimization via behavioral equivalences.

Static analysis and abstract interpretation.

- Analysis and verification of software resource consumption (e.g., energy bounds for programs).
- Compile- and run-time assertion checking.

Languages, Compilers, and Systems

Our research on *Languages, Compilers, and Systems* provides software engineers with the means they need to describe their ideas in more concise and modular ways, and to generate correct and performant executables from these descriptions. Progress in this area has the potential to dramatically increase programmer productivity as well as the maintainability and reusability of software.

IMDEA researchers are world leaders in this quest. Our results include powerful multi-paradigm languages, environments, and techniques that facilitate the programmer's job as well as novel methods for improving program performance. Regarding program correctness and robustness, the aims are similar to those in verification, but the focus here is on tools that find errors and verify programs *during the process of writing such programs*, rather than a posteriori. This focus requires efficient and fully automatic program analysis tools. In addition, our researchers keep up with the latest advances in applications of artificial intelligence, building systems software to accelerate their performance. The increased complexity in the internal functionality of these applications reduces the efficiency of certain components in the computer systems software stack. In response, our researchers explore the integration of machine learning methods into systems software to improve their efficiency and performance.

The following are some of the research topics that are being explored:

Programming languages and environments

- Multiparadigm programming language theory and implementation. Constraint/logic/functional programming.
- Modern programming features for abstraction, information hiding and code reuse: higher-order, monads, polymorphism, tabling, modules.
- Languages to express and reason with non-monotonic knowledge.
- Combining static and dynamic language characteristics.
- Semantics-based emulation of languages and systems.

Type systems and compiler-based assertion checking

- Type-based program verification, refinement types, liquid types.
- Analysis-based verification of functional and non-functional properties. Assertion languages. Static profiling of resources.

Compilation, transformation, generation

- Resource-aware program transformation and synthesis, partial evaluation.
- Abstract machines, code optimizations, native code generation.
- Auto-parallelization and distribution, with automatic control of resources.

Testing and other dynamic techniques

- Directed testing, random/fuzz testing.
- Run-time verification.

Increased efficiency through the implementation of full systems in hardware

- Pushing computation closer to data.
- Implementation of data movement-intensive stacks (blockchain, distributed algorithms) in reconfigurable hardware.

Computer systems for machine learning

- Systems software solutions that improve the performance and efficiency of applications that use artificial intelligence.

Machine learning for computer systems

- Integration of machine learning methods into the systems software stack of emerging computing platforms.

Security and Privacy

The ever-increasing interconnection, data processing, and storage capabilities enabled by technological advances open up tremendous opportunities for society, the economy, and individuals. At the same time, the digital world is threatened by many kinds of cyberattacks that aim to undermine the security and privacy of digital interactions such as communications, payments, computations, and data storage. These cyberattacks may endanger the economy of our society, but also target important values such as privacy and democracy. Indeed, if the privacy of citizens, governments, and corporations is threatened, this can also impact people's freedom, ultimately creating an imbalance in power relations, which in turn may damage our democratic society.

The research on *security and privacy* at the IMDEA Software Institute aims to deliver technology that enables computation, communication, and storage in open, untrusted, and possibly malicious environments, such as the Internet. Our research results include novel cryptographic protocols and privacy-enhancing technologies, as well as cutting-edge techniques and tools for detecting and analyzing vulnerabilities and malicious activities in software, hardware, and network traffic.

More specifically, our security and privacy research includes:

Cryptography

- Privacy-preserving computation (e.g., homomorphic encryption, functional encryption, multiparty computation).
- Secure outsourcing of data and computation (e.g., verifiable computation, zero-knowledge proofs, homomorphic authentication).
- Privacy in blockchains.

Systems and networks security

- Defending against malware, cybercrime, and targeted attacks.
- Enhancing software security (e.g., automated testing, vulnerability detection).
- Privacy in the mobile application ecosystem.

Side-channel attacks and countermeasures

- Detection and analysis of micro-architectural side-channels.
- Compilation and verification of constant-time software defenses.
- Protecting against privacy leaks based on side-channels.

research highlights

Machine Learning and Computer Systems

Thaleia-Dimitra Doudali

In the current era of Big Data, video analytics, sensor-based products and autonomous operations, the amount of data generated, captured, and then analyzed is enormous, reaching unprecedented scales of Zeta- and Peta- bytes. In addition, this set of application domains exhibits much more complex data access behaviors than traditional data analytics. In response, machine learning methods are now heavily used across scientific domains and commercial products to extrapolate information and relations across data points, that human intelligence and well-established approaches fail to capture at such massive scales.

Systems for Machine Learning. The operations performed by applications of artificial intelligence rely on complex mathematical formulas and can be very time-consuming to execute. Thus, there is a need to speed up such applications via hardware- and software-level solutions. In response, there are research and commercial solutions that focus on building customized computer systems software, tailored to specific types of machine learning workloads. These solutions analyze the way workloads access data and design software that optimizes various system-level operations to improve their runtimes and resource efficiency. This customization at the computer systems software layer together with the use of emerging hardware technologies, can significantly accelerate widely used applications of artificial intelligence.

Machine Learning for Systems. At the same time, there are recent efforts to integrate machine learning methods inside computer systems software, to enable more robust decision-making for the purpose of boosting performance across application domains. In this direction, emerging systems solutions use machine learning methods to learn data access patterns, as observed by the computer system, to improve data management over hardware configurations of cutting edge computing platforms. In addition, early results show that visualization and computer vision methods have the potential to accelerate systems software pipelines, by revealing insights and relations across data that are currently ignored due to the limitations of existing approaches. Such machine intelligent systems show great promise in boosting performance and efficiency across different types of application domains and computing platforms.

The researchers of our institute embraces the latest advances in research efforts and commercial products that use artificial intelligence across software solutions and applications, to address the limited effectiveness of traditional approaches. The solutions that we build leverage well-established mechanisms to the best of their potential and use machine intelligence when and where necessary. We use our human intelligence to reveal insights that allow for practical use of machine learning inside computer systems software (machine learning for systems), as well as to enable the design of custom system components for workloads of artificial intelligence (systems for machine learning).

ERC Project RACCOON: A Rigorous Approach to Consistency in Cloud Databases

Alexey Gotsman

The past decade has witnessed a spectacular growth of cloud-based Internet services. Websites such as Amazon and Facebook process hundreds of thousands of user requests per second, yet stay available at all times. To achieve this, the shared data accessed by the requests is managed by novel *cloud databases*, which partition and replicate the data across a large number of nodes and/or a wide geographical span.

A key challenge that cloud databases have to address is maintaining data consistency in the presence of massive numbers of concurrent modifications at different nodes and despite inevitable failures. The classical approach is for the database to make data distribution and parallel processing transparent to the application, i.e., to behave as if it processes application requests serially on a single, undivided copy of the data. This *strong consistency* model makes it easier for the programmer to construct correct applications. Unfortunately, achieving it requires different database nodes to synchronise, and this undermines the benefits of parallelism.

This has motivated academia and industry to explore alternative architectures for cloud databases that *relax synchronisation* between their nodes. This enables high availability and low latency, by allowing a database node to respond to a request without contacting others. It also enables high scalability, since adding more nodes to the database translates into increased throughput. Finally, relaxing synchronisation creates more parallelism and thus utilises the available hardware in a more cost-efficient way. However, there is a downside: databases that relax synchronisation expose applications to the undesirable effects of parallelism. The resulting programming models are very challenging to use correctly, and we currently do not have advanced methods and tools that would help programmers in this task.

The goal of the RACCOON ERC project is to develop a synergy of novel reasoning methods, static analysis tools and database implementation techniques that maximally exploit parallelism inside cloud databases, while enabling application programmers to ensure correctness. To this end, we first develop methods for reasoning formally about how weakening the consistency guarantees provided by cloud databases affects application correctness and the parallelism allowed inside the databases. This builds on techniques from the areas of programming languages and software verification. The resulting theory then serves as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that its side effects do not compromise application correctness.

PICOCRYPT: Cryptography for Privacy and Integrity of Computation on Untrusted Machines

Dario Fiore

Due to phenomena like the ubiquity of the Internet and the advent of cloud computing, it is increasingly common for users to exchange and receive digital information processed on remote machines. Online storage services are already widely available over the Internet, and allow users to access, modify and share their data from anywhere in the world and from multiple devices. This phenomenon is not limited to storage: it is increasingly common to rely on *computation* performed on third party machines. This is something that can happen on a daily basis for a smartphone user: when searching over emails, the search physically happens in the servers of the email provider; when dictating a message or using the voice assistant (e.g., Apple Siri, Google Voice Typing), the voice recognition is often outsourced to remote servers.

This computing trend is undoubtedly successful: remote computing can boost productivity and reduce costs, as well as enable innovative applications, new sharing capabilities, etc. At the same time, this shift in the computing trend is also bringing to light a number of serious security concerns. In particular:

How to ensure that the results computed by third parties are correct (integrity), and no unauthorized information is leaked (privacy)?

The current way to deal with these problems is to trust third parties under legislation guarantees. This approach assumes that third-party machines stay honest all time, even if they get hacked! This is unrealistic and contradicted by the numerous security incidents that are regularly reported.

At the IMDEA Software Institute we are working to address these challenges in the scope of the *ERC project PICOCRYPT*, funded by the European Research Council.

The vision of the project is that any computing device must be able to store and process data on untrusted machines without risking for privacy and integrity and without the need of trusting these machines. Recent trends in cryptography (such as fully homomorphic encryption, verifiable computation, and zero-knowledge proofs) promise solutions to realize our vision. However, the existing generation of protocols is limited due to its high costs and its poor support of emerging applications such as data stream processing.

The goal of the PICOCRYPT project is to invent a new generation of cryptographic protocols for computing securely on untrusted machines in a way that is cost-effective and suitable for future application scenarios. Our project focuses on designing protocols that provide three fundamental security properties: computation’s integrity, computation’s authenticity, and privacy-preserving computation. To achieve our goals, we are working on designing new methods to scale up the applicability of cryptographic protocols for these problems. One of our key approaches is trading generality for efficiency. While existing solutions are either general but impractical or efficient but of limited applicability, in PICOCRYPT we look for protocols that support a wide range of applications while staying efficient.

The project started in June 2021 and will run until 2026. The outcomes of PICOCRYPT have the potential of enabling a paradigm shift in the way privacy and integrity will be enforced in remote computing and can have impact in the IT world by making remote computing safer not only for citizens but also for public and private organizations that due to the current risks renounce to these services.

people

The IMDEA Software Institute strives towards the level of excellence and competitiveness of the highest-ranked institutions worldwide. Success in this goal can only be achieved by recruiting highly-skilled personnel for the scientific teams and support staff. The Institute considers this one of the key critical factors and measures of its success.

Competition for talent in Computer Science is extremely high at the international level, since essentially all developed countries have identified the tremendous impact that IT has on the economy and the crucial competitive advantage that attracting truly first class researchers entails. To meet this challenge, the Institute offers a world-class working environment that is competitive with similar institutions in Europe and in the US and which combines the best aspects of a University department and a research laboratory.

Hiring at the Institute follows internationally-standard open dissemination procedures with public, international calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and mailing lists. Appointments at (or promotion to) the Assistant Professor, Associate Professor, and Full Professor levels (i.e., tenure-track hiring, tenure, and promotion decisions) are approved by the Scientific Advisory Board.

In addition to faculty positions, the Institute also has its own programs for visiting and staff researchers, post-docs, graduate scholarships, and internships. In all aspects related to human resources, the Institute follows the recommendations of the European Charter for Researchers and a Code of Conduct for their Recruitment (http://ec.europa.eu/), which it has duly signed.

In 2021, the scientific staff of the Institute was composed of 12 senior faculty (full or associate professors, two part-time and one on leave), 8 junior faculty (tenure-track or researchers), 12 postdoctoral researchers, 4 research programmers, 31 research assistants (Ph.D. candidates, not counting visiting Ph.D. candidates) and 31 interns who spent a variable length of time (from one month to a year) at the Institute collaborating with faculty members. The Institute enjoyed the presence of one senior faculty visitor.

The support (project management, administration, infrastructures) department was composed of 3 project management staff, 3 system support staff, 4 REDIMadrid staff, 6 administrative support members, 1 communication and media manager, and 1 part-time administrative support that also gives general service to the rest of the IMDEA Institutes.

Figure 1 shows the ratio of each category at the end of 2021. Figure 2 summarizes where these researchers obtained their Ph.D. (by continents plus Spain), and Figure 3 shows the location where the Institute researchers were working before joining IMDEA. Finally, Figure 4 presents the nationalities of researchers at or above the Ph.D. level.

faculty members	20
post-doctoral researchers	12
research assistants	31
research programmers	4
project management	3
interns	31
IT staff	3
REDIMadrid	4
communication	1
administrative support	6

people

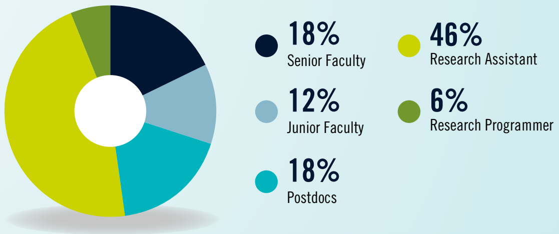


Figure 1
Type of position, all researchers

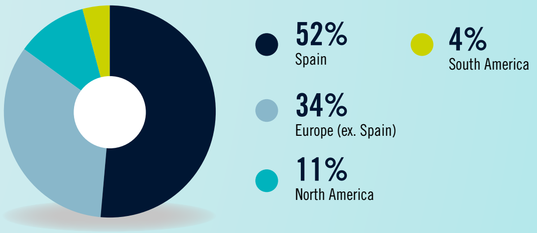


Figure 2
Where Ph.D. was obtained (by continent + Spain)

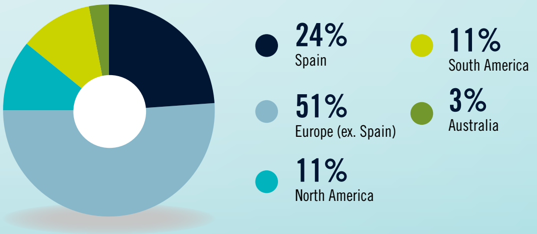


Figure 3
Location of previous institution of researchers at or above postdoc level (by continent + Spain)

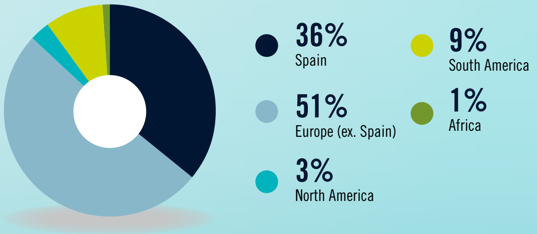


Figure 4
Nationality of researchers at or above PhD level (by continent + Spain)

faculty

Manuel Carro

Associate Research Professor and Scientific Director

Manuel Carro received his Bachelor degree in Computer Science from the Technical University of Madrid (UPM), and his Ph.D. degree from the same University in 2003. He is currently an Associate Professor at the Technical University of Madrid, Associate Research Professor at the IMDEA Software Institute and, since May 2017, its Director. He is the representative of the Institute at Informatics Europe and at the Node Strategy Committee of EIT Digital Spain. He has previously been Deputy Director at the IMDEA Software Institute, representative of UPM at the NESSI and INES technological platforms, representative of UPM at SpaRCIM, deputy representative of IMDEA Software at ERCIM, and CLC Manager and Scientific Coordinator of the Madrid Node of EIT Digital. He has published over 80 papers in international conferences and journals, and received best paper awards at ICLP 2005 and ICSOC 2011.

He has been organizer and PC member of many international conferences and workshops, including conference chair of ICLP 2014 and PC Chair of ICLP 2016, the flagship conference in the field of Logic Programming. He has participated in research projects at the regional, national, and European level. He was UPM's principal investigator for the S-Cube European Network of Excellence and is currently the principal investigator of several national and a regional research projects. He has completed the supervision of five Ph.D. theses.

Research Interests

His interests span several topics, including the design and implementation of high-level (logic- and constraint-based) programming languages to express non-monotonic knowledge and reasoning and to improve the quality of software production, the analysis of service-based systems, and the effective usage of formal specifications in teaching programming. He has long been interested in parallel programming, parallel implementations of declarative languages, and visualization of program execution.

Juan Caballero

Associate Research Professor and Deputy Director

Juan Caballero received his Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University, USA, in 2010. He joined the Institute in November 2010 as an Assistant Research Professor and was promoted to Associate Research Professor in December 2016. He was appointed Deputy Director of the Institute in September 2017. Prior to joining the Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. Juan also holds an M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH), Sweden, and a Telecommunications Engineer degree from Technical University of Madrid (UPM), Spain. His research regularly appears at the top venues in computer security and has won two best paper awards at the USENIX Security Symposium, a distinguished paper award at the ACM Internet Measurement Conference, and the DIMVA Most Influential Paper 2009-2013 award. He is a recipient of the La Caixa fellowship for graduate studies. He has been principal investigator of multiple national and European projects. He has been program chair or co-chair for the ACSAC, DIMVA, DFRWS, ESSOS, and EuroSec conferences, and is a member of the steering committee for ACSAC, DIMVA, and ESSOS. He has been a member of the technical committee for the top computer security venues including IEEE S&P, ACM CCS, USENIX Security, and NDSS.

Research Interests

Juan's research focuses on computer security, including security issues in systems, software, and networks. He designs and implements novel defenses against cybercrime including defenses against malware and software vulnerabilities. He is also interested on big data analysis for security, program binary analysis, and censorship resistance.

Manuel Hermenegildo

Distinguished Professor

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. He joined the Institute on January 1, 2007 as its founding Scientific Director, continuing in this role until May 2017. He is currently Distinguished Professor at the Institute and also Full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining IMDEA Software, he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He was also project leader at the MCC research center and Adjunct Assoc. Prof. at the CS Department of the U. of Texas, both in Austin, Texas, USA. He has received the Julio Rey Pastor Spanish National Prize in Mathematics and Information Science and Technology and the Aritmel National prize in Computer Science, and he is an elected member of the Academia Europea. He is the president of the Scientific Board of INRIA, member of the Scientific Advisory Board of Dagstuhl, and a member of the ACM Europe Technology Policy Committee. He was also vice-President of Informatics Europe, and the founding director of the Spanish node of EIT Digital, and member of its Steering Board. He has published more than 250 refereed scientific papers and monographs and has given numerous keynotes and invited talks in major conferences. He has also been coordinator and/or principal investigator of many international and national projects, area editor of several journals, and chair and PC member of numerous first-level conferences. He served as General Director for the Spanish national research funding agency, as well as a member of the European Union's high-level advisory boards in information technology (ISTAG, CREST), the board of directors and the scientific board of the Spanish Scientific Research Council (CSIC) and of the Center for Industrial and Technological Development (CDTI), among other national and international duties.

Research Interests

His areas of interest include global program analysis, optimization, verification, and debugging (including resources such as energy and other non-functional properties); abstract interpretation; partial evaluation; parallelism and parallelizing compilers; constraint/logic/functional programming language design and implementation; abstract machines; automatic program documentation; and sequential and parallel computer architecture.

Gilles Barthe

Research Professor (part-time)

Gilles Barthe received a Ph.D. in Mathematics from the University of Manchester, UK, in 1993, and an *Habilitation à diriger les recherches* in Computer Science from the University of Nice, France, in 2004. He has published extensively in programming languages, security, privacy, and cryptography, and was awarded the Best Paper Awards at CRYPTO 2011, PPoPP 2013, and FSE 2016.

He was an invited speaker at numerous venues, including CAV 2016, CSF 2014, ESORICS 2012, ETAPS 2013, EUROCRYPT 2017, IJCAR 2016. He has been coordinator/principal investigator of many national and European projects, and served as the scientific coordinator of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices (2005-2009). He is a member of the editorial board of the Journal of Automated Reasoning and of the Journal of Computer Security. He is also (since 2019) one the Scientfic Directors of the Max-Plank Institute for Security and Privacy in Bochum, Germany.

Research Interests

Gilles' research is currently focused on program verification techniques for probabilistic programs, with a focus on relational verification and its applications to cryptography, differential privacy, and machine learning. He has previously worked on building foundations for computer-aided cryptography and privacy and on the development of tools for proving the security of cryptographic constructions and differentially private computations.

John Gallagher

Research Professor (part-time)

John Gallagher received the B.A. (Mathematics with Philosophy) and Ph.D. (Computer Science) degrees from Trinity College Dublin in 1976 and 1983 respectively. He held a research assistantship in Trinity College (1983-4), and post-doc appointments at the Weizmann Institute of Science, Israel (1987 - 1989) and Katholieke Universiteit Leuven, Belgium (1989). From 1984-1987 he was employed in research and development in a software company in Hamburg, Germany. Between 1990 and 2002 he was a lecturer and later senior lecturer at the University of Bristol, UK. Since 2002, he has been a professor at the University of Roskilde, Denmark in the research group Programming, Logic and Intelligent Systems and the interdisciplinary Experience Lab and holds a dual appointment at IMDEA Software Institute since February 2007. He chaired the program committee of several international conferences and been a member of the program committee of about 60 others. He has also been in executive committee of the Association for Logic Programming, the steering committee of the ACM SIGPLAN workshop on Partial Evaluation and Program Manipulation and is currently in the steering committee of the International Symposium on Functional and Logic Programming. He has published approximately 60 peer-reviewed articles which have over 2000 citations.

Research Interests

His research interests focus on program specialization, constraint logic programming, rewrite systems, static analysis of software including analysis of energy consumption and other resource properties of programs, automatic software verification, temporal logics, and semantics-based emulation of languages and systems, and has participated in and led a number of national and European research projects on these topics.

César Sánchez

Associate Research Professor

César Sánchez received a Ph.D. degree in Computer Science from Stanford University, USA, in 2007. His thesis studies the applications of formal methods for guaranteeing deadlock freedom in distributed algorithms. After a post-doc at the University of California at Santa Cruz, USA, César joined the IMDEA Software Institute in 2008. He become a Scientific Researcher at the Spanish Council for Scientific Research (CSIC) in 2009. In 2013, he was promoted to Associate Professor at the IMDEA Software Institute.

César holds a degree in Ingeniería de Telecomunicación (MSEE) from the Technical University of Madrid (UPM), Spain, granted in 1998. Funded by a Fellowship from La Caixa, he moved to Stanford University, USA, receiving an M.Sc. in Computer Science in 2001, specializing in Software Theory and Theoretical Computer Science. César was the recipient of the 2006 ACM Frank Anger Memorial Award, and he enjoyed a Juan De La Cierva Fellowship between 2008 and 2009.

Research Interests

César's general research interests are the applications of logic, games and automata theory for the development, the understanding, and the verification and synthesis of sofware and hardware. In particular, César's main line of research is the use of formal methods for reactive systems with emphasis on concurrent, embedded and distributed systems. His foundational research includes specification languages for reactive systems, temporal logic based verification and synthesis, runtime verification and monitoring, and applications to smart-contracts. The applications of his research include the reliability of unmanned vehicles, formal methods for security and static and dynamic verification of smart contracts.

Pierre Ganty

Associate Research Professor

Pierre holds a joint Ph.D. degree in Computer Science from the University of Brussels, Belgium and from the University of Genova, Italy. Prior to join the IMDEA Software Institute in 2009 he did a nearly two-year postdoc at the University of California, Los Angeles. Pierre is associate research professor at the IMDEA Software Institute since late 2015. He is the recipient of a Ramón y Cajal fellowship.

Research Interests

Pierre is interested in fundamental computational problems arising in automated verification of systems with infinitely many states. Recently, he focused on algorithms to decide the containment problem between formal languages of finite and infinite words, a fundamental problem arising in model-checking.

Aleks Nanevski

Associate Research Professor

Aleks Nanevski obtained his Ph.D. in Computer Science from Carnegie Mellon University, and held postdoctoral research positions at Harvard University and Microsoft Research in Cambridge, before joining IMDEA in 2009. He is a recipient of Ramon y Cajal award in 2010, and an ERC consolidator grant in 2017.

Research Interests

Aleks' research is in type theory for program verification, with the special focus on shared-memory concurrent programs. He relies on type-theoretic idea of structuring programs and proofs together, to enable effective and scalable verification of realistic and challenging concurrent programs.

Alexey Gotsman

Associate Research Professor

Alexey Gotsman received his Ph.D. degree in Computer Science from the University of Cambridge, UK in 2009. His Ph.D. thesis received a Best Dissertation Award of the European Association for Programming Languages and Systems (EAPLS). Alexey was a postdoctoral fellow at the University of Cambridge before joining IMDEA in September 2010. He is a recipient of a Ramón y Cajal fellowship and an ERC Starting Grant.

Research Interests

Alexey's research interests are at the intersection of distributed computing and formal verification.

Dario Fiore

Associate Research Professor

Dario Fiore received his Ph.D. degree in Computer Science from the University of Catania, Italy in 2010. Prior to joining the IMDEA Software Institute in November 2013, Dario held postdoctoral positions at Max Planck Institute for Software Systems (Germany), New York University (USA), and École Normale Supérieure (France). During his Ph.D., he was also a visiting student at the IBM T.J. Watson research center and the New York University (USA). He is the recipient of a Juan de la Cierva Incorporacíon fellowship awarded in 2015, and an ERC Consolidator grant in 2020.

Research Interests

Dario's research interests are on theoretical and practical aspects of cryptography and its applications to security and privacy. His research focuses on designing provably-secure cryptographic protocols, and his recent work has particular emphasis on developing novel paradigms for the security of data during computation. More specifically, some of the topics he works on include: secure delegation of data and computation to the cloud, homomorphic authentication, zero-knowledge proofs, homomorphic encryption, functional encryption, and foundations of cryptography.

Alessandra Gorla
Assistant Research Professor

Alessandra Gorla received her Bachelor's and Master's degrees in computer science from the University of Milano-Bicocca in Italy. She completed her Ph.D. in informatics at the Università della Svizzera Italiana in Lugano, Switzerland in 2011. In her Ph.D. thesis she defined and developed the notion of Automatic Workarounds, a self-healing technique to recover Web applications from field failures, a work for which she received the Fritz Kutter Award for the best industry-related Ph.D. thesis in computer science in Switzerland. Before joining IMDEA Software Institute in December 2014 as an assistant research professor, she has been a postdoctoral researcher in the software engineering group at Saarland University in Germany. During her postdoc, she has also been a visiting researcher at Google in Mountain View.

Research Interests

Alessandra's research interests are in software engineering, and in particular on testing and analysis techniques to improve the reliability and security of software systems. She is also interested in malware detection for mobile applications.

Niki Vazou
Assistant Research Professor

Niki Vazou obtained her Ph.D. in Computer Science from University of California, San Diego in 2016 and held a postdoctoral fellow position at University of Maryland, College Park. In 2018 Niki joined IMDEA as a Research Assistant Professor. Niki received an MSR graduate research fellowship in 2014 and is a member of the Haskell.org committee since 2016. She has published in many programming languages conferences (e.g., POPL, ICFP, and OOPSLA) and received the Best Paper Award at OOPSLA 2018. Niki has been an invited speaker at research and industrial conferences including Zurihac and Haskell eXchange.

Research Interests

Niki's interests include refinement types, automated program verification, and type systems, and her goal is to make theorem proving a useful part of mainstream programming. She developed Liquid Haskell, an SMT-based, refinement type checker for Haskell programs that has been used for various applications ranging from fully automated light verification of Haskell code (e.g., bound checking) to sophisticated theorem proving (e.g., non-interference).

Ignacio Cascudo
Assistant Research Professor

Ignacio Cascudo received a Ph.D. in Mathematics from the University of Oviedo, Spain, in 2010. After that, he was a postdoctoral researcher at the Centrum Wiskunde en Informatica (CWI) Amsterdam, the Netherlands, and later at the Department of Computer Science of Aarhus University in Denmark. Between 2016 and 2019, he was first assistant professor and then associate professor at the Department of Mathematics of Aalborg University, Denmark. In September 2019, he joined the IMDEA Software Institute as a research assistant professor.

Research Interests

Ignacio's main research interests are within the area of cryptography, specially regarding threshold cryptography technologies such as secret sharing and secure multiparty computation, which study how to distribute information and computations among a number of servers in a privacy-preserving way. He is also interested in applications of these techniques to problems such as random number generation, and in the interplay between these problems and other research fields such as the theory of error-correcting codes, and areas of pure mathematics (algebraic geometry and number theory, finite fields, and algebraic complexity).

Marco Guarnieri
Assistant Research Professor

From June 2019, Marco is an Assistant Research Professor at IMDEA Software Institute, which he joined as a postdoctoral researcher in July 2018. Before that, he worked as a postdoctoral researcher at ETH Zürich, where he also completed a Ph.D. in the Information Security group. He received his bachelor's and master's degrees in computer engineering from Università degli Studi di Bergamo.

Research Interests

Marco's research focuses on the design, analysis, and implementation of practical systems for securely storing and processing sensitive data. To achieve this goal, he combines concepts and techniques from diverse domains, such as databases, logics, probabilistic models, programming languages, and program verification. He applies his research to the analysis of microarchitectural side-channel attacks (and countermeasures), database security, and the enforcement of probabilistic security policies. More generally, he is interested in security and privacy, programming languages, and formal methods.

Pedro Moreno-Sánchez

Assistant Research Professor

Pedro received his PhD degree in Computer Science from Purdue University (USA) in 2018. Prior to joining the IMDEA Software Institute in October 2020, Pedro held a postdoctoral position at Technical University of Vienna (Austria). During his PhD, he was also a visiting student at Ripple Labs (USA), IBM-Research Zürich (Switzerland). He received his bachelor and master degree in Computer Science from University of Murcia (Spain). During his master, he was a visiting student at Philips Research Europe (The Netherlands).

Research Interests

Pedro's main research interest lies in the areas of distributed ledgers (blockchain), privacy-enhancing technologies and applied cryptography. His research aims to bridge the gap between theory and practice and design cryptographic protocols with formal security and privacy guarantees that are practical and can help users today. More specifically, some of the topics he works on include: anonymous communication protocols, credit networks, privacy-preserving smart contracts, payment-channel networks, quantitative analysis of blockchain data and supply chain.

Thaleia-Dimitra Doudali

Assistant Research Professor

Thaleia received her PhD from the Georgia Institute of Technology (Georgia Tech, USA) in 2021. Prior to that she earned an undergraduate diploma in Electrical and Computer Engineering at the National Technical University of Athens in Greece. While at the United States she interned at VMWare and AMD Research, while contributing to successful patent applications. In 2020, Thaleia was selected to attend the prestigious Rising Stars in EECS academic workshop. Aside from research, Thaleia actively strives to improve the mental health awareness in academia and foster diversity and inclusion.

Research Interests

Thaleia's research lies at the intersection of Operating Systems and Machine Learning, where she explores novel methodologies, such as machine learning and computer vision, to improve system-level resource management of emerging hardware technologies and computing environments at massive scale. Her dissertation added machine intelligence to hybrid memory management and part of it has been recognized as a best paper award finalist at the 28th International Symposium on High-Performance Parallel and Distributed Computing (HPDC 2019).

Pedro López-García

Researcher

Pedro López-García received a MS degree and a Ph.D. in Computer Science from the Technical University of Madrid (UPM), Spain in 1994 and 2000, respectively. On May 28, 2008 he obtained a Tenured Researcher position at the Spanish National Research Council (CSIC) and joined the IMDEA Software Institute. Immediately prior to this position, he held associate and assistant professor positions at UPM and was deputy director of the Artificial Intelligence unit at the Computer Science Department. He has published more than 70 refereed scientific papers, many of them at conferences and journals of high or very high impact. He served as the local principal investigator of the European projects ES_PASS "Embedded Software Product-based ASSurance," and the FP7 FET ENTRA "Whole-Systems Energy Transparency." He has also participated as a researcher in many other international, national, and regional projects.

Research Interests

His areas of interest include energy-aware software development; multi-language analysis, verification, debugging and optimization of non-functional properties, focusing on resources (energy, execution time, user defined), determinism, non-failure, etc.; automatic static profiling of resources; abstract interpretation; low energy and highly parallel computing in different application domains (internet of things, healthcare, big data, and HPC); resource-aware program synthesis; automatic control of resources in parallel and distributed computing; tree automata; constraint and logic programming.

José Francisco Morales

Researcher

Jose F. Morales joined the IMDEA Software Institute as a postdoctoral researcher in November 2011, after receiving his Ph.D. degree in Computer Science from the Technical University of Madrid (UPM), Spain. Previously, he held a teaching assistant position at the Universidad Complutense de Madrid, starting in 2005.

Research Interests

Jose's past work focused on mechanisms for the efficient execution of logic programs: inference of program properties by abstract interpretation, highly-optimizing translation to low-level code using those properties, and the development of abstractions for the specification and automated construction of abstract machines. His current research interests include the design of multiparadigm languages (declarative, imperative) based on a constraint/logic programming kernel; abstract machines, program optimizations, and native code generation; and program analysis, abstract interpretation, and static and dynamic verification.

Srdjan Matic

Researcher

Srdjan received his PhD degree in Computer Science from Università degli Studi di Milano in 2017. Prior to joining the IMDEA Software Institute in October 2021, he held a postdoctoral position at IMDEA Networks Institute. From 2018 to 2020, Srdjan was a postdoctoral fellow at University College London at Technische Universität Berlin, studying Internet privacy and abuses in the IoT ecosystem. He received his bachelor and master degree in Computer Science from Università degli Studi di Milano.

Research Interests

Srdjan's main research interest lies in the areas privacy, networking and measurement. His research aims at developing new systems that will allow end-users to quantify and asses privacy and security violations in their own environments. More specifically, some of the topics he works on include: privacy on the Web and smart devices, information leakage and anonymous networks.

faculty members on leave of absence

Juan José Moreno-Navarro

Research Professor, on leave

Juan José Moreno-Navarro received his Ph.D. degree in Computer Science from the Technical U. of Madrid (UPM), Spain in 1989. He developed a large part of his Ph.D. at RWTH Aachen (Germany). He has been Full Professor at the UPM Computer Science Department since 1996 and joined the IMDEA Software Institute upon its foundation. He served as Deputy Director up to 2008. He is currently on leave from the Institute. He has published more than 100 papers in international conferences, books, and journals. He has organized, served in program committees, and given invited talks and tutorials in many conferences in the IST field.

He has been actively involved in research and university policy, serving as General Director for University Policies (Ministry of Education, 2009-2012), General Director for Technology Transfer and Enterprise Development (Ministry of Science and Innovation, 2009) and General Director for Planning and Coordination (Ministry of Science and Innovation, 2008-2009). During this period he has been chairman of CNEAI (Spain's Researcher Activity Evaluation Agency), has been involved in the setting up of several research infrastructures, secretary of the Spanish University Council and of the Spanish Science and Technology Council, and member of the steering board of several foundations (ANECA, UIMP, CENER-Ciemat, Universidad.es, CSIC, ISCIII, IDAE, etc.)

He has been the founding director of SpaRCIM. He has been responsible for the Spanish ICT research program, in charge on International Relations for IST, FP6 IST Committee member, and Spanish National Contact Point for the Spanish Ministry of Education and Science. He also coordinated the Spanish Turing Year and was general chair of the Spanish Conference of Informatics 2013. He is currently an MP in the Madrid Regional Government.

Research Interests

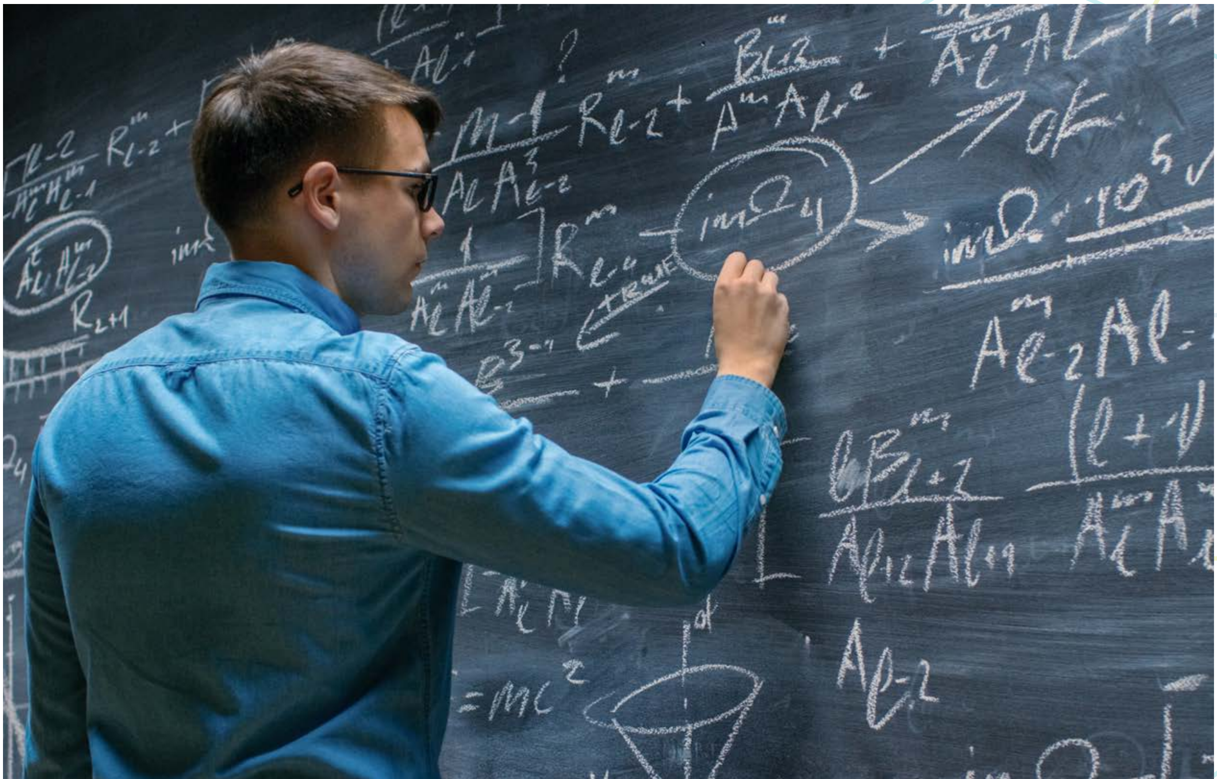
His research interests include all aspects related to declarative and rigorous software development technologies. This includes software development techniques, specially specification languages, automatic generation of code (programming from specifications), and software services description. His interests also include the integration of functional and logic programming. He has led the design and implementation of the language BABEL and took part in the activities of the international committee involved in the design of the language Curry. He is also currently involved in scientific policy analysis, bibliometrics, and research impact evaluation and analysis.

visiting and affiliate faculty

Roberto Giacobazzi
Affiliate Faculty

Anindya Banerjee
Affiliate Faculty

Boris Köpf
Affiliate Faculty



postdoctoral researchers

Manuel Bravo

Postdoctoral Researcher

Manuel joined the IMDEA Software Institute as a postdoctoral researcher in June 2018. He obtained his Ph.D. in 2018 from the Instituto Superior Técnico of the Universidade de Lisboa in Portugal and the Université Catholique de Louvain in Belgium where he worked with Prof. Luís Rodrigues and Prof. Peter Van Roy. Before that, he obtained his M.Sc. in 2013 from the Instituto Superior Técnico of the Universidade de Lisboa in Portugal and the Royal Institute of Technology in Stockholm, Sweden.

Research Interests

Manuel's research interest is in the design and implementation of distributed systems. Specifically, he is interested in understanding replication and consistency in such systems.

František Farka

Postdoctoral Researcher

František received his Master's degree in Theoretical Computer Science from Charles University, The Czech Republic, and his Ph.D. degree jointly from the University of St Andrews and Heriot-Watt University, UK. In his doctoral work he focused on foundations of constructive proof search with applications to type inference and term synthesis developing proof-relevant semantics of resolution. Starting from November 2018, he worked as a research assistant at Heriot-Watt University on proof-relevant verification of planning languages. He joined IMDEA Software Institute in July 2019. He is working with Aleks Nanevski on verification of shared-memory concurrent programs.

Research Interests

František's research is focused on the application of type theory and logic in the verification of software. He applies concepts arising from these areas to the design of programming languages that facilitate development of software that is correct by construction. More concretely, he has been recently studying separation logic for shared-memory concurrency with particular focus on its algebraic characterisation.

Fernando Macías

Postdoctoral Researcher

Fernando Macías joined the IMDEA Software Institute in September 2019, after a short teaching period at the University of Extremadura, Spain. Before, he carried out his research at the Western Norway University of Applied Sciences and got a PhD in Computer Science from the University of Oslo, Norway in June 2019. Fernando also received an MSc in Computer Science in 2014, a Major in Computer Science (Ingeniería Informática) in 2013, and a BSc in Computer Science (Ingeniería Técnica Informática) in 2011 at University of Extremadura, where he also worked as a research associate.

Research Interests

Fernando's research focuses on different areas of software engineering, including Software analysis, testing, and verification, including formal methods, model-driven software engineering, including multilevel modelling, model transformation and model-based reverse engineering of software.

Bishoksan Kafle

Postdoctoral Researcher

Bishoksan received his PhD in Computer Science from Roskilde university, Denmark in 2016. His thesis focused on safety verification of integer programs, using the so-called representation of Constrained Horn clauses. During his PhD, he was also a visiting student at NASA Ames Research center, USA. After a post-doc at the university of Melbourne, Australia, he Joined the IMDEA Software Institute in 2019.

He received a Bachelor degree in Computer Science from Central University of Las Villas, Cuba in 2009 and a joint Master degree in Computational Logic from Dresden University of Technology, Germany; Free university of Bolzano, Italy, and the new university of Lisbon, Portugal in 2012 under an Erasmus Mundus scholarship.

Research Interests

He is interested in automated program analysis and verification. In particular, he applies static analysis, automaton-theoretic approaches, and program specialization techniques to program verification and resource analysis problems based on Horn clauses.

Christian Roldán

Postdoctoral Researcher

Christian Roldán completed his Ph.D. at Universidad de Buenos Aires, Argentina. His thesis focused on specification and semantics of replicated data types. He contributed to the development of programming models and analysis techniques suitable for applications that rely on weak consistent, replicated stores. In April 2020, he joined IMDEA Software Institute as a postdoctoral researcher where he works with Alexey Gotsman on formal verification of distributed protocols.

Research Interests

His main interests are concurrency theory, formal verification and distributed systems.

Ida Tucker

Postdoctoral Researcher

Ida completed her Ph.D. at the École Normale Supérieure of Lyon, France, where she was advised by Guilhem Castagnos and Fabien Laguillaumie. In October 2021, she joined IMDEA Software Institute as a postdoctoral researcher where she works with Dario Fiore on cryptography.

Research Interests

Ida's research interests are in the design of provably secure advanced cryptographic protocols, efficient enough to be applied in large scale information systems. Her current interests include the secure delegation of data and computations to the cloud, zero-knowledge proofs, and multi-party computation. During her Ph.D., her work focussed on the design of protocols (linearly homomorphic encryption, functional encryption, zero-knowledge proof systems, threshold signatures) from class group cryptography.

Nicolas Mazzocchi

Postdoctoral Researcher

Prior to joining IMDEA Software Institute in December 2020, Nicolas obtained a Ph.D. in Computer Science from Brussels University (ULB) that was funded by the competitive FNRS-FRIA fellowship. In France, he received the master's degree MPRI from ENS Paris-Saclay and the bachelor's degree in Computer Science from Aix-Marseille University.

Research Interests

Nicolas' work lies in the domain of formal methods for computer-aided verification. He is focusing on specification models with a good tradeoff between the expressiveness of system behaviors and the decidability of algorithms that ensure safety and robustness. His Ph.D. contributes to the research effort of automata-based quantitative model-checking methods. His current postdoc aims at the tractability of these techniques by using of order theory, abstract interpretation, and compositionality.

Peter Chvojka

Postdoctoral Researcher

Peter received his PhD degree in Computer science from University of Wuppertal (Germany) in 2021 where he was supervised by Tibor Jager. Part of his Phd studies were completed at University of Paderborn (Germany). He has received his bachelor and master degree in Computer Science from Slovak University of Technology in Bratislava (Slovakia). During his master studies, he was a visiting student at ETH Zurich (Switzerland).

Research Interests

Peter's research interest focus on different areas of public-key cryptography. Currently, his main research focus is on building practical primitives of timed cryptography and efficient proof systems in general.

Lydia Helen Garms

Postdoctoral Researcher

Lydia completed her PhD studies at Royal Holloway, University of London in 2020 as part of the Centre for Doctoral Training in Cyber Security. During her PhD she undertook an internship at IBM-Research Zurich. Previously to joining IMDEA software institute she was a post-doctoral researcher, again at Royal Holloway, until April 2021. She completed her bachelor's degree in mathematics and master's degree in applicable mathematics at the University of Cambridge and the London School of Economics and Political Sciences, respectively.

Research Interests

Lydia's general research interests include modelling provable security for cryptographic primitives, considering the trade-off between usability and privacy, and designing primitives that satisfy this. Her PhD focused on variants of group signatures, with applications to reputation systems and processing user data. Her subsequent post-doctoral position focused on quantum-resistant hybrid key exchange protocols. At IMDEA she has focused on publicly verifiable secret sharing schemes with applications to blockchain technologies.

Louis-Marie Dando

Postdoctoral Researcher

Louis-Marie obtained his Ph.D. in 2019 from the Université de Bordeaux. After a teaching position in Orléans and a postdoc position in Marseille, he joined IMDEA Sofware Institute in October 2021 where he works with Pierre Ganty.

Research Interests

His research interests are mainly playing with automata and various kind of machines, triyng to find equivalent formalisms. Currently working on learning infinite regular languages.

Elena Gutierrez

Postdoctoral Researcher

Elena obtained a double BS in Computer Science and Mathematics from the Universidad Autónoma de Madrid (UAM), Spain.

Research Interests

Her research interests are mainly in finite and weighted automata theory and applications.

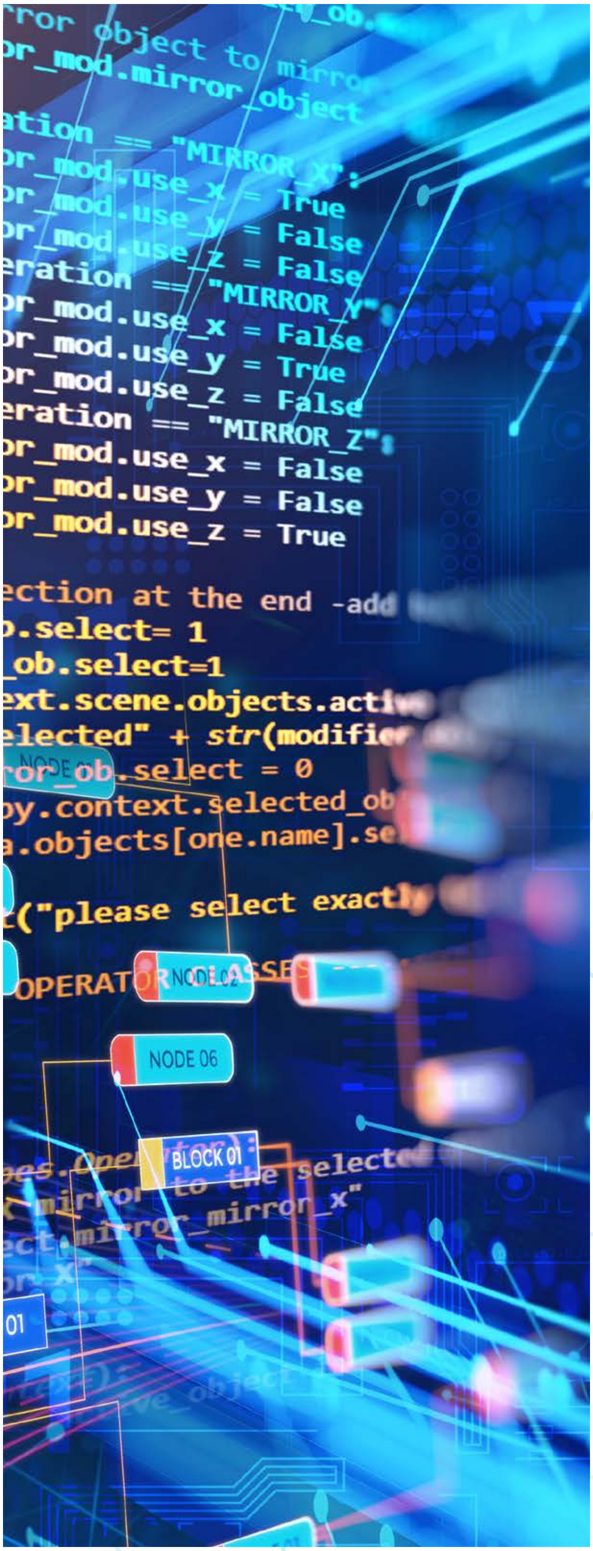
Dimitrios Vasilopoulos

Postdoctoral Researcher

Dimitrios received his PhD degree in Information Technology, Telecommunications and Electronics from Sorbonne University (France) in 2019. He holds a master degree in Communications and Computer Security from Telecom ParisTech (France) and an engineering diploma in Electronic and Computer Engineering from the Technical University of Crete (Greece).

Research Interests

Dimitrios's main research interest lies in the areas of applied cryptography and privacy-enhancing technologies with a focus on Blockchain security & privacy and cloud storage security.



research programmers

Aliaksandr Hryzlou

Degree: M.Sc. University of Mannheim, Germany.

Borja de Regil

Degree: B.Sc. in Computer Science, Universidad Complutense de Madrid, Spain.

Hadrián Rodríguez

Degree: M.Sc. in Mathematics, University of Rennes 1, France.

Andrés Mareca

Degree: B.Sc. in Computer Science, Technical University of Madrid (UPM), Spain.

research assistants

Research Assistants hold full scholarships or contracts at the Institute, performing research within one of the Institute's research lines under the supervision of a junior or senior researcher, and they undertake their Ph.D. at one of the Universities that the Institute has agreements with.

Many of our Research Assistants obtain their degrees from the Technical University of Madrid (UPM), with whom the Institute collaborates in the development of graduate programs.

Maximiliano Klemen
Research Assistant

Degree: B.Sc., Universidad Nacional del Comahue (UNCo), Argentina.

Research: Abstract interpretation-based static analysis for inferring energy consumption information about (concurrent) program executions.

Alejandro Aguirre
Research Assistant

Degree: M.Sc. in Informatics, Université Paris Diderot (Paris 7), France.

Research: Formal methods for software verification, with emphasis on the design and implementation of type systems to check relational properties of programs.

Isabel García
Research Assistant

Degree: M.Sc. in Artificial Intelligence, Technical University of Madrid (UPM), Spain.

Research: Abstract interpretation-based static analysis of programs and how it can be applied to semantic code search. Incremental analysis and verification of programs and its applications. Applications of (constraint) logic programming.

Joakim Öhman
Research Assistant

Degree: M.Sc., University of Gothenburg, Sweden.

Research: Formal verification of software and systems, with emphasis on verification of concurrent programs using type theoretic approaches.

Jesús Domínguez

Research Assistant

Degree: M.Sc., National Autonomous University of Mexico, México.

Research: Formal verification of software, concurrency, and type theory.

Felipe Gorostiaga

Research Assistant

Degree: Bsc Universidad Nacional de Rosario (UNR), Argentina

Research: Lightweight dynamic formal methods, and in particular stream approaches to the runtime verification of reactive systems. The target application is cloud testing and formal monitoring of hybrid and continuous systems.

Anaïs Querol

Research Assistant

Degree: M.Sc. in Computer Science (MPRI), Université Paris Diderot (Paris 7), France.

Research: Design and analysis of cryptographic schemes: zero-knowledge proofs for privacy-enhancing technologies and their applicability in blockchains.

Silvia Sebastián

Research Assistant

Degree: M.Sc. in Cybersecurity, Carlos III University of Madrid (UC3M), Spain.

Research: Attribution of malware, lineage of malware, PUP, malware developers in Android systems.

Nikita Zyuzin

Research Assistant

Degree: M.Sc., MPI-SWS / Saarland University, Germany

Research: Broadly interested in programming languages, type theory, and logic. Currently working on combining algebraic effects with modal types.

Daniel Domínguez

Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Mobile security and ecosystem, program and binary analysis of mobile applications, automated reverse engineering, vulnerability detection, metaheuristics for fuzzing techniques.

Kyveli Doveri

Research Assistant

Degree: M.Sc. in Mathematical Logic, Université Paris Diderot, France.

Research: Formal languages of finite and infinite words.

Luis Miguel Danielsson

Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Lightweight formal methods, in particular stream runtime verification of reactive systems. Applied to monitor decentralized systems in reliable (synchronous) and unreliable (timed asynchronous) networks with uncertainties such as failures, message losses or message reordering.

Dimitris Kolonelos
Research Assistant

Degree: M.Sc. in Electrical And Computer Engineering, National Technical University of Athens, Greece.

Research: Design of secure and privacy-preserving cryptographic protocols, zero-knowledge proofs, decentralized protocols, scalability, post-quantum cryptography.

Panagiotis Bougoulias
Research Assistant

Degree: M.Sc. in Electrical and Computer Engineering, National Technical University of Athens, Greece.

Research: Generally interested in programming languages and more specifically program synthesis, functional programming, type systems and automated theorem proving.

Alejandro Naser
Research Assistant

Degree: B.Sc., Universidad Nacional de Córdoba (UNC), Argentina.

Research: Alejandro's interests lie at the intersection of distributed protocols and formal verification.

Fedor Ryabinin
Research Assistant

Degree: M.Sc. in Computer Science, Université Paris Diderot, France.

Research: Fedor's current research interests are design and implementation of distributed protocols.

Gibran Gómez
Research Assistant

Degree: M.Sc., Technical University of Madrid (UPM), Spain.

Research: Computer, software and network security. Analysis of blockchains and their misuse on cybercrime, applying big data and machine learning techniques. Analysis of networking protocols and how to secure them.

Miëtek Bak
Research Assistant

Degree: B.Sc. in Computer Science, Uniwersytet Wrocławski, Poland.

Research: Logical foundations for programming languages, constructive theorem-proving, and proof-theoretic semantics. Intensional analysis of code in total functional programming.

Víctor Pérez
Research Assistant

Degree: B.Sc. in Computer Science, Technical University of Madrid (UPM), Spain.

Research: Static cost analysis of smart contracts via its previous compilation to a Horn Clauses intermediate representation. Currently applying this technique to the study of gas consumption in Michelson smart contracts in the Tezos blockchain.

Martín Ceresa
Research Assistant

Degree: B.Sc. in Computer Science, National University of Rosario, Santa Fe, Argentina.

Research: Programming languages design and implementation, formal verification of programs, logic, and constructive mathematics.

Zilong Wang

Research Assistant

Degree: M.Sc. Universidad Autónoma de Madrid, Spain and The University of Science and Technology of China.

Research: Zilong's interests are information security and formal methods. More specifically, apply formal methods to analysis microarchitectural side-channel attacks.

Christian Poveda

Research Assistant

Degree: M.Sc. in Systems and Computing Engineering, University of Los Andes, Colombia.

Research: Refinement type, SMT-automated verification for Rust programs with cryptographic applications.

Emanuele Giunta

Research Assistant

Degree: M.Sc. in Mathematics, University of Catania, Italy.

Research: Cryptographic topics such as secure multi-party computation and succinct non-interactive arguments of knowledge over rings. Applications to blockchain.

Juan Manuel Copia

Research Assistant

Degree: B.Sc. in Computer Science, National University of Río Cuarto, Córdoba, Argentina.

Research: Symbolic execution, software testing and automatic test generation techniques.

Diego Castejón Molina

Research Assistant

Degree: MSc in Data Science, Universitat Oberta de Catalunya.

Research: Diego insterest is in Central Bank Digital Currency (CBDC) a topic in which he was also working on in the European Central Bank. He is also interested in scalability and privacy in decentralized payment systems.

David Balbás

Research Assistant

Degree: M.Sc. in Computer Science, KTH Royal Institute of Technology, Stockholm.

Research: Cryptography for privacy-preserving verifiable computation and applications, including cloud computing, verifiable machine learning, and secure messaging.

Claudia Bartoli

Research Assistant

Degree: M.Sc. in Mathematics and applications, University Autonoma of Madrid (UAM), Spain.

Research: Analyse and secure cryptographic protocols for multi-party computation, zero-knowledge proofs, secret sharing schemes.

Elizaveta Vasilenko

Research Assistant

Degree: B.Sc., HSE University, Russia.

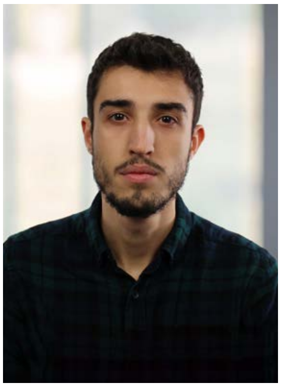
Research: Programming Languages and Software Verification, in particular design of relational type and proof systems for probabilistic programs.

Nicolas Manini

Research Assistant

Degree: M.Sc. in Computer Science, University of Pisa, Italy.

Research: Program analysis and formal verification, more specifically minimization of transition systems and abstract interpretation.



Andoni Rodríguez

Research Assistant

Degree: B.Sc. in Computer Science, University of the Basque Country, Spain.

Research: Formal methods and artificial intelligence. Currently focused on reactive synthesis and its applications in self-driving vehicles.

Margarita Capretto

Research Assistant

Degree: B.Sc. in Computer Science, National University of Rosario, Argentina.

Research: Formal verification of smart contracts and blockchain scalability.

visiting PhD

Intern	Period	Nationality
Hamidreza Khoshakhlagh	20/10/21-18/1/22	Iran
Kasra Edalatnejadkhamene	13/7/21-12/11/21	Iran
Lukas Aumayr	8/11/21-3/12/21	Austria
Man Kit Sit	1/4/20-31/3/21	Hong Kong
Mustapha Bouhali	15/9/20-14/3/21	Algeria

interns

Intern	Period	Nationality
Miguel Ángel Sánchez	09/19-06/21	Spain
Aldana Ramírez	09/20-03/21	Argentina
Elena Ortiz	11/20-02/21	Spain
Daniel Jurjo	11/20-11/21	Spain
Pablo Martínez de Leiva	09/20-06/21	Spain
Guillermo García	09/20-07/21	Spain
Nicola Amadio	09/20-02/21	Italy
Alejandro De La Cruz	09/20-07/21	Spain
Adrian Ciudad	07/20-06/21	Spain
Alberto Fernandez de Retana	12/21-12/21	Spain
Ana Marija Eres	10/21-12/21	Croatia
Arturo Villacañas	09/21-12/21	Spain
Chrysoula Oikonomou	09/21-12/21	Greece
Daniela Ferreiro	11/21-12/12	Spain
Dominik Kos	09/21-11/21	Croatia
Esteban Gil Gonzalez	09/21-12/21	Spain
Gustavo Sanchez Collado	03/21-05/21	Spain
Istvan Andras Seres	09/21-12/21	Hungray
Juan Francisco Garcia Casado	11/20-11/21	Spain
Kevin Karel Van Liebergen Avila	06/21-12/21	Spain
Lubica Jancova	05/21-11/21	Slovakia
Luka Hadzi	10/21-12/21	Serbia
Marta Centellas Nadal	04/21-09/21	Spain
Matias Nicolas Brizzio	07/21-12/21	Argentina
Meresa Gebrehiwot Gebrewahd	03/21-09/21	Ethiopia
Orfeas Kazepis	01/21-03/21	Greece
Paola Matta	12/21-12/21	France
Pierre Bourse	06/21-07/21	France
Raluca Gerogia Diugan	05/21-08/21	Rumania
Salvatore Caruso	02/21-06/21	Italy
Xiao Peng Ye	07/21-08/21	China

management and administration

María Alcaraz
General Manager

Degree: PADIIT – IESE (2019), MBA, Escuela Internacional de Negocios, CEREM, Madrid, Spain.

Tania Rodríguez
General Services Coordinator

Degree: M.Sc. in Business Administration, Universidad Centroamericana José Simeón Cañas.

Carlota Gil
Accounting & Tax Officer

Degree: M.Sc. in Business Administration, Universidad Rey Juan Carlos, Madrid, Spain.

Lídice González
Administrative Assistant

Degree: BD in Education, University of Pedagogical Sciences Félix Varela, Cuba.

Andrea Iannetta
Human Resources Assistant

Degree: B.Sc. in Economics, Godspell College, Argentina.

Ignacio Echaide
Human Resources Coordinator

Degree: M.A. in Law, Autonomous University of Madrid (UPM), Spain.

communication

Blanca Gutiérrez
Communication Manager

Degree: M.Sc. MS in Corporate Communication Management, EAE, OBS and University of Barcelona, Spain.

project management

Project management provides additional support for the development of projects and contracts being carried out at the Institute. They are often co-funded by such projects.

Juan José Collazo
Project Manager

Degree: B.Sc. in Economic Sciences, Complutense University, Madrid, Spain.

Teresa Giménez
Project Manager, N-GREENS

Degree: MS in Integrated Systems Management, University of the Balearic Islands, Spain.

Aiora Garalde
Project Assistant

Degree: BS in Business Administration and Management, University of Alicante, Spain; National University of Distance Education, Spain.

technical support

and infrastructures

Research Support Technical Staff provide support for the research infrastructures provided to the researchers at the Institute. These include virtualization environments, version control systems, research collaboration tools, continuous integration platforms, experimentation harnesses, computing farms, communications, etc.

Roberto Lumbreras

Computing and Communication Infrastructures

Degree: M.Sc. Elec. & Computer Eng., Technical University of Madrid (UPM), Spain.

Juan Céspedes

Network and Systems Engineer

Degree: M.Sc. Elec. & Computer Eng., Technical University of Madrid (UPM), Spain.

Tomas Kriukelis

Systems Administrator

Degree: M.Sc. in Telecommunications, European University of Madrid, Spain.

REDIMadrid

Carlos Ricardo de Higes
REDIMadrid Technician and Computer Operations

Degree: Licensed Electrical Technician, Instituto Juan de la Cierva, Madrid, Spain.

David Rincón
REDIMadrid Network Engineer

Degree: B.Sc. in Telecommunications, Technical University of Valladolid, Spain.

Óscar Rebollo
REDIMadrid Network Engineer

Degree: M.Sc. in Technical Telecom Engineer, Technical University of Madrid (UPM), Spain.

Alicia Cardeñosa
REDIMadrid Programmer

Degree: Network Technician.

common IMDEA services

Begoña Moreno
IMDEA Institutes' Coordination

Degree: Ph.D. in Economic Science, Universidad de Alcalá, Madrid, Spain.

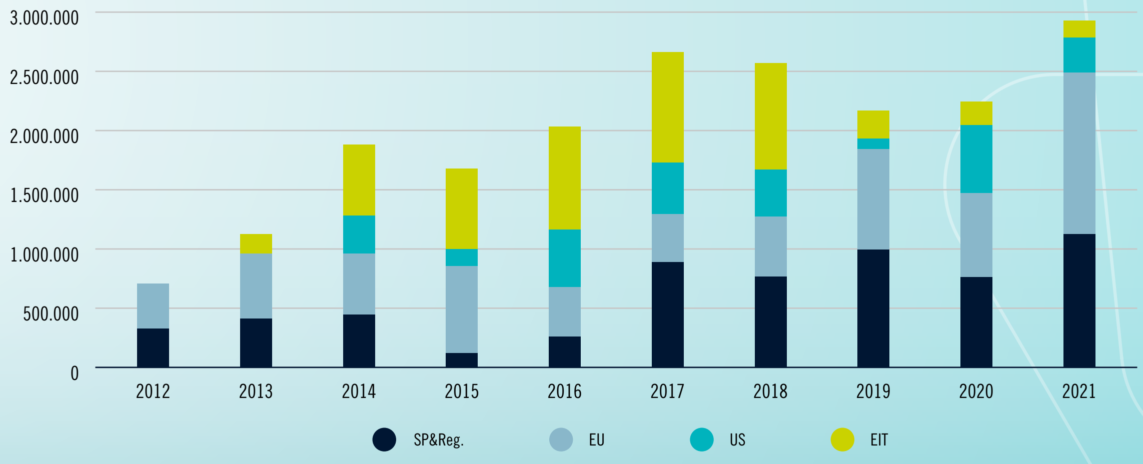
research projects and contracts

An important source of funding and technology transfer opportunities for the Institute are grants, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. During 2021, the Institute participated in a total of 25 funded research projects and contracts, of which thirteen of them (or 50%) involve collaboration with industry and eleven of them have direct industrial funding. Of these 25 projects, fifteen come from international sources (four funded by the European Union, one by the ONR-US agency, another one funded by EIT Digital and nine by foreign companies), eight have a national source, and funds for three come from regional sources, either through competitive calls or via contracts with companies. This section summarizes all the externally funded research projects active in 2021 at the IMDEA Software Institute. Note that in some of them the information that can be made public is restricted due to the funding conditions. Figure 10.1 shows the origin of project funding.

The trend of external funding for the period 2012-2021 is shown in Figure 10.2. The amount of external funding for 2021 amounts to e2.1M, with the percentage of external funding for research and innovation w.r.t. the total Institute budget reaching 42%.

research projects and contracts

Figure 1
R&I External Income



projects running in 2021

HACrypt

High-Assurance Crytography

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2019-2022
Principal Investigator: Res. Prof. Gilles Barthe

HACrypt is the continuation of SynCrypt project. HACrypt is a collaboratibe project coordinated by Stanford University, with the participation of the University of Pennsylvania, and Johns Hopkins University, funded by ONR and which runs from June 2019 until June 2022. The budget allocated for IMDEA Software in HACrypt projects is over 600 K Euros. The project will contribute to the emergence of high-assurance cryptography through the design and security analysis of key components for a high- assurance cryptographic toolbox (in particular, RNGs, proof systems). In addition, this project will develop new tools and methods for building high-assurance cryptographic implementations. The HACrypt project build on the results developed in its predecessors, Autocrypt and SynCrypt projects.

Within the project, the IMDEA Software team will work in the following research topics: automated generation of high-assurance advanced cryptographic implementation, high assurance of correctness and security against side-channel attacks, and automated synthesis of cryptographic constructions.

BLOQUES-CM

Contratos inteligentes y blockchains escalables y seguros mediante verificación y análisis

Funding: Regional Government of Madrid
Duration: 2019–2022
Project Coordinator: Assoc. Res. Prof. Juan Caballero

The BLOQUES-CM project addresses the growing importance of blockchain-based technology, which, by using techniques from distributed systems and cryptography, and within the framework of a distributed database that registers transactions, allows participants to agree on which of these transactions are valid. Once transactions are accepted, the blockchain ensures that these cannot be modified. Likewise, it is practically impossible to present as valid a non-existent transaction.

In particular, BLOQUES-CM will advance the state of the art in: anonymity and integrity properties of distributed ledgers; verification of infrastructures for distributed ledgers; proofs of correction and resource usage of smart contracts; the application of testing to distributed ledgers; and the availability and development of tools to support the previous goals.

BLOQUES-CM is a consortium involving groups from Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and the IMDEA Software Institute, which is the project coordinator.

MadQuantum-CM

Proyecto coordinado de Comunicaciones Cuánticas: Comunidad de Madrid

Funding: Regional Government of Madrid - Spanish Ministry of Science, Innovation - EU Next Generation
Duration: 2021–2024
Principal Investigators: Assoc. Res. Prof. César Sánchez

The *MadQuantum-CM* project is part of the "Complementary R&D&I Plans" of the Spanish "Recovery, Transformation and Resilience Plan" within the quantum communications line.

MadQuantum-CM aims at providing a unique quantum communication technology development environment. MadQuantum-CM will allow realistic demonstrations of the capabilities of the technologies in production environments and also of the services that can be provided by quantum networks such as critical infrastructure protection, highly secure database connections, symmetric key distribution for defense services, applications in banking, medicine, etc. These capabilites will eventually pave the way for the Region of Madrid to become a permanent node of the European Quantum Communications Infrastructure (EuroQCI).

The MadQuantum-CM consortium includes the Technical University of Madrid (UPM), the Spanish Metrology Center (CEM), the Complutense University of Madrid (UCM), the Autonomous University of Madrid (UAM), the National Institute for Aerospace Technology (INTA), the IMDEA Networks Institute, and the Vithas Foundation.

MadQuantum-CM is supported by MCIN with funding from European Union NextGenerationEU (PRTR-C17.I1) and by Comunidad de Madrid.

MadridFlightOnChip

Consortium Madrid for Next-Generation Flight Systems Based on Multiprocessor System-on-a-Chip Technology

Funding: Regional Government of Madrid
Duration: 2019–2022
Principal Investigators: Asst. Res. Prof. Alessandra Gorla – Assoc. Res. Prof. César Sánchez – Res. José Francisco Morales

Madrid Flight on Chip (MFoC) is a research and innovation project linked to the RIS3 Smart Specialization Platform and co-funded by the Comunidad de Madrid. It consists on a platform for the development of space missions, particularly research and demonstrator satellites. IMDEA Software will focus on developing innovation in the area of software validation, specifically adapted to these missions.

MFoC is a consortium involving groups from academic partners, Universidad Carlos III de Madrid and IMDEA Software, and also from the industrial partners CENTUM Solutions, GENERA Soluciones Tecnológicas, Knowledge Centric Solutions, MARM Desarrollo de Sistemas, and SENER Aerospacial, which is the project coordinator.

BOSCO

Foundations for the development, analysis and understanding of BlOck chains and Smart COntracts

Funding: Spanish Ministry of Science, Innovation and Universities
Duration: 2019-2021
Principal Investigators: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Pierre Ganty

The main goal of BOSCO project is the development of foundations for (1) the formal analysis of the distributed infrastructure that implements Blockchains and how to optimize its performance; and (2) the analysis and verification of smart contracts. Proving mathematically the correctness of software is not a new problem and many aspects has been extensively studied for years. However, Blockchains present new risks and opportunities.

In terms of the infrastructure, there are two fundamental elements in the Blockchain: cryptographyc functions and consensus algorithms to reconcile the distributed database. One of the lines of this project is devoted to the study how to verify consensus algorithms, which is critical to guarantee that the Blockchain does not present errors that could be exploited. Another line in this project is devoted to hardware based optimizations, and another task studies how to improve the scalablility of consensus using sharding.

In addition, the most promising applications of Blockchain will be the use of smart contacts. On one hand, smart contracts are a computer representation of legal contracts among entities, possibly humans. On the other hand, smart contracts are very similar to computer programs in the sense that they precisely describe the steps taken in the evolution of a contract and what are the capabilities of each agent at each point. From this second point of view, smart contracts are pieces of software, with the same potential and risks of pitfalls. Technically, smart contracts present some of the opportunities because some of the aspects that make software verification hard are not present, like complex computer architectures, dynamic memory and instruction level parallelism. On the other hand, to reason about smart contracts we need to model aspects like interactions between agents and the interlevings between different accesses to the Blockchain. We devote two lines to develop the foundations for the study of smart contracts. Particularly, one of the lines study the deductive verification using interactive theorem provers. The other focuses on logics for the specification and runtime verification.

SCUM

Securing Untrusted Machines

Funding: Spanish Ministry of Science, Innovation and Universities
Duration: 2019-2022
Principal Investigators: Assoc. Res. Prof. Juan Caballero – Assoc. Res. Prof. Dario Fiore

The objective of the SCUM project is increasing the trust on the machines used to build information systems. The project focuses on three fundamental challenges related to this objective: (1) Providing trust on remote computations and data storage on third-party machines; (2) Detecting systems that may have been compromised, and thus should not be trusted, as well as identifying those responsible for the compromise; and (3) Removing vulnerabilities in the software and platform components used as building blocks of the digital systems.

The project is organized in a number of coordinated lines that cover advances in analysis, verification, testing, optimization and code generation, and tool development.

The research carried out in SCUM will impact multiple booming digital economy markets including data protection, cloud computing, blockchain, malware defenses, and secure software testing. To achieve its objectives the scientific team of the SCUM project comprises researchers from one of Europe's leading research groups in cybersecurity, as well as Ph.D. students and prominent international collaborators.

ProCode

Rigorous methods for the development of software systems with certified quality and reliability

Funding: Spanish Ministry of Science and Innovation
Duration: 2020-2024
Principal Investigators: Assoc. Res. Prof. Manuel Carro – Res. José Francisco Morales

The objective of the ProCode project is to contribute both foundations and technologies that can facilitate the task of developing software systems with certified quality and reliability, following the current trend of increasing use of formal methods. Indeed, techniques such as abstract interpretation-based analysis and formal verification are now a crucial element in program development toolchains.

The work plan of the project is organized in 3 research lines covering those challenges: Untrusted Third-Party Machines, Untrusted Compromised Systems and Untrusted Vendors.

This project is in part an evolution of our previous coordinated project TRACES, including the two participating research goups from IMDEA Software and Universidad Complutenses de Madrid, but it puts less focus on the issue of resource analysis and covers the topics of analysis, verification, testing, and optimization, which are relevant topics due to the rising importance of ensuring software integrity.

SECURING

Secure cryptographic protocols for ring arithmetic

Funding: Spanish Ministry of Science and Innovation
Duration: 2020-2023
Principal Investigator: Asst. Res. Prof. Ignacio Cascudo

This project is framed within a program designed to provide funding for promising young researchers. SECURING will address two topics within the area of cryptography that have been received a great deal of attention in the last years, namely: secure multiparty computation and zero-knowledge proofs.

The goal of this project is to solve a specific problem that impacts many constructions of general-purpose secure computation protocols and zero knowledge proofs. This source of this problem is that part of the techniques used to design these protocols require the function describing the computation to be represented as a series of basic operations over what is mathematically known as finite field. However, this is not a natural representation in many cases and this causes and additional source of complexity. We will work towards overcoming these limitations by providing alternative constructions.

Europa Excelencia

CRYPTOEPIC: Criptografía para asegurar la privacidad y la integridad de la computación en máquinas no confiables

Funding: Spanish Ministry of Science, Innovation and Universities
Duration: 2019-2021
Principal Investigator: Assoc. Res. Prof. Dario Fiore

The *Europa Excelencia* grants, funded by the MCIU, support proposals submitted to ERC Starting and Consolidator Grants from Spanish research centers which were ranked with A, but not funded due to budget constraints. IMDEA Software has obtained one of these grants to support the development of some tasks included in the research proposals submitted to the European Research Council (for Consolidator Grants by Dario Fiore) in the 2019 call.

PICOCRYPT

Cryptography for Privacy and Integrity of Computation on Untrusted Machines

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2021-2026
Principal Investigator: Assoc. Res. Prof. Dario Fiore

The grand challenge of this project is to invent a new generation of cryptographic protocols for computing securely on untrusted machines in a way that is cost-effective and suitable for future application scenarios. Towards this goal IMDEA researchers will design new methods to scale up the applicability of cryptographic protocols. One of the key approaches will be trading generality for efficiency. While existing solutions are either general but impractical or efficient but of limited applicability, in PICOCRYPT our researchers will look for protocols that support a wide range of applications while staying efficient. The PICOCRYPT solutions will enable a paradigm shift in the way privacy and integrity will be enforced and will have impact in the IT world by making remote computing safer not only for citizens but also for public and private organizations that due to the current risks renounce to these services.

RACCOON

A Rigorous Approach to Consistency in Cloud Databases

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2017-2023
Principal Investigator: Assoc. Res. Prof. Alexey Gotsman

The goal of this project is to develop a synergy of novel reasoning methods, static analysis tools, and database implementation techniques that maximally exploit parallelism inside cloud databases, while enabling application programmers to ensure correctness. We intend to achieve this by first developing methods for reasoning formally about how weakening the consistency guarantees provided by cloud databases affects application correctness and the parallelism allowed inside the databases. This will build on techniques from the areas of programming languages and software verification. The resulting theory will then serve as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that its side effects do not compromise application correctness.

Mathador

Type and Proof Structures for Concurrent Software Verification

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2017-2023
Principal Investigator: Assoc. Res. Prof. Aleksandar Nanevski

The grand challenge of this project is to remove existing limitations which make proofs generated with proof assistants unmanageable by humans, and to scale dependent types to support the implementation of stateful concurrent programs and their correctness proofs simultaneously. By applying the modularizing power of dependent types to both programs and proofs, the project will obtain novel and scalable foundations for the field of concurrent software verification. Writing mechanized proofs of software, concurrent or otherwise, is generally considered infeasible. But if one chooses the right linguistic abstractions to express the proofs, we argue that it does not have to be so. This observation is supported by our encouraging preliminary results. The project will design further novel linguistic abstractions that facilitate engineering of practically feasible formal proofs, and experimentally evaluate them by mechanically verifying extensive concurrent programs drawn from realistic applications, such as concurrent garbage collectors, OS kernels, and popular open-source concurrent libraries.

OPENQKD

Open European Quantum Key Distribution Testbed

Funding: European Union – H2020 Framework Program
Duration: 2019-2022
Principal Investigator: Assoc. Res. Prof. César Sánchez

The Project goal is the establishment of QKD-based secure communications as a well-accepted, robust and reliable technology instrumental for securing traditional industries and vertical application sectors, and to prepare the deployment of a future Europe-wide QKD-based infrastructure.

The high level objectives are: raising the awareness about the maturity of QKD; working with end-users to test and validate end-to-end security for businesses and industry sectors based on or requiring QKD; advancing QKD systems and QKD-based secure-communication solutions to meet market demands in terms of specifications, standards, and certification; and, finally, provide several open test facilities to encourage the development of new QKD-based applications by a wide community.

The consortium is composed by 38 members (including 18 private European companies), four of them from Spain. The IMDEA Software Institute participates by providing the REDIMadrid telecommunications network, managed by the Institute, as physical infrastructure, as well as the expertise of the REDIMadrid staff. With this participation, a research network will be deployed over REDIMadrid. That will make it possible to work around renting network capacity, which is less flexible than the dark fiber whose rights of used were already bought by IMDEA Software: in the REDIMadrid network, quantum transmission channels will physically coexist with traditional (research) channels without interfering, thereby making it possible to verify how the proposed quantum distribution solutions work in a real environment.

EIT Digital CLC

EIT Digital Co-Location Center

Funding: EIT Digital

The Institute hosts the headquarters of EIT Digital, a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT), which became a full node in September 2016, still under the leadership of IMDEA Software.

The Co-Location Center of EIT Digital Spain is the main meeting point for the members of the node and its joint activities. Its presence is supported by a specific agreement aimed at funding the usage and maintenance of the facilities (offices, A/V, meeting spaces, etc.) that are made available to EIT Digital Spain. Having the CLC in the headquarters of the Institute makes it possible for PhD and Master students registered at the EIT-labeled degrees to interact with Institute researchers. Likewise, the startups hosted at the CLC can interact with the Institute researchers and attend activities at the Institute (technical talks, workshops, etc).

INTEL

Information Flow Tracking across the Hardware-Software Boundary

Funding: Intel Corporation
Duration: 2018-2021
Principal Investigator: Asst. Res. Prof. Marco Guarnieri.

This project focuses on the development of a novel, principled approach for software defenses against SPECTRE-style attacks. Its key feature is that it is backed by semantic security guarantees, yet it does not require programmers to provide any specification or annotations. It will pave the way to formally characterize the security guarantees envisioned by the project; these will lead to a blueprint for the design, implementation, and evaluation of program analysis techniques to detect this kind of attacks. The project is completely funded by Intel, and puts together a team from the IMDEA Software Institute, the University of Saarland, the Catholic University of Leuven, and the Technical University of Graz.

HascoSec

Principled security verification of processors using hardware-software contracts

Funding: Intel Corporation
Duration: 2021-2022
Principal Investigator: Asst. Res. Prof. Marco Guarnieri.

This project focuses on preventing microarchitectural and side-channel attacks by addressing two challenges:

1. Processors' security guarantees must be precisely formalized in a way that is understandable for programmers— which will rely on them to construct secure systems— ideally without being tied to specific microarchitectural details.

2. Scalable verification techniques are needed to (a) check whether processor designs satisfy a given set of security guarantees, and (b) to infer the security guarantees satisfied by processor designs.

To address the first challenge, HascoSec researchers proposed hardware-software contracts as an abstraction that captures a processor's security guarantees in a simple, mechanism-independent manner. Current security verification techniques for processors, however, fall short of addressing the second challenge: they focus on low-level security properties tailored towards specific microarchitectural details and they require user-provided annotations of security properties.

HascoSec will develop models, verification techniques, and tools for automatically verifying and inferring security properties from processors designs specified in Verilog. To specify security properties, project's researchers rely on hardware-software contracts, which concisely model which program executions a side-channel adversary can distinguish. HascoSec will provide hardware designers with languages for specifying security contracts and techniques for automatically determining whether processors comply with a given contract. Therefore, hardware designers will be able, during the design phase (detect phase in the security lifecycle), to automatically assess a design's security guarantees or find security violations. The use of contracts will enable them to easily specify security properties at a high level and with minimal effort, while low-level encodings of the property in Verilog will be automatically generated through the verification process.

After introducing hardware-software contracts, HascoSec researcher will discuss the plans for designing, implementing, and evaluating new verification techniques.

This project is funded by Intel Corp., and includes research teams from the IMDEA Software Institute (which is the project coordinator) and the University of Saarland.

NEC Industrial Research Grant

Secure Computation for Machine Learning

NEC

Funding: NEC Labs Europe Duration: 2021
Principal Investigator: Assoc. Res. Prof. Dario Fiore

Machine Learning platforms are key to mining vast amounts of data stemming from diverse application scenarios, such as e-health, IoT, or 5G networks. Nevertheless, there is an increasing discussion on the collection and usage of privacy-sensitive data by Machine Learning platforms. In order to leverage their full power, technological advances in terms of data privacy and security are necessary.

To face this challenge, IMDEA and NEC researchers have started a research program investigating how to balance the functionality of Machine Learning platforms with the security and privacy of both data suppliers and data consumers. This investigation addresses two main topics. First, the general problem of computation over encrypted data which allows to find a balance between utility and privacy;

and second, attestation, i.e., authentication and authorization mechanisms for effective access control and data handling.

SECURITAS

Red de Investigación en Ciberseguridad y Privacidad

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2020-2022
Principal Investigator: Assoc. Res. Prof. Dario Fiore

The Research Network on Cybersecurity and Privacy (SECURITAS), which is coordinated by Rovira and Virgili University and includes researchers from 9 spanish universities and research centers, aims at consolidating and reinforcing a common area of research in cybersecurity and high-level information privacy in Spain. The various groups are working to formalize an alliance to make research and its transfer more effective and competitive. In order to do this, each of the groups will contribute their experience in one or more specific aspects so that multifarious research advances become possible through cooperation with the rest of the members of the network. At the same time, the network will work so that the developed solutions are effectively transferred to society through the work of a valorization expert, who will be an intermediary between universities and the interested productive sectors. Another objective of the network will be to promote the participation of different groups in national and European initiatives, specifically in the H2020 and Horizon Europe programs of the European Commission. The experience of the groups that are currently participating in European projects will help the rest of the groups to explore the possibilities of participating in proposals with another member of the network or on their own.

TEZOS

Cryptographic Primitives for Randomness Generation and Privacy

Funding: TEZOS Foundation - Nomadic Labs
Duration: 2020–2022
Principal Investigators: Assoc. Res. Prof. Dario Fiore – Asst. Res. Prof. Ignacio Cascudo

Collaboration project arised from the framework agreement signed between the franch company Nomadic Labs and IMDEA Software to maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation, through the French company Nomadic Labs, is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem.

The goal of this project is to design zkSNARKs that support only specific classes of computations but with better efficiency than general-purpose solutions. To this end, IMDEA researchers will follow the commit-and-prove approach of LegoSNARK so that these new specialized proof systems can be combined. The specialized computations that our investigators aim to address will include set (non)membership, vector commitments, and digital signatures.

TEZOS

Cost Analysis, Verification, and Optimization for Tezos via Parametric Resource Analysis

Funding: TEZOS Foundation - Nomadic Labs
Duration: 2020–2023
Principal Investigator: Res. Prof. Manuel Hermenegildo

Collaboration project arised from the framework agreement signed between the franch company Nomadic Labs and IMDEA Software to maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation, through the French company Nomadic Labs, is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem.

The main goal of this project is to develop a flexible and easily configurable method and tool for the static analysis, verification, and optimization of resources for Tezos. The objective is to estimate the resource usage of smart contracts as functions parameterized by metrics of the input data, and deal with a wide range of resources such as gas and storage space, as well as more basic resources (number of allocations, steps, bytes read, bytes written, etc.). The tool will allow the user to define resources and the associated cost models in a flexible way by means of an assertion language.

TEZOS

Systematic Design of Blockchain Consensus Protocols

Funding: TEZOS Foundation - Nomadic Labs
Duration: 2021–2023
Principal Investigators: Assoc. Res. Prof. Alexey Gotsman – Post. Res. Manuel Bravo

Collaboration project arised from the framework agreement signed between the franch company Nomadic Labs and IMDEA Software to maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation, through the French company Nomadic Labs, is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem.

The goal of this project is to develop generic techniques that will enable systematically designing correct Byzantine consensus protocols for blockchains. IMDEA researchers envision constructing a blockchain consensus protocol with desired features in a modular way, by applying generic and provably correct transformations to baseline protocols with well-understood characteristics.

SLN

Scalability for the Lightning Network

Funding: Chaincode labs Inc. - Technical University of Wien
Duration: 2020–2021
Principal Investigator: Asst. Res. Prof. Pedro Moreno

This project plans to lay the foundations of security and privacy for off-chain contracts and study practical cryptographic constructions as well as theoretical limits with this technology.

The main goals of the SLN project are: 1) To design and build efficient cryptographic constructions for off-chain contracts; 2) Formally prove their security and privacy guarantees; and 3) Create a software tool where we can develop and test prototypical implementations in order to bootstrap its practical deployment.

STELLAR

Increasing the Confidence in the Consistency and Liveness of the Stellar Ledger

Funding: Stellar Foundation
Duration: 2021-2022
Principal Investigator: Assoc. Res. Prof. Alexey Gotsman

This project proposes to improve a) the formal analysis of SCP (Secure Copy Protocol) and b) the SCP protocol itself, to give stronger safety and liveness guarantees to the Stellar Ledger. On the formal analysis front, the project's researchers have proposed to mechanically prove the safety and liveness properties of the concrete, bounded-state ballot protocol, proposing a fine-grained analysis of the properties of SCP under dynamically changing slices. On the protocol front, the project aims to modify SCP to make use of a leader-election component in order to achieve liveness under eventual synchrony, proposing to devise a practical leader-election algorithm.

This project is funded by Stellar Development Foundation, and includes research teams from the University of Surrey, which coordinates the project, Galois Inc., and the IMDEA Software Institute.

GMV Industrial contract

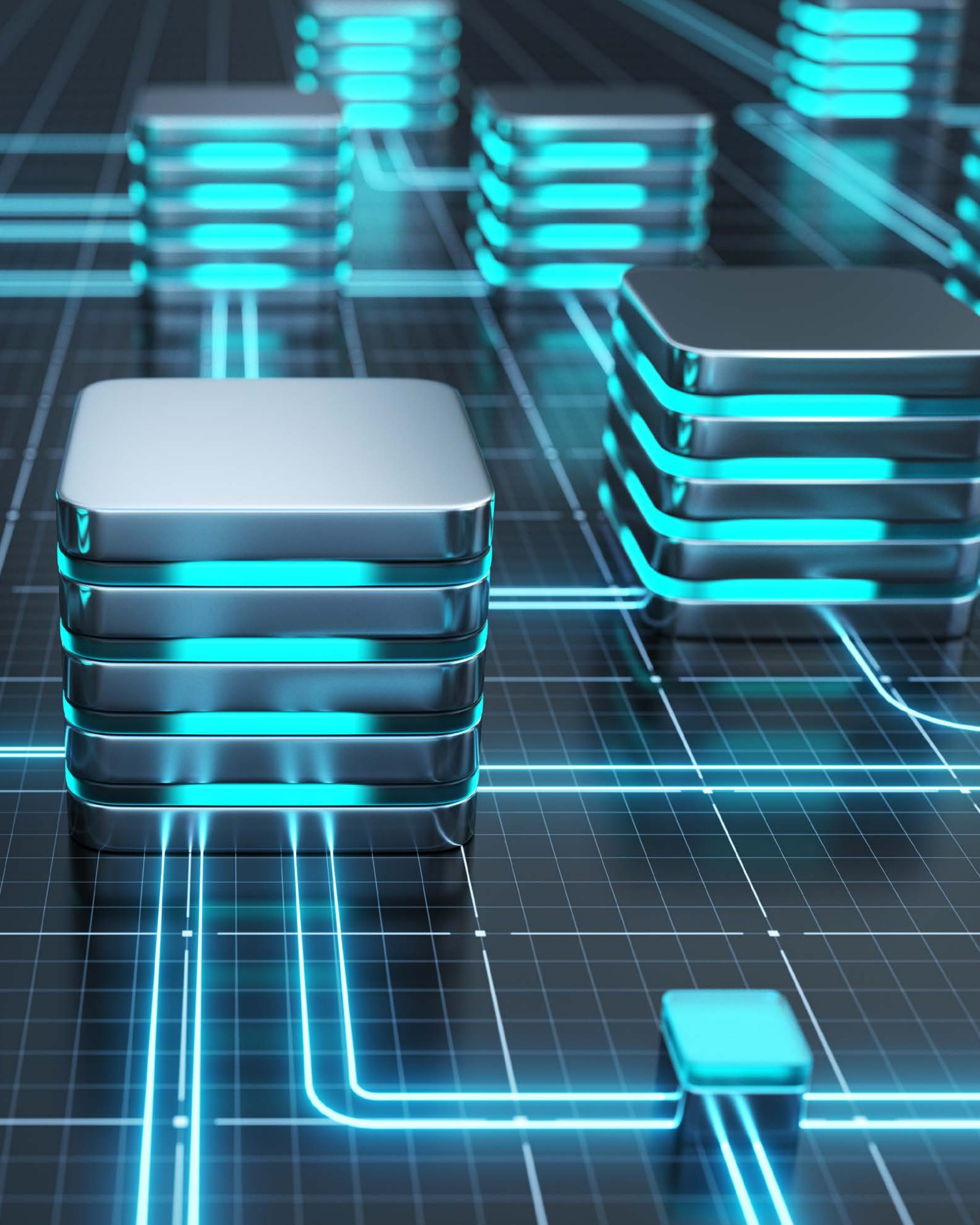
Security analysis of multiparty computation protocols

Funding: GMV Soluciones Globales Internet S.A.U.
Duration: 2021
Principal Investigator: Assoc. Res. Prof. Dario Fiore – Asst. Res. Prof. Ignacio Cascudo

uTile PET (2021-H2)

uTile PET (2021-H2)

Funding: GMV Soluciones Globales Internet S.A.U.
Duration: 2021
Principal Investigator: Asst. Res. Prof. Ignacio Cascudo – Assoc. Res. Prof. Dario Fiore



Some companies with which the IMDEA Software Institute has collaborated through projects and contracts to date

Project/Contract	Funding Entity	Industrial Partners
MOBIUS	FP6: IP	France Telecom, SAP AG, Trusted Labs
HATS	PF7: IP	Fredhopper
NESSoS	PF7: NoE	Siemens, ATOS
ES_PASS (*Through an associated group at UPM.*)	ITEA2, MITyC	Airbus France, Thales Avionics, CS Systèmes d'Information,Daimler AG, PSA Peugeot Citroën, Continental, Siemens VDO Automotive, EADS Astrium, GTD, Thales Transportation, and IFB Berlin
EzWeb	MITyC	Telefónica I+D, Alimerka, Integrasys, Codesyntax, TreeLogic, Intercom Factory, GESIMDE, Yaco, SoftTelecom
DESAFIOS-10	MICINN	BBVA-GlobalNet, LambdaStream, Deimos Space
PROMETIDOS	Madrid Regional Government	Deimos Space, Atos Origin, BBVA-GlobalNet, Thales, Telefónica I+D
MTECTEST	Madrid Regional Government	Deimos Space
SEIF awards	Microsoft SEIF	Microsoft Research
Ph.D. Scholarships	Microsoft	Microsoft Research
ENTRA	FP7: STREP	XMOS
VARIES	FP7: ARTEMIS	Barco NV, HI iberia, IntegraSys, Tecnalia, Sirris, Spicer, FraunhoferGesellschaft,Pure-SystemsGmbh,STiftelsenSintef, Autronica, Franders Mechatronics Technology Centre, Atego Systems, Teknologia Tutkimuskeskus VTT, Mobisoft, HIQ Finland, Softkinetic Sensors, Macq, MetsoAutomation.
4CaaST	FP7: IP	Telefónica I+D, SAP, France Telecom, Telecom Italia, Ericsson, Nokia-Siemens, Bull SAS, 2nd Quadrant, Flexiant
POLCA	FP7: STReP	Maxeler, Recore
Cadence	EIT	Reply SpA
FI-PPP-Liaison	EIT	Engineering Ingegneria Informatica SpA, Orange, Thales, Create-Net
NEXTLEAP	H2020	Merlinux
ELASTEST	H2020	Fraunhofer, Telecom Italia, Atos, Tikal Technologies, IBM Ireland, Relational
DataMantium	MINECO	Scytl
AxE Javascript	MINECO	Scytl
HC@WORKS	EIT	Atos, Thales, Engineering, CEA List
SMAPPER	EIT	Telecom Italia, Backes SRT
ANTIFRAUD	EIT	Reply SpA
MadridFlightOnChip	Madrid Regional Government	SENER Aerospacial, CENTUM, GENERA, REUSE, MARM
Information Flow Tracking across the Hardware-Software Boundary	Intel Corporation	Intel Corporation
POST	Protocol Labs	Protocol Labs
Contracts	Microsoft	Microsoft Research
Contracts	AbsInt	AbsInt GmbH
Contracts	Boeing	Boeing Research & Technology Europe
Contracts	Telefónica	Telefónica I+D
Contracts	LogicBlox	LogicBlox
Contracts (eTUR2020)	Zemsania	Zemsania, Tecnocom, Groupalia, Solusoft, Eurona, BDigital
Contracts	NEC	NEC Labs Europe GmbH

Contracts	INDRA	INDRA Sistemas S.A.
Contracts (Ciber 4.0)	RedBorder	RedBorder.
Contracts (RiskIoT)	Nextel	Nextel S.A. Ingeniería y Consultoría
Contracts (Facebook)	Facebook	Facebook Connectivity Lab Tech, Inc.
OPENQKD	H2020	Services Industriels de Geneve, Toshiba Research Europe, Id Quantique, Deutsche Telekom, Rohde and Schwarz Cybersecurity, ADVA Optical, Mellanox, Nokia Bell Labs, Fragmentix,Telefónical+D,BritishTeleCom,Orange,Citycom, DINDeutschesInstitutfürNormung,NPLManagement,Thales, IXBLUE, Thales, MT Pelerini GroupSA
ACCORD	H2020	IBM Research
AutoCrypt	ONR - Stanford University	SRI65International
SynCrypt	ONR - Stanford University	SRI International
Contracts (BBVA)	BBVA	BBVA
Contracts (SLN)	Chaincode	Chaincode Labs Inc.
Contracts (Consensus Scalability, Resource Analysis, Randomness, Runtime Verification)	Nomadic Labs	Tezos / Nomadic labs.
HascoSec	Intel Corporation	Intel Corporation
Contracts	GMV	GMV Soluciones Globales Internet S.A.U.
Contracts (functional vector commitments)	Protocol Labs	Protocol Labs
Contracts (Consistency and Liveness)	University of Surrey / Stellar Foundation	Galois

fellowships

1. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2018 and ending in 2023 (**Pierre Ganty**).

2. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2016 and ending in 2021 (**Alexey Gotsman**).

3. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2021 and ending in 2026 (**Alessandra Gorla**).

4. *Juan de la Cierva grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2021 (**Manuel Bravo**).

5. *Juan de la Cierva grant*, Spanish Ministry of Science and Innovation, awarded in 2020 and ending in 2022 (**Marco Guarnieri**).

6. *Juan de la Cierva grant*, Spanish Ministry of Science and Innovation, awarded in 2020 and ending in 2023 (**Niki Vazou**).

7. *Juan de la Cierva grant*, Spanish Ministry of Science and Innovation, awarded in 2021 and ending in 2025 (**Pedro Moreno-Sanchez**).

8. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2024 (**Niki Vazou**).

9. *Atracción de talento grant*, Madrid Regional Government, awarded in 2021, and ending in 2025 (**Srdjan Matic**).

10. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2017 and ending in 2021 (**Elena Gutierrez**).

11. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2020 and ending in 2024 (**Gibrán Gómez**).

12. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture, and Sports, awarded in 2017 and ending in 2021 (**Isabel García**).

13. *FPU Doctoral Grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2023 (**Silvia Sebastián**).

14. *FPU Doctoral Grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2024 (**Luís Miguel Danielsson**).

15. *La Caixa Doctoral Grant*, La Caixa Foundation, awarded in 2018 and ending in 2021 (**Anaïs Querol**).

Comunidad de Madrid

Unión Europea
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Financiado por la Unión Europea
NextGenerationEU

Obra Social
Fundación "la Caixa"

GOBIERNO DE ESPAÑA · MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

projects to start in 2022

CRETE

Certified Refinement Types

Funding: European Union, European Research Council – Horizon Europe Framework Program
Duration: 2021-2026
Principal Investigator: Asst. Res. Prof. Niki Vazou

The goal of the CRETE project is to design a sound and practical refinement type system. This ambitious goal entails the development of a verification system that is as practical as refinement types and constructs machine-checked mathematical proofs. The system will be implemented on refinement type systems for mainstream languages (i.e., Haskell and Rust) and will be evaluated on real-world code, such as web applications and cryptographic protocols.

TEZOS

Off-chain Runtime Verification of Tezos

Funding: TEZOS Foundation - Nomadic Labs
Duration: 2022–2024
Principal Investigators: Assoc. Res. Prof. César Sánchez

This collaboration project arose from the framework agreement signed between the French company Nomadic Labs and the IMDEA Software Institute to maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem.

The goal of this project is to create the technology to be able to monitor and analyze the execution of a blockchain without impacting the blockchain itself (that is, as an off-chain process) in order to obtain information about the behavior of the different agents (external users, bakers, etc.) to assess their security and fairness, assign blame, synthesize explanations, etc.

To achieve these goals, the IMDEA Institute will (1) design a specific runtime verification language to query information about the blockchain execution, (2) adapt and extend existing techniques to collect and index the necessary information in order to evaluate queries in the language, and (3) build tools to inspect the blockchain using these indices, as well as simulate the behaviour of smart contracts to reason about hypothetical executions, correlate executions at different times, evaluate monitors, etc.

NEC Industrial Research Grant

Secure, Private, and Verifiable Computation for Machine Learning

NEC

Funding: NEC Labs Europe
Duration: 2022
Principal Investigator: Assoc. Res. Prof. Dario Fiore

This project continues the research collaboration between IMDEA and NEC Labs started in 2018. This specific collaboration will unfold along three main axes. Firstly, it will make advances on cryptographic mechanisms to compute over encrypted data to allow Machine Learning applications use data of sensitive nature, such as medical data. Secondly, it will research techniques for effective access control by means of authentication and authorization, in order to regulate access to data and applications. And thirdly, it will devise mechanisms for verifiable Machine Learning refining the trust model of computing platforms.

Protocol Labs industrial project

Improve the understanding of functional vector commitments: quadratic functions and underlying assumptions

Protocol Labs

Funding: Protocol Labs
Duration: 2022-2024
Principal Investigator: Assoc. Res. Prof. Dario Fiore

This project aligns with the collaboration established with the US company *Protocol Labs* in 2018. Its main goal is to advance the study of functional vector commitments (VC) beyond linear functions. In particular, our researchers are interested in studying the challenges of realizing functional VCs in this scenario from simple assumptions and on realizing functional VCs that can be updated.

To reach this goal, the Institute will investigate the limits and possible improvements of the construction of functional VCs. As an initial direction towards this goal, our researchers will investigate the possibility of designing concise VC for linear functions with sublinear parameters, which would immediately imply a functional VC for quadratic functions with sub-quadratic parameters. In addition, the IMDEA Software researchers also plan to exploit this connection to study potential impossibility results.

MADRIDNIGHT

Researchers and citizens: facing together the European challenges

Funding: European Union – Horizon Europe Framework Program
Duration: 2022-2024
Principal Investigator: Assoc. Res. Prof. Manuel Carro

The MADRIDNIGHT project will bring together researchers and the general public to increase the awareness about the relevance and benefits of research and innovation, create an understanding of the impact of researchers' work on the citizen's daily life, and raise the young people's interest in science and research careers.

The project will pursue these objectives by means of lively activities to be carried out in the Region of Madrid during the evening and morning of the last Friday and Saturday, resp., of September in 2022 and 2023. Pre-events and post-events will be also organized. The Madrid Night project also includes *Researchers at the School* activities throughout the year. In these activities, researchers will be visiting schools, allowing teachers and students to engage with them on important topics faced by our society. Students and teachers will also visit the researchers' institutions.

The MADRIDNIGHT activities are devised for people regardless of their scientific background: children, teachers, students, the elderly... and will present STEM topics to high-school students, university students, and students in vocational training to increase the number of students in this area.

The project includes the participation of all the Madrid public Universities and many research centres, museums, hospitals, NGOs, and companies in the Madrid Region.

communication and dissemination

munication

ssemination

Publications

The vast majority of the research of the Institute is published at highly-ranked conferences and journals. In line with what is common in Computer Science, and unlike what happens in other disciplines, conferences are often preferred to journals for a variety of reasons. Therefore, most of our researchers target them primarily to present bleeding-edge work, and submit to journals only archival papers after they have been presented at the leading conferences of their fields.

In addition to peer-reviewed papers, we list in this section conference proceedings edited by our researchers, articles in books, and theses (at the levels of Bachelor, Master, and PhD).

Refereed Publications

Journals

1. Emanuele De Angelis, Fabio Fioravanti, *John P. Gallagher*, *Manuel V. Hermenegildo*, Alberto Pettorossi, Maurizio Proietti. Analysis and Transformation of Constrained Horn Clauses for Program Verification. Theory and Practice of Logic Programming, Cambridge U. Press, November 2021.

2. *Pierre Ganty*, Francesco Ranzato, *Pedro Valero*. Complete Abstractions for Checking Language Inclusion. ACM Trans. Comput. Logic, Vol. 22, Num. 4, pages 1–40, Association for Computing Machinery, September 2021.

3. M.A. Sanchez-Ordaz, *I. Garcia-Contreras*, V. Perez-Carrasco, *J. F. Morales*, *P. Lopez-Garcia*, *M. V. Hermenegildo*. VeriFly: On-the-fly Assertion Checking via Incrementality. Theory and Practice of Logic Programming, Vol. 21, Num. 6, pages 768–784, Cambridge U. Press, September 2021. Special Issue on ICLP'21.

4. *I. Garcia-Contreras*, *J. F. Morales*, *M. V. Hermenegildo*. Incremental and Modular Context-sensitive Analysis. Theory and Practice of Logic Programming, Vol. 21, Num. 2, pages 196–243, Cambridge U. Press, January 2021.

5. *Alejandro Aguirre*, *Gilles Barthe*, Marco Gaboardi, Deepak Garg, Shin-ya Katsumata, Tetsuya Sato. Higher-order probabilistic adversarial computations:

categorical semantics and program logics. Proc. ACM Program. Lang., Vol. 5, Num. ICFP, pages 1–30, 2021.

6. *Alejandro Aguirre*, *Gilles Barthe*, Justin Hsu, Benjamin Lucien Kaminski, Joost-Pieter Katoen, Christoph Matheja. A pre-expectation calculus for probabilistic sensitivity. Proc. ACM Program. Lang., Vol. 5, Num. POPL, pages 1–28, 2021.

7. *Gilles Barthe*, Marc Gourjon, Benjamin Grégoire, Maximilian Orlt, Clara Paglialonga, Lars Porth. Masking in Fine-Grained Leakage Models: Construction, Implementation and Verification. IACR Trans. Cryptogr. Hardw. Embed. Syst., Vol. 2021, Num. 2, pages 189–228, 2021.

8. Ranjit Jhala, *Niki Vazou*. Refinement Types: A Tutorial. Found. Trends Program. Lang., Vol. 6, Num. 3-4, pages 159–317, 2021.

9. Arianna Blasi, *Alessandra Gorla*, Michael D. Ernst, Mauro Pezzè, Antonio Carzaniga. MeMo: Automatically identifying metamorphic relations in Javadoc comments for test automation. Journal of Systems and Software, Vol. 181, 11 2021.

10. Arianna Blasi, *Nataliia Stulova*, *Alessandra Gorla*, Oscar Nierstrasz. Replicomment: identifying clones in code comments. Journal of Systems and Software, Vol. 182, 12 2021.

11. Gregory Chockler, *Alexey Gotsman*. Multi-Shot Distributed Transaction Commit. Distributed Computing, Vol. 34, Num. 4, pages 301–318, Springer, 2021.

12. Hagit Attiya, Sebastian Burckhardt, *Alexey Gotsman*, Adam Morrison, Hongseok Yang, Marek Zawirski. Specification and Space Complexity of Collaborative Text Editing. Theoretical Computer Science, Vol. 855, pages 141–160, Elsevier, 2021.

13. Somayeh Dolatnezhad Samarin, *Dario Fiore*, Daniele Venturi, Morteza Amini. A compiler for multi-key homomorphic signatures for Turing machines. Theoretical Computer Science, Vol. 889, pages 145–170, 2021.

14. *Miguel Ambrona*, *Dario Fiore*, Claudio Soriente. Controlled Functional Encryption Revisited: Multi-Authority Extensions and Efficient Schemes for Quadratic Functions. Proceedings on Privacy Enhancing Technologies, Vol. 2021, Num. 1, pages 21–42, Sciendo, 2021.

15. *Ignacio Cascudo*, Reto Schnyder. A note on secure multiparty computation via higher residue symbols. Journal of Mathematical Cryptology, Vol. 15, Num. 1, pages 284–297, 2021.

16. Nikita Zyuzin, *Aleksandar Nanevski*. *Contextual Modal Types for Algebraic Effects and Handlers*. PACMPL, Vol. 5, Num. ICFP, pages 1–29, 2021.

17. František Farka, *Aleksandar Nanevski*, *Anindya Banerjee*, *Germán Andrés Delbianco*, *Ignacio Fábregas*. On Algebraic

Abstractions for Concurrent Separation Logics. PACMPL, Vol. 5, Num. POPL, pages 1–32, 2021.

18. *Pierre Ganty*, *Elena Gutiérrez*, *Pedro Valero*. A Congruence-Based Perspective on Finite Tree Automata. Fundam. Informaticae, Vol. 184, Num. 1, pages 1–47, 2021.

19. *Felipe Gorostiaga*, *César Sánchez*. Stream runtime verification of real-time event streams with the Striver language. International Journal on Software Tools for Technology Transfer, Vol. 23, Num. 2, pages 157–183, 2021.

20. Sandro Stucki, *César Sánchez*, Gerardo Schneider, Borzoo Bonarkdarpour. Gray-Box Monitoring of Hyperproperties with an Application to Privacy. Formal Methods in Systems Desing, Vol. 58, Num. 1-2, pages 126–159, 2021.

21. Alfonso Ortega, Julian Fiérrez, Aythami Morales, *Zilong Wang*, Marina de la Cruz, César Luis Alonso, Tony Ribeiro. Symbolic AI for XAI: Evaluating LFIT Inductive Programming for Explaining Biases in Machine Learning. Computers, Vol. 10, Num. 11, Multidisciplinary Digital Publishing Institute, 2021.

22. Irfan Ul Haq, *Juan Caballero*. A Survey of Binary Code Similarity. ACM Comput. Surv., Vol. 54, Num. 3, pages 1–51, 2021.

23. *John P. Gallagher*, Martin Sulzmann. Preface, Special Issue on FLOPS 2018. Science of Computer Programming, Vol. 202, 2021.

24. Olivier Blazy, Laura Brouilhet, Céline Chevalier, Patrick Towa, *Ida Tucker*, Damien Vergnaud. Hardware security without secure hardware: How to decrypt with a password and a server. Theoretical Computer Science, Vol. 895, pages 178–211, 2021.

Conferences

1. *Matteo Campanelli*, *Antonio Faonio*, *Dario Fiore*, *Anaïs Querol*, Hadrián Rodriguez. Lunar: a Toolbox for More Efficient Universal and Updatable zkSNARKs and Commit-and-Prove Extensions. ASIACRYPT 2021: 27th Annual International Conference on the Theory and Applications of Cryptology and Information Security, Lecture Notes in Computer Science, Vol. 13092, pages 3–33, Springer, December 2021.

2. Lukas Aumayr, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostáková, Matteo Maffei, *Pedro Moreno-Sanchez*, Siavash Riahi. Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures. ASIACRYPT 2021: 27th Annual International Conference on the Theory and Applications of Cryptology and Information Security, LNCS, Vol. 13091, pages 635–664, Springer, December 2021.

3. Lukas Aumayr, *Pedro Moreno-Sanchez*, Aniket Kate, Matteo Maffei. Blitz: Secure Multi-Hop Payments Without Two-Phase Commits. 30th USENIX Security Symposium, pages 4043–4060, USENIX Association, August 2021.

4. Nico Lehmann, Rose Kunkel, Jordan Brown, Jean Yang, *Niki Vazou*, Nadia Polikarpova, Deian Stefan, Ranjit Jhala. STORM: Refinement Types for Secure Web Applications. 15th USENIX Symposium on Operating Systems Design and Implementation (OSDI 21), pages 441–459, USENIX Association, July 2021.

5. Eduardo Blázquez, Sergio Pastrana, Álvaro Feal, Julien Gamba, *Platon Kotzias*, Narseo Vallina-Rodriguez, Juan Tapiador. Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem. 42nd IEEE Symposium on Security and Privacy, SP 2021, pages 1606–1622, IEEE, May 2021.

6. Lukas Aumayr, Matteo Maffei, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Siavash Riahi, Kristina Hostáková, *Pedro Moreno-Sanchez*. Bitcoin-Compatible Virtual Channels. Proceedings of the 42nd IEEE Symposium on Security and Privacy, pages 901–918, IEEE, May 2021.

7. Erkan Tairi, *Pedro Moreno-Sanchez*, Matteo Maffei. A2L: Anonymous Atomic Locks for Scalability and Interoperability in Payment Channel Hubs. Proceedings of the 42nd IEEE Symposium on Security and Privacy, pages 1834–1851, IEEE, May 2021.

8. *Platon Kotzias*, *Juan Caballero*, Leyla Bilge. How Did That Get In My Phone? Unwanted App Distribution on Android Devices. Proceedings of the 42nd IEEE Symposium on Security and Privacy, pages 53–69, IEEE, May 2021.

9. *Marco Guarnieri*, *Boris Köpf*, Jan Reineke, Pepe Vila. Hardware-Software Contracts for Secure Speculation. Proceedings of the 42nd IEEE Symposium on Security and Privacy, S&P 2021, IEEE, 2021.

10. Marco Patrignani, *Marco Guarnieri*. Exorcising Spectres with Secure Compilers. Proceedings of the 28th ACM Conference on Computer and Communications Security, CCS 2021, pages 445–461, ACM, 2021.

11. Enrico Bacis, Dario Facchinetti, *Marco Guarnieri*, Marco Rosa, Matthew Rossi, Stefano Paraboschi. I Told You Tomorrow: Practical Time-Locked Secrets Using Smart Contracts. Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES 2021, ACM, 2021.

12. *Marco Guarnieri*, *Boris Köpf*, Jan Reineke, Pepe Vila. Hardware-Software Contracts for Secure Speculation. 42nd IEEE Symposium on Security and Privacy, SP 2021, pages 1868–1883, IEEE, 2021.

13. *Gilles Barthe*, Benjamin Grégoire, *Vincent Laporte*, Swarn Priya. Structured Leakage and Applications to Cryptographic Constant-Time and Cost. CCS '21: 2021 ACM SIGSAC Confer-

ence on Computer and Communications Security, pages 462–476, ACM, 2021.

14. Manuel Barbosa, *Gilles Barthe*, Benjamin Grégoire, Adrien Koutsos, *Pierre-Yves Strub*. Mechanized Proofs of Adversarial Complexity and Application to Universal Composability. CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, pages 2541–2563, ACM, 2021.

15. Manuel Barbosa, *Gilles Barthe*, Xiong Fan, Benjamin Grégoire, Shih-Han Hung, Jonathan Katz, *Pierre-Yves Strub*, Xiaodi Wu, Li Zhou. EasyPQC: Verifying Post-Quantum Cryptography. CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, pages 2564–2586, ACM, 2021.

16. *Gilles Barthe*, Sandrine Blazy, Rémi Hutin, David Pichardie. Secure Compilation of Constant-Resource Programs. 34th IEEE Computer Security Foundations Symposium, CSF 2021, pages 1–12, IEEE, 2021.

17. Li Zhou, *Gilles Barthe*, Justin Hsu, Mingsheng Ying, Nengkun Yu. A Quantum Interpretation of Bunched Logic & Quantum Separation Logic. 36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, pages 1–14, IEEE, 2021.

18. Manuel Barbosa, *Gilles Barthe*, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, Bryan Parno. SoK: Computer-Aided Cryptography. 42nd IEEE Symposium on Security and Privacy, SP 2021, pages 777–795, IEEE, 2021.

19. *Gilles Barthe*, Sunjay Cauligi, Benjamin Grégoire, Adrien Koutsos, Kevin Liao, Tiago Oliveira, Swarn Priya, Tamara Rezk, Peter Schwabe. High-Assurance Cryptography in the Spectre Era. 42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021, pages 1884–1901, IEEE, 2021.

20. Man-Kit Sit, *Manuel Bravo*, *Zsolt István*. An experimental framework for improving the performance of BFT consensus for future permissioned blockchains. DEBS '21: The 15th ACM International Conference on Distributed and Event-based Systems, pages 55–65, ACM, 2021.

21. *Manuel Bravo*, *Alexey Gotsman*, Borja de Régil, Hengfeng Wei. *UniStore: A fault-tolerant marriage of causal and strong consistency*. USENIX ATC'21: USENIX Annual Technical Conference, pages 923–937, USENIX, 2021.

22. Vitor Enes, Carlos Baquero, *Alexey Gotsman*, Pierre Sutra. Efficient replication via timestamp stability. EuroSys'21: European Conference on Computer Systems, pages 178–193, ACM, 2021.

23. Alexandre Bois, *Ignacio Cascudo*, *Dario Fiore*, Dongwoo Kim. Flexible and Efficient Verifiable Computation on Encrypted Data. Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and

Theory of Public-Key Cryptography, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 12711, pages 528–558, Springer, 2021.

24. Daniel Benarroch, *Matteo Campanelli*, *Dario Fiore*, Kobi Gurkan, Dimitris Kolonelos. Zero-Knowledge Proofs for et Membership: Efficient, Succinct, Modular. Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I, Lecture Notes in Computer Science, Springer, 2021.

25. Ismaël Jecker, *Nicolas Mazzocchi*, Petra Wolf. Decomposing Permutation Automata. 32nd International Conference on Concurrency Theory (CONCUR 2021), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 203, pages 1–19, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

26. Erkan Tairi, *Pedro Moreno-Sanchez*, Matteo Maffei. Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments. Proceedings of the 25th International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 12675, pages 131–150, Springer, 2021.

27. Matteo Romiti, Friedhelm Victor, *Pedro Moreno-Sanchez*, Peter Sebastian Nordholt, Bernhard Haslhofer, Matteo Maffei. Cross-Layer Deanonymization Methods in the Lightning Protocol. 25th International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 12674, pages 187–204, Springer, 2021.

28. Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Elefterios Kokoris-Kogias, *Pedro Moreno-Sanchez*, Aggelos Kiayias, William Knottenbelt. SoK: Communication Across Distributed Ledgers. 25th International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 12675, pages 3–36, Springer, 2021.

29. Kyveli Doveri, *Pierre Ganty*, Francesco Parolini, Francesco Ranzato. Inclusion Testing of Büchi Automata Based on Well-Quasiorders. 32nd International Conference on Concurrency Theory (CONCUR 2021), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 203, pages 1–22, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

30. Ignacio Casso, *José F. Morales*, *Pedro López-García*, *Manuel V. Hermenegildo*. *Testing Your (Static Analysis) Truths*. Logic-Based Program Synthesis and Transformation - 30th International Symposium, Post-Proceedings, Lecture Notes in Computer Science, Vol. 12561, pages 271–292, Springer, 2021.

31. Ashley Fraser, *Lydia Garms*, Anja Lehmann. Selectively Linkable Group Signatures - Stronger Security and Preserved Verifiability. Cryptology and Network Security - 20th International Conference, CANS 2021, Lecture

Notes in Computer Science, Vol. 13099, pages 200–221, Springer, 2021.

32. *Felipe Gorostiaga*, *César Sánchez*. Nested Monitors: Monitors as Expressions to Build Monitors. Proc. of the 21st Int'l Conference on Runtime Verification (RV'21), LNCS, Vol. 12974, pages 164–183, Springer, 2021.

33. *César Sánchez*. Synchronous and asynchronous stream runtime verification. Proc. of the 5th ACM Int'l Workshop on Verification and mOnitoring at Runtime EXecution (VORTEX'21), pages 5–7, ACM, 2021.

34. Jan Baumeister, Norine Coenen, Borzoo Bonakdarpour, Bernd Finkbeiner, *César Sánchez*. A Temporal Logic for Asynchronous Hyperproperties. Proc. of the 33rd Int'l Conf. on Computer Aided Verification (CAV'21), Part I, LNCS, Vol. 12759, pages 694–717, Springer, 2021.

35. *Felipe Gorostiaga*, *César Sánchez*. HStriver: A Very Functional Extensible Tool for the Runtime Verification of Real-Time Event Streams. Proc. of the 24th Int'l Symp. on Formal Methods (FM'21), LNCS, Vol. 13047, pages 563–580, Springer, 2021.

36. Sebastián Zudaire, *Felipe Gorostiaga*, *César Sánchez*, Gerardo Schneider, Sebastián Uchitel. Assumption Monitoring Using Runtime Verification for UAV Temporal Task Plan Executions. Proc. of the IEEE Int'l Conf. on Robotics and Automation, (ICRA'21), pages 6824–6830, IEEE, 2021.

37. Laura Bozzelli, Adriano Peron, *César Sánchez*. Asynchronous Extensions of HyperLTL. Proc. of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'21), pages 1–13, IEEE, 2021.

38. *Felipe Gorostiaga*, *César Sánchez*. HLola: a Very Functional Tool for Extensible Stream Runtime Verification. Proc. of the 27th Int'l Conf on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'21). Part II, LNCS, Vol. 12652, pages 349–356, Springer, 2021.

39. Tzu-Han Hsu, *César Sánchez*, Borzoo Bonakdarpour. Bounded Model Checking for Hyperproperties. Proc. of the 27th Int'l Conf on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'21). Part I, LNCS, Vol. 12651, pages 94–112, Springer, 2021.

40. Daniel Wilms, Carsten Stöcker, *Juan Caballero*. Data Provenance in Vehicle Data Chains. 93rd IEEE Vehicular Technology Conference, VTC Spring 2021, pages 1–5, IEEE, 2021.

Workshops

1. Bishoksan Kafle, *John P. Gallagher*, *Manuel V. Hermenegildo*, Maximiliano Klemen, *Pedro Lopez-Garcia*, *José F. Morales*. Regular Path Clauses and their Application in Solving Loops. roceedings of the Eighth International Workshop on Horn Clauses for Verification and Synthesis (HCVS 2021), Electronic Proceedings in Theoretical

Computer Science (EPTCS), Vol. 344, pages 22–35, Open Publishing Association (OPA), August 2021. Co-located with ETAPS 2021.

2. M. A. Sanchez-Ordaz, *I. Garcia-Contreras*, V. Perez-Carrasco, *J. F. Morales*, *P. Lopez-Garcia*, *M. Hermenegildo*. VeriFly: On-the-fly Assertion Checking with CiaoPP. 6th Workshop on Formal Integrated Development Environment (F-IDE 2021), Electronic Proceedings in Theoretical Computer Science (EPTCS), pages 1–5, Open Publishing Association (OPA), May 2021. Co-located with ETAPS 2021.

3. Juan Francisco García, Daniel Jurjo, *Fernando Macías*, *José Francisco Morales*, *Alessandra Gorla*. *An application of KLEE to aerospace industrial software*. 2nd International KLEE Workshop on Symbolic Execution, 2021.

4. *Joaquín Arias*, Gopal Gupta, *Manuel Carro*. A Short Tutorial on s(CASP), a Goal-directed Execution of Constraint Answer Set Programs. Proceedings of the 37th ICLP 2021 Workshops, Vol. 2970, CEUR-WS.org, 2021.

Doctoral, Master and Bachelor Theses

1. Alejandro Aguirre Galindo. *Relational logics for higher-order effectful programs*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). February 2021. Advisor: Gilles Barthe (IMDEA Software Institute).

2. Maximiliano Klemen. *A General Framework for Static Resource Analysis and Profiling of (Parallel) Programs and an Application to Runtime Checking*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). March 2021. Advisor: Pedro Lopez-Garcia (IMDEA Software Institute and Spanish Council for Scientific Research).

3. Isabel García Contreras. *A Scalable Static Analysis Framework for Reliable Program Development Exploiting Incrementality and Modularity*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2021. Advisors: Manuel Hermenegildo (IMDEA Software Institute and Technical University of Madrid) and Jose Francisco Morales (IMDEA Software Institute).

4. Jakob Abfalter. *Adaptor Signature Based Atomic Swaps Between Bitcoin and a Mimblewimble Based Cryptocurrency*. Master Thesis. Technical University of Vienna. July 2021. Advisors: Pedro Moreno-Sanchez (IMDEA Software Institute) and Matteo Maffei (T.U. of Vienna).

5. Ignacio Casso. *An Integrated Approach to Assertion-Based Random Testing in Logic Languages*. Master Thesis. Universidad Politécnica de Madrid. July 2021. Advisors: Manuel Hermenegildo, Jose Francisco Morales and Pedro Lopez-Garcia (IMDEA Software Institute).

6. Víctor Pérez Carrasco. *Improvements to Parametric Cost Analysis and its Application to Smart Contracts*. Master Thesis. Universidad Politécnica de

Madrid. July 2021. Advisors: Manuel Hermenegildo, Jose Francisco Morales and Pedro Lopez-Garcia (IMDEA Software Institute).

7. Andoni Rodriguez. *The Temporal Booleanization Theorem: realizability checking over numerical-LTL industrial requirements*. Master Thesis. Universidad Complutense de Madrid. September 2021. Advisor: Cesar Sanchez (IMDEA Software Institute).

8. Marta Centellas Nadal. *Analysis of Proof of Assets for Different Cryptocurrencies*. Master Thesis. Universidad Complutense Madrid. October 2021. Advisors: Ignacio Cascudo and Pedro Moreno-Sanchez (IMDEA Software Institute).

9. Andrea Colato. *Hadesius: Una soluzione per il controllo e il monitoraggio del perimetro cibernetico nazionale*. Master Thesis. Universita degli Studi di Milano. October 2021. Advisors: Stelvio Cimato (U. degli Studi di Milano) and Dario Fiore (IMDEA Software Institute).

10. Meresa Gebrewahd. *Empirical Analysis of Trace-ability in the Lightning Network*. Master Thesis. Sapienza University of Rome. October 2021. Advisors: Pedro Moreno-Sanchez (IMDEA Software Institute) and Angelo Spognardi.

11. Alejandro de la Cruz Alvarado. *A Platform for Automating the Preparation of iOS Apps for Binary Analysis*. Bachelor Thesis. Universidad Carlos III de Madrid. June 2021. Advisor: Juan Caballero (IMDEA Software Institute).

Invited Talks

Invited and plenary Talks by IMDEA Scientists

1. *Alexey Gotsman*. Rigorous Design of Atomic Transaction Commit Protocols. IFIP Workshop on Trends in Concurrency Theory. online. August 2021.

2. *Cesar Sanchez*. Synchronous and Asynchronous Stream Runtime Verification. ACM International Workshop on Verification and mOnitoring at Runtime EXecution (VORTEX). Aarhus University. July 2021.

3. *Dario Fiore*. A journey in vector commitments. International Workshop on Security (IWSEC). online. September 2021.

4. *Pedro Moreno-Sanchez*. Security and Privacy of Payment Channels and Applications. Crypto Valley Conference (CVC). online. 2021.

5. *Pedro Moreno-Sanchez*. Layer 2 Swaps. Advances of Financial Technologies (AFT). 2021.

6. *Pedro Moreno-Sanchez*. Blitz: Secure Multi-Hop Payments Without Two-Phase-Commits. Protocol Research Labs. 2021.

7. *Pedro Moreno-Sanchez*. Security, Privacy and Scalability for Blockchains. Cryptography Research Centre, Abu Dhabi. 2021.

8. *Thaleia Dimitra Doudali*. Adding Machine Learning to the Management of Heterogeneous Resources. Workshop on Distributed Cloud Computing (DCC). online. June 2021.

9. *Dimitrios Stylianos Kolonelos*. Zero-Knowledge Proofs for Set Membership Efficient Succinct Modular. Financial Cryptography and Data Security (FC). online. March 2021.

10. *Emanuele Giunta*. On Interactive Oracle Proofs for Boolean R1CS Statements. Annual conference on Cryptography and Coding Theory. July 2021.

11. *Felipe Gorostiaga*. HStriver: a Very Functional Extensible Tool for the Runtime Verification of Real-Time Event Streams. Formal Methods. online. November 2021.

12. *Felipe Gorostiaga*. HLola: a Very Functional Tool for Extensible Stream Runtime Verification. International Conference on Tools and Algorithms for the Construction and Analysis of Systems. online. April 2021.

13. *Silvia Sebastián*. Extended Abstract – AVCLASS2: Massive Malware Tag Extraction from AV Labels. Jornadas Nacionales de Investigación en Ciberseguridad (JNIC). online. June 2021.

Invited Seminars and Lectures by IMDEA Scientists

1. *Cesar Sanchez*. Stream Runtime Verification Revisited. Seminar. Austria Institute of Sciente and Technology. March 2021.

2. *Dario Fiore*. Cryptography for Privacy and Integrity of Computation on Untrusted Machines. Summer seminars on cybersecurity. Department of Computer, Control and Management Engineering of Sapienza University of Rome. June 2021.

3. *Ignacio Cascudo*. Códigos correctores de errores en computación segura. Seminario de Álgebra, Geometría algebraica y Singularidades. Universidad de La Laguna, Tenerife. July 2021.

4. *Ignacio Cascudo*. Cryptographic Primitives for Randomness Generation and Privacy. Meeting with Nomadic Labs. July 2021.

5. *Marco Guarnieri*. Hardware-software security contracts: Principled foundations for building secure microarchitectures. Seminar. Universidad Complutense de Madrid. December 2021.

6. *Marco Guarnieri*. Contract-aware secure compilation: a foundation for side-channel resistant compilers - challenges and open questions. Seminar. Schloss Dagstuhl, Germany. December 2021.

7. *Marco Guarnieri*. Database security: Formalization, verification, and testing – Challenges and open questions. Seminar. Schloss Dagstuhl, Germany. November 2021.

8. *Marco Guarnieri*. Hardware/Software Security Contracts - Principled Foundations for Building Secure Speculation Mechanisms. Intel Side-channel Academic Program Workshop. November 2021.

9. *Marco Guarnieri*. HascoSec: Principled security verification of processors using hardware-software contracts. Intel Kickoff: Scalable Assurance Cluster. October 2021.

10. *Marco Guarnieri*. Hardware-Software Contracts for Secure Speculation. Hardware Security reading group . University of Illinois at Urbana Champaign. June 2021.

11. *Marco Guarnieri*. Hardware-Software Contracts for Secure Speculation. IEEE Symposium on Security and Privacy (S&P). May 2021.

12. *Marco Guarnieri*. Contract-aware secure compilation (short talk). Workshop on Principles of Secure Compilation (PriSC). January 2021.

13. *Thaleia Dimitra Doudali*. Building smart and fast systems using Machine

Learning and Computer Vision. Graduate Conference. Universidad Complutense de Madrid. November 2021.

14. *Dimitrios Stylianos Kolonelos*. Zero-Knowledge Proofs for Set Membership Efficient Succinct Modular. Monash Cybersecurity Seminars. online. February 2021.

15. *Emanuele Giunta*. Efficient and Universally Composable Single Secret Leader Election from Pairings. Protocol Research Labs. August 2021.

16. *Felipe Gorostiaga*. Introducción a Stream Runtime Verification. Laboratorio de Fundamentos y Herramientas para la Ingeniería de Software (LaFHIS). Universidad de Buenos Aires, Argentina. August 2021.

Invited Speaker Series

During 2021, 21 external speakers were invited to give talks at IMDEA Software. Due to the pandemic, all the seminars have been given in a hybrid mode with both in-person attendance and a live streaming open to the public. All the seminars and talks in our building are open to the campus and the academic community at large. The following list shows the speakers and the titles of their talks.

1. *Sandro Stucky*. Post-doctoral Researcher, University of Gothenburg, Sweden: Gray-Box Monitorability of Hyperproperties.

2. *Gerardo Schneider*. Research Professor, University of Gothenburg, Sweden: Monitor-Triggered Temporal Logic.

3. *Diego Garbervetsky*. Associate Professor, Universidad de Buenos Aires and CONICET, Argentina: Using abstractions to validate and test programs with rich protocols.

4. *Louis-Marie Dando*. Post-doctoral Researcher, ANR Delta, LIS, Marseille, France: Weighted Automata and Expressions over Pre-Rational Monoids.

5. *Chana Weil-Kennedy*. PhD candidate, TU Munich, Germany: Verification of Immediate Observation Petri Nets.

6. *Damien Robissout*. PhD Student, Laboratoire Hubert Curien, University of Lyon, France: Online Performance Evaluation and Improvement of Deep Learning Networks for Side-Channel Analysis.

7. *Nikos Vasilakis*. Researcher, MIT CSAIL, USA: Retrofitting Security, Module by Module.

8. *Andres Sanchez*. Master Intern, EPFL, Switzerland: Leaking Secrets Through Compressed Caches.

9. *Miguel Ambrona*. Post-doctoral Researcher, NTT Secure Platform Laboratories, Japan: Acyclicity Programming for Sigma-Protocols.

10. *Thaleia-Dimitra Doudali*. PhD candidate, Georgia Institute of Technology,

USA: Adding Machine Learning to the Management of Heterogeneous Resources.

11. *Matteo Dell'Amico*. Researcher, EURECOM, France: Approaches to Explore Complex Data.

12. *Danilo Francati*. PhD candidate, Stevens Institute of Technology, Hoboken, USA: Kolmogorov complexity and cryptography: New connections and applications to space-demanding functions.

13. *Duc Le*. PhD candidate, Purdue University, USA: Cryptographic Constructions for Resource-Constrained Devices with Applications to Blockchains.

14. *Vanessa Frias-Martinez*. Associate Professor, University of Maryland, USA: Data-driven decision making for cities and communities.

15. *Tianhao Wang*. PhD candidate, Purdue University, USA: Collecting Sensitive Data with Local Differential Privacy.

16. *Lana Josipovic*. Doctoral Assistant, EPFL, Switzerland: High-Level Synthesis of Dynamically Scheduled Circuits.

17. *Nik Sultana*. Post-doctoral Researcher, University of Pennsylvania, USA: Programming for Distributed and Heterogeneous Resources.

18. *Manuel Rigger*. Post-doctoral Researcher, ETH Zürich, Switzerland: Robustifying Data-Centric Systems.

19. *Marios Kogias*. Researcher, Microsoft Research, Cambridge, United Kingdom: Building Latency-Critical Datacenter Systems.

20. *Christian Schilling*. Interim Professor, University of Konstanz, Germany: Outside the Box: Scalable Formal Methods.

21. *Rahul Gopinath*. Post-doctoral Researcher, CISPA Helmholtz Center for Information Security, Germany: The Science of Fuzzing.

Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **15** seminars were given in 2021.

Scientific Service and Other Activities

Conference and Program Committee Chairmanship

Marco Guarnieri

1. Program co-chair of Workshop on Principles of Secure Compilation (PriSC) 2022.
2. Program co-chair of Workshop on Programming Languages and Security (PLAS) 2021.

Niki Vazou

3. Program co-chair of Programming Language Design and Implementation - Artifact Evaluation Commitee (PLDI) 2021.

Pedro Moreno-Sanchez

4. Program co-chair of IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) 2021.
5. Program co-chair of IEEE Workshop on Security & Privacy on the Blockchain (IEEE S&B) 2021.

Pierre Ganty

6. Program co-chair of International Symposium on Games, Automata, Logics, and Formal Verification (GandALF) 2021.

Editorial Boards and Conference Steering Committees

Dario Fiore

1. Editor of International Journal of Applied Cryptography 2021.

Gilles Barthe

2. Editor of ACM Transactions on Privacy and Security 2021.
3. Editor of Journal of Computer Security 2021.
4. Editor of Journal of Automated Reasoning 2021.

John Gallagher

5. Steering Committee of International Symposium on Functional and Logic Programming (FLOPS) 2021.
6. Steering Committee of International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR) 2021.

Manuel Hermenegildo

7. Steering Committee of Conference on Compiler Construction (CC) 2021.
8. Steering Committee of International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR) 2021.
9. Steering Committee of ACM SIGPLAN Workshop/Symposium on Partial Evaluation and Program Manipulation (PEMP) 2021.

10. Steering Committee of International Symposium on Functional and Logic Programming (FLOPS) 2021.
11. Editorial Advisor of Theory and Practice of Logic Programming 2021.
12. Area editor of Algorithms in Programming Languages and Software Engineering, of the Logic Journal of the IGPL 2021.
13. Area editor of Logic and Constraint Logic Programming, of the Journal of Applied Logics 2021.

Marco Guarnieri

14. Review Editor of Frontiers in Compute Science/Frontier in ICT (Frontier) 2021.
15. Steering committee member of Workshop on Programming Languages and Security (PLAS) 2021.
16. Steering committee member of Workshop on Principles of Secure Compilation (PriSC) 2021.

Niki Vazou

17. Steering committee member of Haskell Symposium 2021.

Pedro Lopez

18. Steering committee member of International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR) 2021.

Pedro Moreno-Sanchez

19. Editorial board member of Privacy Enhacing Technologies Symposium Journal (PoPETS) 2021.

Manuel Carro

20. Area editor of Theory and Practice of Logic Programming 2021.

Participation in Program Committees

Alexey Gotsman

1. PC of Symposium on Principles of Distributed Computing (PODC) 2021.
2. PC of International Conference on Concurrency Theory (CONCUR) 2021.
3. PC of International Conference on Principles of Distributed Systems (OPODIS) 2021.

Cesar Sanchez

4. PC of International Workshop on Formal Methods for Blockchains (FMBC) 2021.
5. PC of IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) 2021.
6. PC of International Conference on Runtime Verification (RV) 2021.
7. PC of International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI) 2021.
8. PC of International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2021.
9. PC of Jornadas de Programación y Lenguajes (PROLE) 2021.

Dario Fiore

10. PC of Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) 2021.
11. PC of Financial Cryptography and Data Security (FC) 2021.

Ignacio Cascudo

12. PC of Conference on Information-Theoretic Cryptography (ITC) 2021.

13. PC of International Conference on Applied Cryptography and Network Security (ACNS) 2021.

John Gallagher

14. PC of Ninth International Workshop on Verification and Program Transformation (VPT) 2021.

Manuel Hermenegildo

15. PC of International Conference on Logic Programming (ICLP) 2021.

Marco Guarnieri

16. PC of IEEE Symposium on Security and Privacy (S&P) 2022.
17. PC of ACM Conference on Computer and Communications Security (CCS) 2021.
18. PC of IEEE Computer Security Foundations Symposium (CSF) 2022.
19. PC of Workshop on Principles of Secure Compilation (PriSC) 2021.
20. PC of IEEE European Symposium on Security and Privacy (EuroS&P) 2021.
21. PC of IEEE European Symposium on Security and Privacy (EuroS&P) 2022.

Niki Vazou

22. PC of ACM Symposium on Principles of Programming Languages (POPL) 2022.
23. PC of Workshop on the Implementation of Type Systems (WITS) 2022.
24. PC of International Conference on Types for Proofs and Programs (TYPES) 2022.
25. PC of ACM SIGPLAN conference on Object-oriented programming systems and applications (OOPSLA) 2022.
26. PC of International Symposium on Functional and Logic Programming (FLOPS) 2022.
27. PC of International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI) 2021.
28. PC of Panhellenic Logic Symposium (PLS) 2021.
29. PC of ACM SIGPLAN Workshop/Symposium on Partial Evaluation and Program Manipulation (PEMP) 2021.

Pedro Lopez

30. PC of International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR) 2021.

Pedro Moreno-Sanchez

31. PC of Financial Cryptography and Data Security (FC) 2021.
32. PC of Network and Distributed System Security Symposium (NDSS) 2021.
33. PC of Conference on Communication and Computer Security (CCS) 2021.
34. PC of Cryptocurrency and Blockchain Technologies Workshop (CBT) 2021.
35. PC of Decentralized Finance Workshop (DeFi) 2021.
36. PC of Theory and Practice of Blockchains Workshop (TPBC) 2021.

Pierre Ganty

37. PC of International Symposium on Automated Technology for Verification and Analysis (ATVA) 2021.
38. PC of International Conference on Networked Systems (NETYS) 2021.
39. PC of International Conference on Computer-Aided Verification (CAV) 2021.
40. PC of Symposium on Principles of Programming Languages (POPL) 2021.

Srdjan Matic

41. PC of Passive and Active Measurement (PAM) 2022.

Fernando Macías

42. PC of International Workshop on Multi-Level Modelling (MULTI) 2021.

Lydia Garms

43. PC of The Cryptographer's Track at the RSA Conference 2021 (CT-RSA) 2021.

Daniel Domínguez Álvarez

44. Proceedings Chair of IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft) 2021.

Manuel Carro

45. PC of International Conference on Logic Programming (ICLP) 2020.
46. PC of Jornadas de Programacion y Lenguajes (PROLE) 2021.

Association and Organizational Committees

Manuel Hermenegildo

1. President of the Scientific Council at Institut National de Recherche en Informatique et en Automatique, France 2021.
2. Member of the Scientific Advisory Board at Schloss Dagstuhl, Germany 2021.
3. Member of the Executive Committee of the ACM Europe Technology Policy Committee 2021.
4. Member of the Nomination Committee at Academia Europaea 2021.
5. Member of the External Advisory Board at NOVA LINCS Institute, Portugal 2021.
6. Member of the Scientific Advisory Board at French Institute for Free Software, France 2021.
7. Member of the Board Nomination Committee at Informatics Europe 2021.
8. Secretary of the International Association for Logic Programming 2021.
9. Member of the International Federation for Computational Logic Advisory Board (IFCoLog) 2021.
10. Member of the Consulting Council at Universidad Politécnica de Madrid, Spain 2021.
11. Member of the Gallery of Distinguished Professors at Universidad Politécnica de Madrid, Spain 2021.

Manuel Carro

12. Member of the Advisory Board at Digitaliza Madrid 2021.
13. Member of the Advisory Board at Madrid Research Programme (PRICIT) 2021.
14. Representative of the IMDEA SOFTWARE Institute at Informatics Europe 2021.
15. Member of the Board of Directors at Informatics Europe 2021.
16. Member of the Joint Board at Erasmus Mundos European Master in Software Engineering 2021.
17. Representative of the IMDEA SOFTWARE Institute at Node Strategy Committee of EIT Digital Spain 2021.
18. Representative of the IMDEA SOFTWARE Institute at GA of EIT Digital 2021.

Awards

Paper Awards

1. Alejandro Aguirre, *Gilles Barthe*, Justin Hsu, Benjamin Lucien, Kaminski, Joost-Pieter Katoen, Christoph Matheja. A Pre-Expectation Calculus for Probabilistic Sensitivity. Symposium on Principles of Programming Languages (POPL). January, 2021.
2. Álvaro Feal, *Paolo Calciati*, Narseo Vallina-Rodríguez, Carmela Troncoso, *Alessandra Gorla*. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. Research and Personal Data Protection Emilio Aced Award from the Spanish National Data Protection Agency (AEPD). January, 2021.
3. Marco Guarnieri, Boris Kopf, Jan Reineke, *Pepe Vila*. Hardware-Software Contracts for Secure Speculation. IEEE Symposium on Security and Privacy (S&P). May 2021.

Other Awards

4. Musard Balliu, *Marco Guarnieri*. InferViz: Weighted Inference and Visualization of Insecure Code Paths. Privacy Enhancing Technologies (PETS). Facebook research award. 2021.
5. *Anaïs Querol*, *Silvia Sebastián*. My PhD in a nutshell. UPM symposium. June, 2021.
6. *Pepe Vila*, *Joaquín Arias*. 2019-2020 Outstanding Thesis Award granted by the Polytechnic University of Madrid (UPM). November, 2021.
7. *Dario Fiore*, Aikaterini Mitrokotsa, Luca Nizzardo and Elena Pagnin. 2020 Premium Award for Best Paper in the IET. February, 2021.

Education

While the Institute focuses on research and technology transfer, our researchers are sometimes involved in teaching courses offered by universities and other entities. The following is a list of courses where IMDEA Software researchers taught in 2021.

1. Computer Security (Master level, 4 ECTS). Master in Software and Systems (MUSS) and European Master in Software Engineering (EMSE), Universidad Politécnica de Madrid (UPM). *Juan Caballero*, *Ignacio Cascudo*, *Dario Fiore*, *Alessandra Gorla*, *Marco Guarnieri*.

2. Design and Analysis of Security Protocols (Master level, 6 ECTS). Master in Formal Methods and Computer Science Engineering (MFII), Universidad Autónoma de Madrid (UAM). *Ignacio Cascudo*, *Dario Fiore*, *Pedro Moreno-Sanchez*.

Communication

As any research institution, the IMDEA Software Institute uses different communication strategies and channels to disseminate both general science and technology principles and, in particular, the advances made by the Institute researchers. These serve to raise the scientific and technological awareness of the general public, to showcase how the investment in research reverts in the society at large, and to present the latest discoveries and developments to the relevant stakeholders. This complements scholarly dissemination, that typically takes place via publications in journals and conferences and address peer researchers.

Among the objectives of communication we may cite:

- Disseminating knowledge about science and technology,
- Making society at large aware of the advances obtained through investment in science and technology,
- Fostering the engagement and participation of the society in STEM-related activities,
- Contributing to attracting the best talent through additional visibility of the Institute.

The communication plan of the Institute is shaped as a matrix for all communication actions carried out in the areas of public relations, content marketing, corporate identity, internal communication, dissemination channels, advertising, and corporate social responsibility.

Stay informed of our news:

web

munication

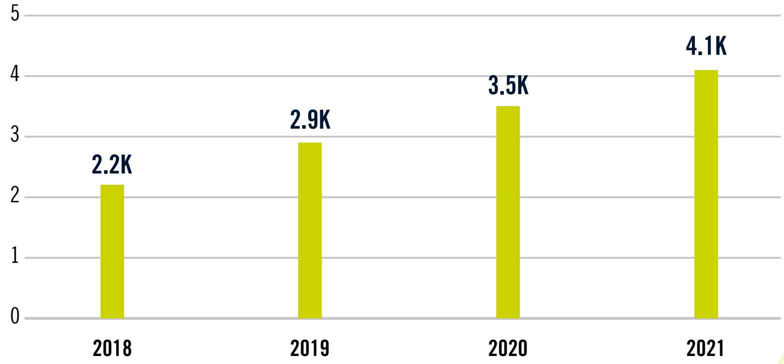
26 web news

8 press releases

102 media impacts

394 social network posts

total community[1]



357K

impressions

286K	18K	6K	41K	7K

4.1K

community

1.367	72	315	1.966	361

[1] Community is defined as the total number of users who follow or are subscribed to the social networks of the IMDEA Software Institute

Dissemination events

During 2021, the IMDEA Software Institute researchers took part in several events (most of them virtual, due to the ongoing pandemic) related to dissemination of science.

European Researchers' Night

What do you do to make the planet better?

September 24, 2021

Eleven researchers from the seven IMDEA Institutes took the stage to show how their research contributes to ensuring a sustainable development and that we all can collaborate, with small and big things, to achieve this goal.

José Manuel Torralba, researcher and director of IMDEA Materials, and Manuel Carro, researcher and director of IMDEA Software, were the masters of ceremonies. They introduced their colleagues Francesco Polazzo (IMDEA Water), María Jesús (Josune) Latasa (IMDEA Food), Héctor Hernando (IMDEA Energy), Mónica Echeverry (IMDEA Materials),Wojciech Gawelda (IMDEA Nanoscience), Borja Genovés, Sarmad Mir, and Javier Talavante (IMDEA Networks), and Pedro Moreno-Sanchez, Marta Centellas, and Juan Manuel Copia (IMDEA Software).

CSIC's *Residencia de estudiantes* + streaming

11 Researchers

200 aprox. (in person + virtual)

Video summary

IMDEA Software Institute

6 Researchers

35

Science and Innovation Week

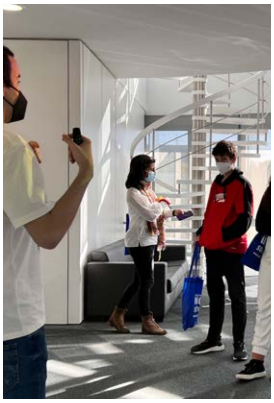
Gymkhana: Software Matters

November 11, 2021

The IMDEA Software Institute took part again in the Science and Innovation Week organised by the Regional Ministry of Science, Universities and Innovation of the Madrid Regional Government, coordinated by the *Fundación para el Conocimiento madrid+d*.

The main objective of the event is to attract students at all levels to STEM careers and introduce young talents to engineering, research, and innovation. Five research assistants from the Institute presented some basic concepts of several areas of Computer Science through a number of challenges to be solved by teams of students, which competed against each other.

institute imdea software
semana de la ciencia y la innovación 2021
Una ciencia para los grandes retos de la humanidad
fundación para el conocimiento madrid
Gymkhana: Software matters
11 NOV 2021
XXI Semana de la Ciencia y la Innovación Madrid



Video summary

High School Visit

IES Gerardo Diego

December 13, 2021

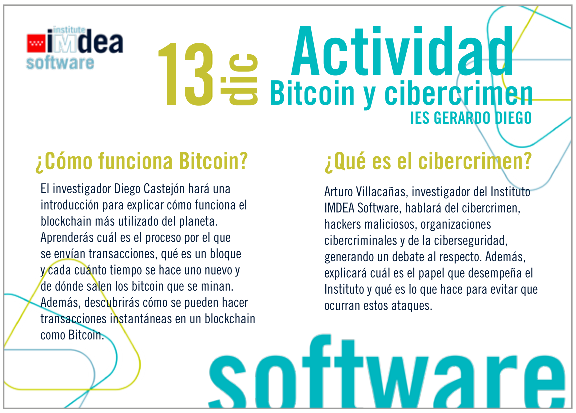
The IMDEA Software Institute hosted a visit of students of the High School Gerardo Diego, from Pozuelo de Alarcón, to the Montegancedo Campus.

Diego Castejón and Arturo Villacañas, research assistants at the IMDEA Software Institute, gave talks to the visitors about cryptocurrencies and cybercrime. Both explained what they had studied and how they got to where they are.

IMDEA Software Institute

2 Researchers

40


institute imdea software

13 dic **Actividad**

Bitcoin y cibercrimen

IES GERARDO DIEGO

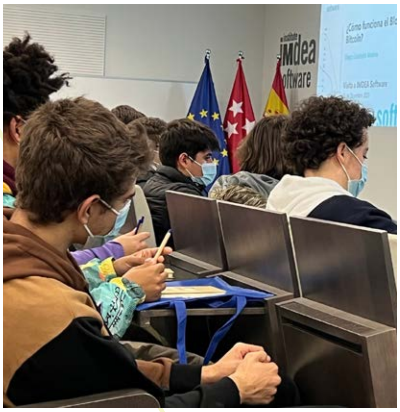
¿Cómo funciona Bitcoin?

El investigador Diego Castejón hará una introducción para explicar cómo funciona el blockchain más utilizado del planeta. Aprenderás cuál es el proceso por el que se envían transacciones, qué es un bloque y cada cuánto tiempo se hace uno nuevo y de dónde salen los bitcoin que se minan. Además, descubrirás cómo se pueden hacer transacciones instantáneas en un blockchain como Bitcoin.

¿Qué es el cibercrimen?

Arturo Villacañas, investigador del Instituto IMDEA Software, hablará del cibercrimen, hackers maliciosos, organizaciones cibercriminales y de la ciberseguridad, generando un debate al respecto. Además, explicará cuál es el papel que desempeña el Instituto y qué es lo que hace para evitar que ocurran estos ataques.

software



of research ensuring that software is safe, reliable and efficient
institute imdea software
science and technology for developing better software
software.imdea.org

Video summary

Research and technology related events

Virtual event

100 aprox. (virtual)

19 Talks

REDIMadrid Workshop

October 20, 2021

Since its creation, REDIMadrid has held an annual thematic workshop where researchers and network users present, share, and compare experiences using the communication network (and especially the technology offered by the Telematic Research Network of the Madrid Regional Government) in their projects, either as research object or as a research tool.

This edition took place online, due to the still present COVID-19. Nonetheless, it was a meeting point where users shared experiences on the use of REDIMadrid, and, in general, on the application of network technologies, as well as proposals for new R&D activities centered on the network and its development and expansion, fulfilling the goals of the workshop.

Video summary

Institutional Events

Visit from the Councilor for University, Research, and Innovation of the Madrid Regional Government

February 19, 2021

The Councilor for University, Research, and Innovation, together and other members of the Madrid Regional Government visited the IMDEA Software Institute. The Director of the Institute presented the strategic lines and the main topics of research performed at IMDEA Software. After this introduction, several researchers of the Institute (Manuel Hermenegildo, Dario Fiore, Ignacio Cascudo, Juan Caballero, Alessandra Gorla, and Alexey Gotsman), gave short talks highlighting the main points of their fields of work.

institute imdea software

Comunidad de Madrid

Visit of the Secretary of State for Digitization and Artificial Intelligence

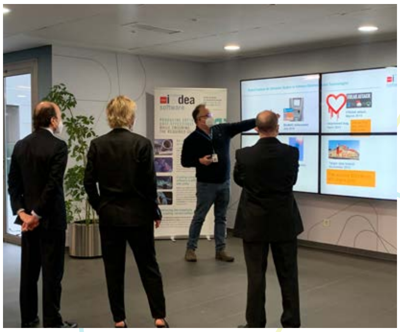
March 2, 2021

The Secretary of State for Digitization and Artificial Intelligence, Carme Artigas, the Councilor for Science, Universities and Innovation, and the Director General for Research and Technological Innovation visited the IMDEA Software Institute.

The director and deputy director of the Institute, together with the former director and Distinguished Professor, Manuel Hermenegildo, received the visitors and took them on a tour of the facilities, which included a presentation of the cutting-edge work performed.

Associate Research Professor Aleks Nanevski gave a brief overview of the Institute and the importance of software research. After this, several researchers (Manuel Hermenegildo, Dario Fiore, Ignacio Cascudo, Juan Caballero, Alessandra Gorla and Alexey Gotsma) presented part of the research being done at the Institute.

Video summary



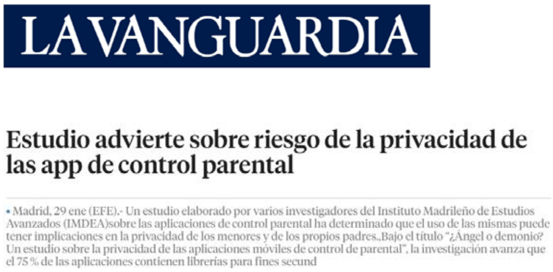
Visit of the Director General of Research and Technological Innovation

April 19, 2021

Following changes in the Regional Government, the new Director General of Research and Technological Innovation, Ms. Ana Isabel Cremades, and the Deputy Director General of Research, Ms. Bárbara Fernández-Revuelta, visited the Institute. As in similar previous occasions, they were shown the Institute and introduced to the research performed by its researchers.

Video summary

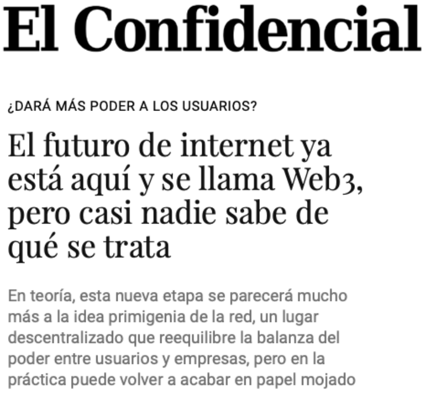
Media impacts



LA VANGUARDIA

Estudio advierte sobre riesgo de la privacidad de las app de control parental

• Madrid, 29 ene (EFE).- Un estudio elaborado por varios investigadores del Instituto Madrileño de Estudios Avanzados (IMDEA)sobre las aplicaciones de control parental ha determinado que el uso de las mismas puede tener implicaciones en la privacidad de los menores y de los propios padres.,Bajo el título "¿Ángel o demonio? Un estudio sobre la privacidad de las aplicaciones móviles de control de parental", la investigación avanza que el 75 % de las aplicaciones contienen librerías para fines secund

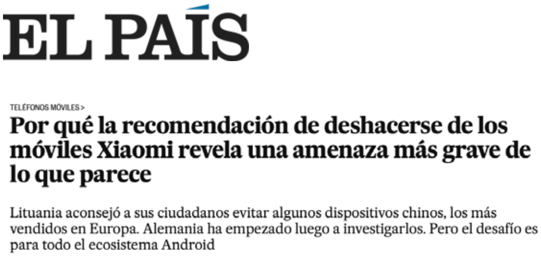


El Confidencial

¿DARÁ MÁS PODER A LOS USUARIOS?

El futuro de internet ya está aquí y se llama Web3, pero casi nadie sabe de qué se trata

En teoría, esta nueva etapa se parecerá mucho más a la idea primigenia de la red, un lugar descentralizado que reequilibre la balanza del poder entre usuarios y empresas, pero en la práctica puede volver a acabar en papel mojado

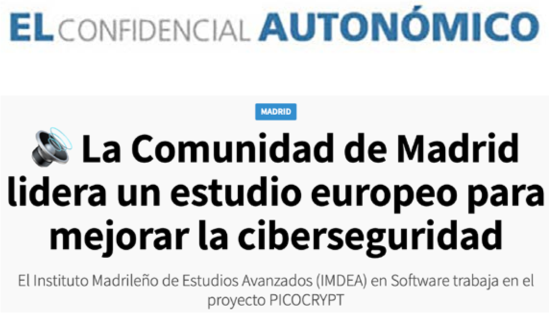


EL PAÍS

TELÉFONOS MÓVILES >

Por qué la recomendación de deshacerse de los móviles Xiaomi revela una amenaza más grave de lo que parece

Lituania aconsejó a sus ciudadanos evitar algunos dispositivos chinos, los más vendidos en Europa. Alemania ha empezado luego a investigarlos. Pero el desafío es para todo el ecosistema Android

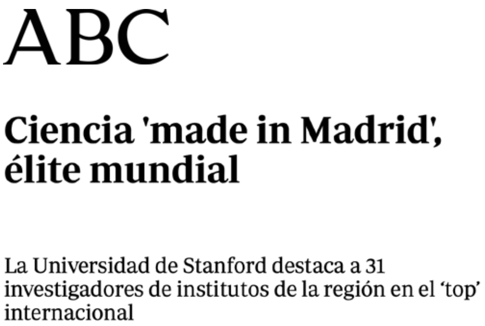


EL CONFIDENCIAL AUTONÓMICO

MADRID

🔉 La Comunidad de Madrid lidera un estudio europeo para mejorar la ciberseguridad

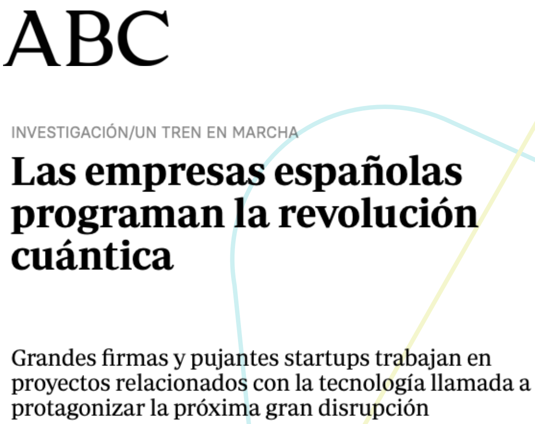
El Instituto Madrileño de Estudios Avanzados (IMDEA) en Software trabaja en el proyecto PICOCRYPT



ABC

Ciencia 'made in Madrid', élite mundial

La Universidad de Stanford destaca a 31 investigadores de institutos de la región en el 'top' internacional



ABC

INVESTIGACIÓN/UN TREN EN MARCHA

Las empresas españolas programan la revolución cuántica

Grandes firmas y pujantes startups trabajan en proyectos relacionados con la tecnología llamada a protagonizar la próxima gran disrupción

Comunidad de Madrid

EUROPEAN UNION
STRUCTURAL FUNDS

annual report 2021

software.imdea.org

software.imdea.org

institute imdea software

Contact
software@imdea.org
tel. +34 91 101 22 02
fax +34 91 101 13 58

Campus de Montegancedo
28223 Pozuelo de Alarcón
Madrid, Spain