institute iMdea software

science and technology for developing better software

annual report 2020

software.imdea.org

software

Manuel Carro
Director, IMDEA Software Institute
April 28, 2021

foreword

It is nearly impossible to write a text referring to the year 2020 without mentioning the COVID-19 pandemia. On 2020, we became fully aware of our fragility, and many families had to mourn the loss of loved ones. But mankind also showed it has the capability to pull amazing feats when facing the need to do so. The superhuman efforts and dedication of health professionals set an example difficult to match. Education at all levels had to adapt in a record time to continue with as little disruption as possible. Workers around the globe switched to a teleworking routine that has arrived to stay, in different degrees for different jobs. As vaccines, developed in a record time, are being administered, we hope that life will return to a "new normality" soon.

It is worthwhile mentioning the role that science, research, and innovation in the computer science / IT domain have played during the pandemia and in the path towards its elimination. As an example, modern vaccine development is partly a computation-based process, as predicting the shape of proteins once folded is key to understanding how the virus attacks and to devising new vaccines. Lockdown measures have caused a spike in the usage of videoconferencing and, in general, software to make remote working possible. Once used rather occasionally, specially in high-tech companies, videoconferencing became in just some months the bread and butter of many activities, from education to music performances. And it is worth mentioning that today's videoconference applications (that can undoubtedly be improved) are the result of tens of years of research in distributed systems, networking, audio and video processing, cryptography, and a myriad of other core computing topics.

The abrupt shift in how business are conducted did not go unnoticed in the research field. Even for disciplines such as computer science which, unlike natural sciences, do not depend on traditional laboratories, the impact cannot be overstated. While computer scientists are among those who could adapt the quickest to the new *status quo*, many aspects of how to perform research effectively had to be adapted — and the adaptation has certainly not finished yet.

Conferences, which are regarded in Computer Science as the primary research venue above most journals in the field, became online events. Some were cancelled, and for those that were not, the reduced interaction with colleagues made them less attractive. Also, videoconference-based relationships with work colleagues, even in the same Institute, cannot fully substitute the spontaneous interaction that takes place in a corridor or in front of a whiteboard. This is especially so in the case of early stage researchers — PhDs or even interns — for whom frequent contact with advisors and peers can bring not only faster learning, but also a feeling of belonging to an institution.

Despite this, the year 2020 has been in some aspects a success for the Institute. A new 2M€ ERC grant was awarded (to cryptography researcher Dario Fiore) and an agreement was made with the Tezos Foundation through the French startup Nomadic Labs to provide funding for research projects on advanced blockchain characteristics. Contracts close to 500K€ were signed in the year 2020, and several other contracts were scheduled to be signed at the beginning of 2021, with a number of others being under evaluation.

The research output of the Institute has also been good, taking into account the difficulties brought about by the pandemia. Sixty papers were published in top conferences and journals and five invited talks in conferences, in addition to 23 invited talks in workshops and scientific meetings, were given by IMDEA Software researchers. Nine PhD, MSc, and BSc thesis advised by Institute researchers were defended during 2020. In addition, several research awards were received by institute researchers: the paper *Multi-Key Homomorphic Authenticators* was given the *2020 Premium Award for Best Paper in the IET*, the then-PhD student Platon Kotzias was awarded the UPM extraordinary 2018-2019 PhD Thesis Prize, and Ida Tucker, who joined the Institute in 2020, was the recipient of the L'Oréal-UNESCO France Rising Talent Award for Women in Science.

Regarding human resources, our researchers and admin staff included, during 2020, 20 faculty members (including two part-time, one visiting faculty member, and one on leave of absence), 14 postdoctoral researchers, four research programmers, 28 research assistants (usually performing their doctoral studies), 32 interns, three project management staff, and 13 support staff members, from 29 different nationalities.

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 web site, **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.

foreword

annual report 2020

software.imdea.org

editor
IMDEA Software Institute

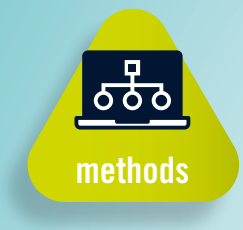
graphic design
loveodesign.es

contents

contents

about us

profile



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 companies such as Protocol Labs and NEC Labs Europe.

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.

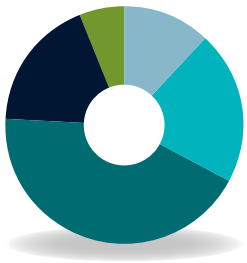
about us

the institute at a glance

2020 in figures

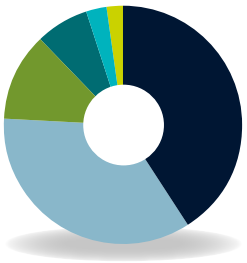
66	32	29	5	16	24
Researchers	Interns	Nationalities	Ph.D. thesis	Active fellowships	Active projects

Researchers



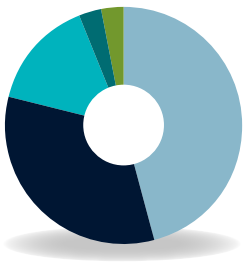
- 18% Senior Faculty
- 43% Research Assistant
- 12% Junior Faculty
- 6% Research Programmer
- 21% Postdocs

Nationalities



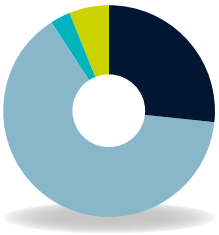
- 41% Spain
- 7% South America
- 35% Europe (ex. Spain)
- 12% Asia
- 3% North America
- 2% Africa

Where Ph.D.was obtained



- 32% Spain
- 3% South America
- 47% Europe (ex. Spain)
- 2% Asia
- 16% North America

Publications



- 17 Journals
- 2 Edited volumes
- 43 Conferences
- 4 Workshops

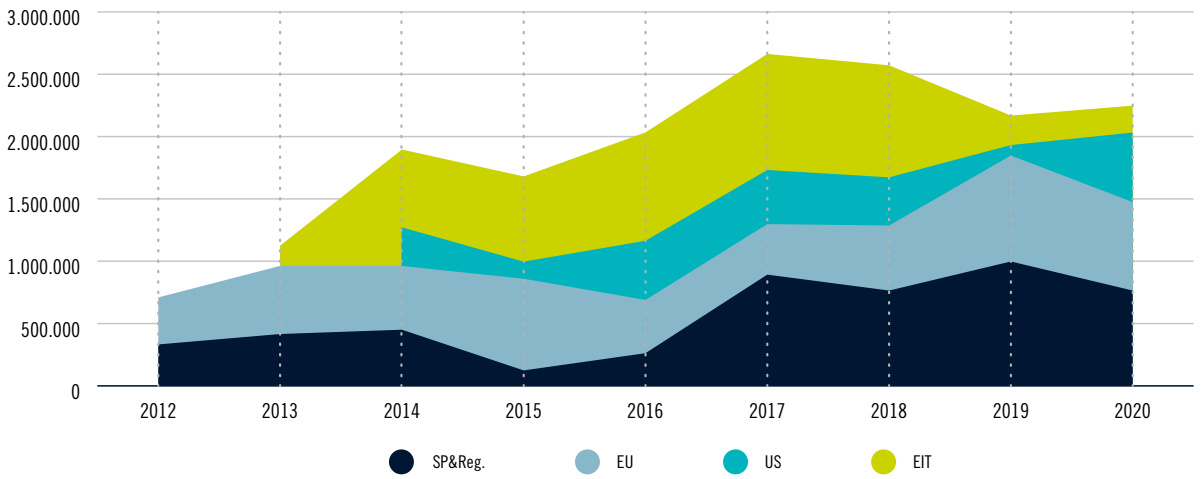
Thesis

- 5 PhD
- 2 Bachelor
- 2 Master

Invited talks

- 5 Invited plenary talks
- 21 Invited external speakers
- 23 Invited seminars and lectures
- 10 Seminar series

R&I External Income



Accumulated projects & fellowships

Projects since 2008

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: according to studies and macroeconomic simulations reported in *Shaping the Digital Transformation in Europe*, the cumulative additional GDP contribution of new digital technologies by 2030 could amount to €2.2 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 €75 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 €42 billion per year.

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

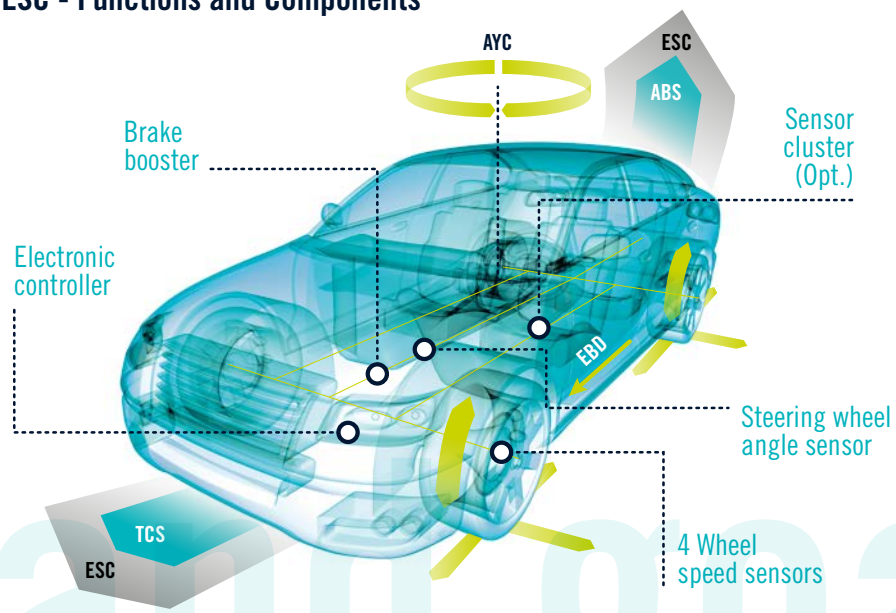
be adequately balanced. There is, therefore, a need not to stop investing in basic research in the post-pandemic world. Earmarking funds for other, more pressing needs to achieve a quick fix for a troubling situation is a temptation, but that should not get in the way of taking strategic steps towards 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 i*n 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.

ESC - Functions and Components



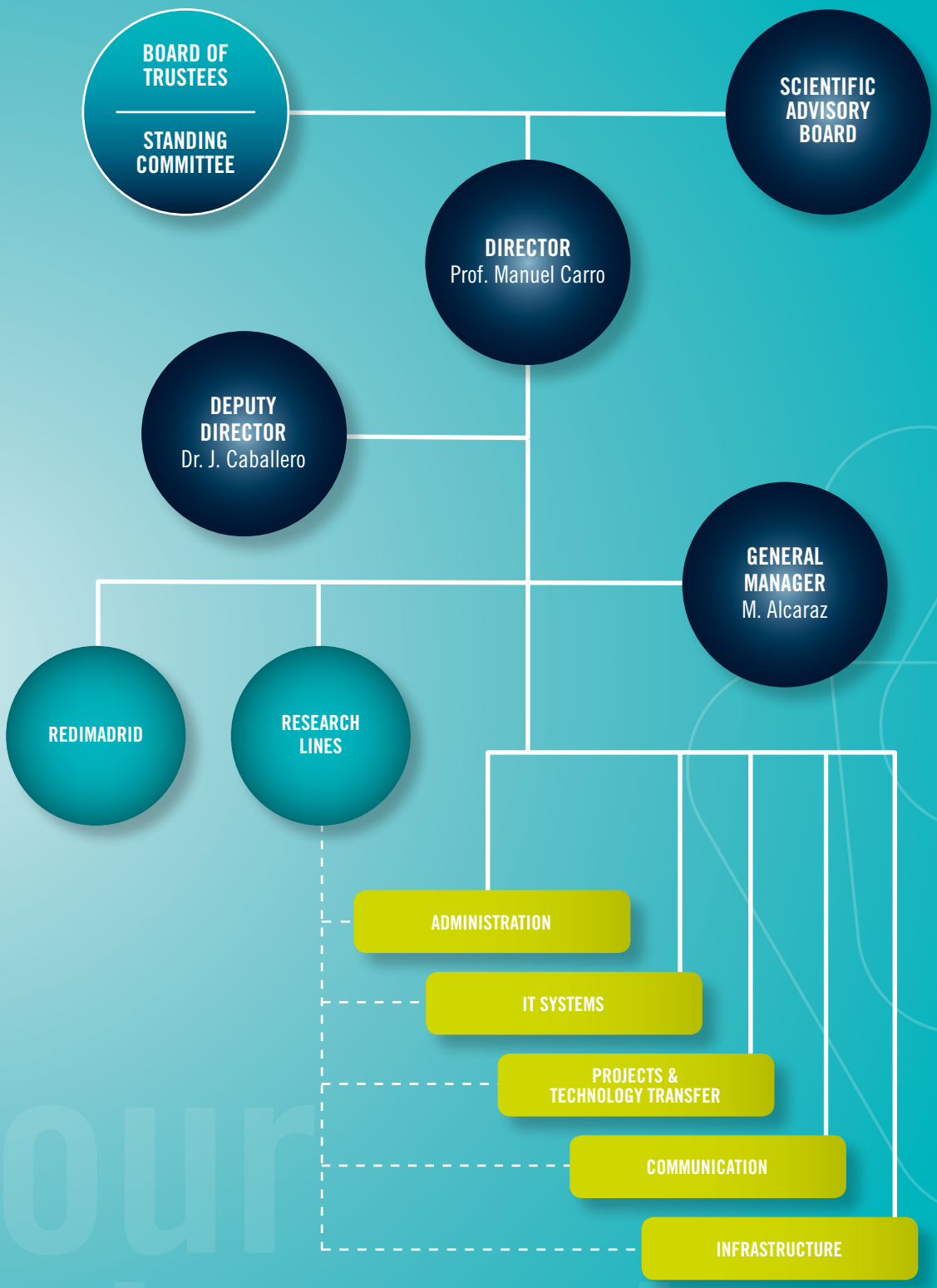
legal status, governance, and management

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

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. EDUARDO SICILIA CAVANILLAS
Councilor for Science, Universities, and Innovation, Madrid Regional Government, Spain.

REGIONAL GOVERNMENT AND PUBLIC ENTITIES

MARÍA LUISA CASTAÑO MARÍN
Director-General for Research and Innovation, Regional Ministry of Science, Universities, and Innovation, Madrid Regional Government, Spain

IRENE DELGADO SOTILLOS
Director-General for Universities and Higher Art Studies, Regional Ministry of Science, Universities, and Innovation, Madrid Regional Government, Spain

BÁRBARA FERNÁNDEZ-REVUELTA FERNÁNDEZ-DURÁN
Deputy Director-General for Research, Regional Ministry of Science, Universities, and Innovation, Madrid Regional Government, Spain

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. LUÍS MONIZ PEREIRA
Universidade Nova de Lisboa, Portugal.

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

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

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

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

SECRETARY

ALEJANDRO BLÁZQUEZ LIDOY

INDEPENDENT EXPERT

JESÚS CONTRERAS
Director EIT Digital Madrid Node

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

PROF. MARÍA ALPUENTE.
Universidad Politécnica de Valencia, Spain.

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

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

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

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

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

cooperation

Companies with which IMDEA Software Cooperated during 2020

Academic Institutions with which IMDEA Software Cooperated during 2020

Other Publicly-Funded Institutions with which IMDEA Software Cooperated during 2020

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, 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 Cyber Security (RENIC) and the European Cyber Security Organization (ECSO) that implements the Cyber Security Public-Private Partnership (cPPP) of the European Commission.

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. A good example of this is 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.

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.
- Technical University of Cluj-Napoca, Romania.
- 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.

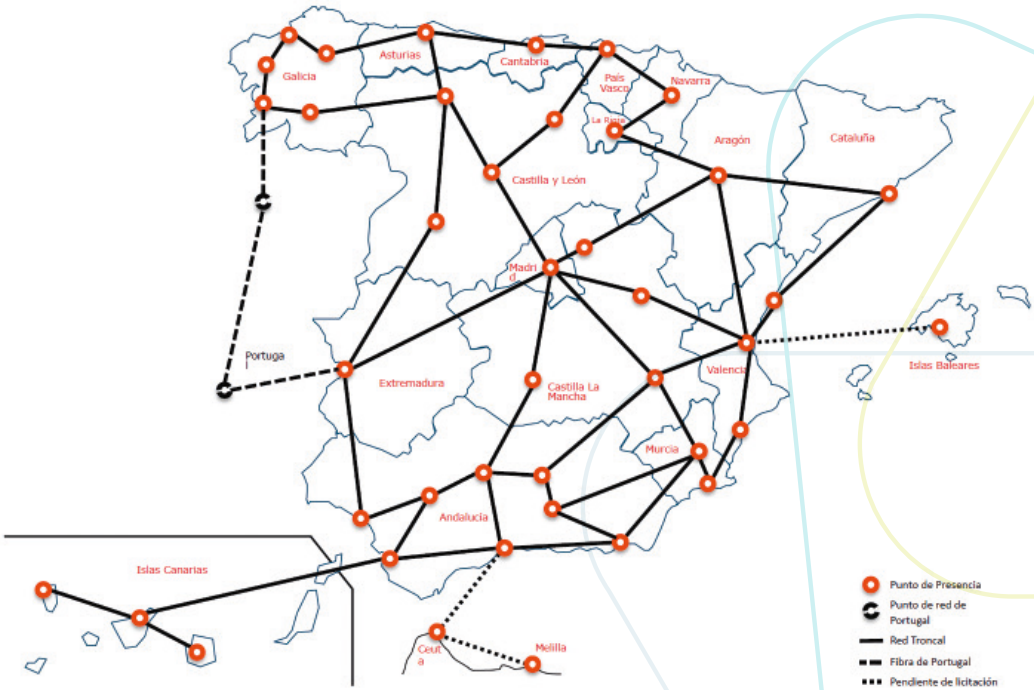
As examples that illustrate the importance of these agreements, the agreements with the Universidad Politécnica de Madrid (UPM) included hosting the Institute building in its Montegancedo Science and Technology Park and paves the way for teaching activities at different levels at the School of CS of 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 data network for research and higher education that provides high-speed 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 at least of 10Gb per second 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.

In 2020, REDIMadrid continued its expansion activating the dark fiber connections of the Institutions of Ciudad Unversitaria (namely, Universidad Complutense, Universidad Politécnica and UNED) with the points of presence of REDIMadrid (at CIEMAT and CSIC), as well as a direct connection between the nodes of REDIMadrid at CSIC and CIEMAT. These connections are activated at 100Gb per second, which will be the standard speed of each link in the new phase of the REDIMadrid deployment.


UAM
Universidad Autónoma de Madrid
UNED
ESIC
Universidad de Alcalá
POLITÉCNICA
UNIVERSIDAD COMPLUTENSE MADRID
CASA DE VELAZQUEZ
IRIS
red.es
imdea software
imdea energía
Universidad Rey Juan Carlos
uc3m Universidad Carlos III de Madrid
imdea networks
CEU Universidad San Pablo
CSIC
Universidad Europea de Madrid
LAUREATE INTERNATIONAL UNIVERSITIES


Galicia
Asturias
Cantabria
País Vasco
Navarra
La Rioja
Aragón
Cataluña
Castilla y León
Madrid
Portuga
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

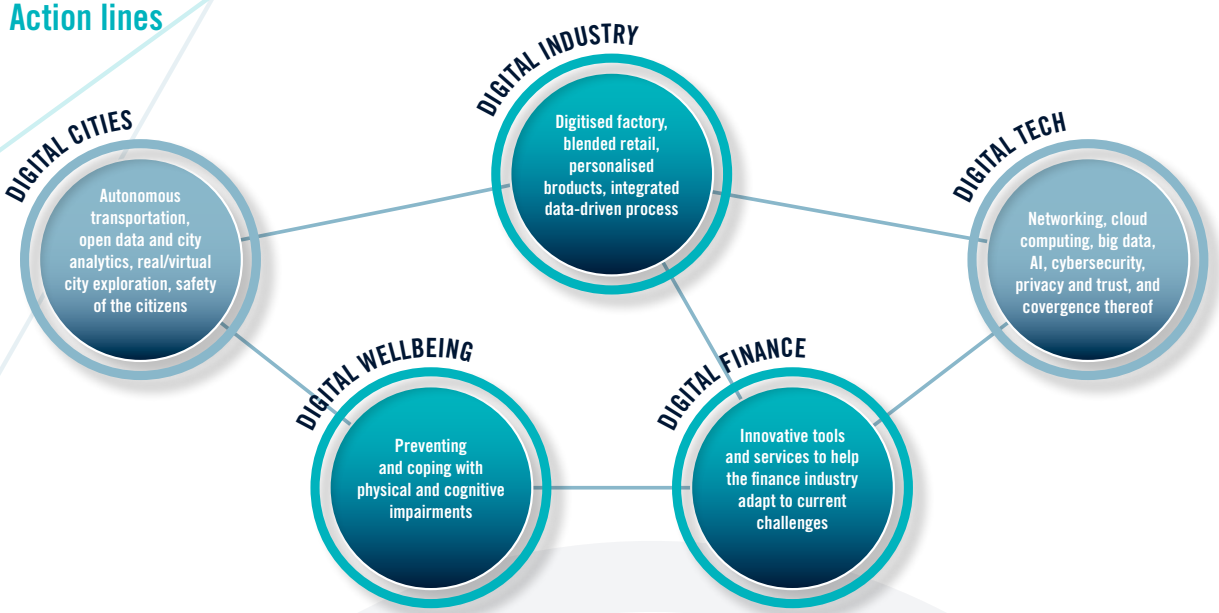
EIT Digital

EIT Digital is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT). EIT Digital (formerly known as EIT ICT Labs) 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).

Action lines



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

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.
- 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, automatic abstraction refinement.
- Decision procedures for complex data-types.
- Automata theory and formal languages.

Static analysis and abstract interpretation.

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

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.

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.

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

highlights

Privacy-Enhancing Technologies

"Arguing that you don't care about the right to privacy because you have nothing to hide, is no different than saying you don't care about free speech because you have nothing to say."

Edward Snowden

Privacy has a distinguished position among all other rights and plays a central role in Computer Science research. For instance, the somewhat recent General Data Protection Regulation (GDPR) articulates the key principles to be followed every time a new technology is designed. In this state of affairs, the design and evaluation of privacy-enhancing technologies (PETs) have become of paramount importance. PETs are cryptographic protocols that provide provable privacy guarantees to the otherwise privacy-invasive technologies. For instance, today's communication between our devices and third party services (e.g., our bank application) is carried out through HTTPS, a PET that creates a secure communication channel between two parties ensuring that no adversary can observe the transmitted information.

The trend in increasing complexity for the new technologies hinders the design of the corresponding privacy solutions. Current systems typically rely on several intertwined layers of functionality and enhancing only one of them with privacy is the same as not having any privacy guarantee at all. One such example are blockchains that combine a communication layer (i.e., users submitting their transactions to blockchain miners) and an application layer (i.e., miners executing a distributed protocol to decide what transactions are added to the ledger). In such a setting, a secure communication channel between the user and the miners is of little use for privacy since an observer of the publicly available transaction ledger can clearly see who pays what to whom.

An additional challenge is that privacy always comes at a cost in terms of performance. In the running example, current attempts at improving the privacy of the transaction ledger have resulted in a lower performant distributed protocol among the miners, effectively reducing the overall transaction throughput of the system. Therefore, achieving the right balance between strong privacy guarantees and high performance is a challenging research goal that appears with every new technology.

At our Institute we are devoting efforts to a systematic research on privacy. In particular, (1) we carry out a principled analysis of current technologies to evaluate possible privacy breaches; (2) we design formal models to characterize what are the privacy notions of interest for a certain technology; (3) we design cryptographic protocols that adapt the functionality of current technologies to meet the privacy notions of interest; (4) we formally prove that our privacy-enhanced protocols faithfully follow our modeled privacy notions; and (5) we create software tools that implement our privacy-enhancing technologies and make them available to the community.

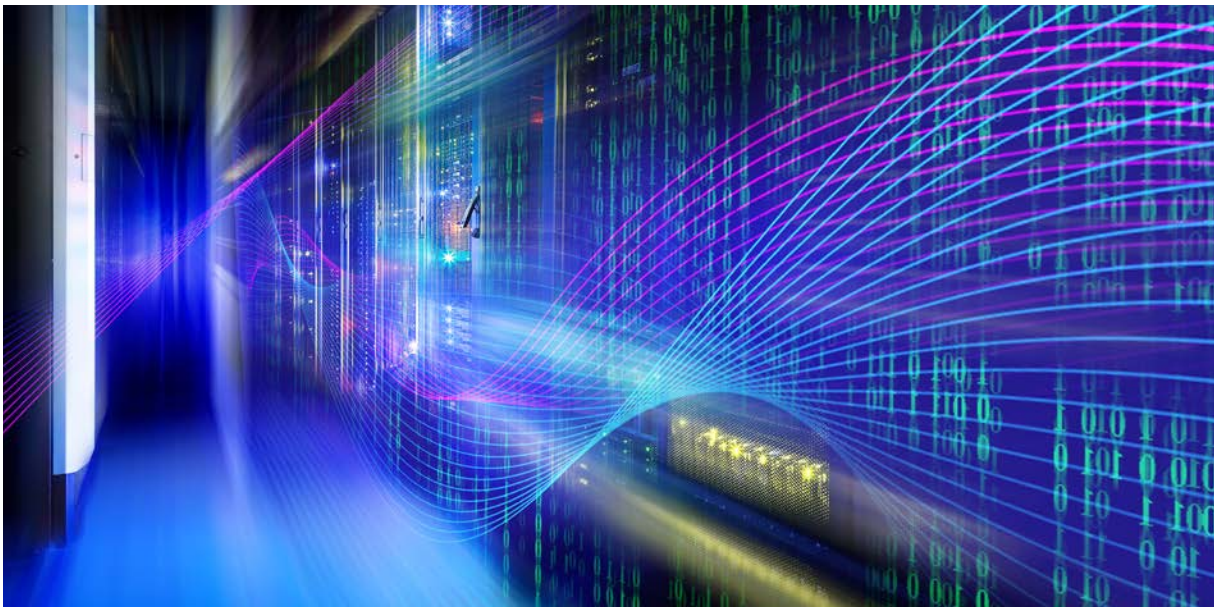
Tezos / Nomadic Labs: A Successful Collaboration

Knowledge transference between academia and industry is a topic on which much has been written and one of the few things that seems to be clear is that it is not straightforward. Researchers are often pointed at as working on abstract topics that do not correspond to actual problems — or, at least, to *current* problems. On the other hand, industry is often accused of focusing on immediacy and obtaining quick results, which is often not aligned with deep discoveries or long-term plans.

Still, there are sometimes meeting points where practical applications pose interesting challenges that can be enticing for researchers and useful for non-academic purposes. The Institute is lucky to be taking part in one of these collaborations where the best of both worlds aligned to provide deep research challenges that, at the same time, are being channeled through a high-tech IT startup into production in Tezos, an advanced, state-of-the-art blockchain initiative.

Tezos is the name of a distributed crypto-ledger technology with some unique characteristics. First and foremost, it has a self-amending model that permits amending its protocols (its governance, including the voting procedures) by voting inside the blockchain changes to the code itself. The structure of Tezos allows it to evolve to simulate other blockchain proposals (Bitcoin, Ethereum, etc.) The seed protocol in Tezos is based on Proof-of-Stake, which makes it much less power-hungry than other well-known blockchain infrastructures. Last, but not least, Tezos' architecture is designed to be highly modular and is written using a technology (the functional language OCaml) that lends itself much more easily to formal correctness proofs than other distributed ledgers. This principle is carried over to Michelson, the native low-level smart contract language of Tezos.

These characteristics make Tezos an ideal ecosystem to apply advanced technologies in distributed systems, verification, compilation, and cryptography on which the Institute has world-level experts. Through an umbrella agreement with the Tezos Foundation and the French company Nomadic Labs, specific research contracts are signed. These focus on topics that are relevant from a research point of view and, at the same time, interesting for the Tezos community from a practical point of view, thus undoubtedly representing the best of both worlds!



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.

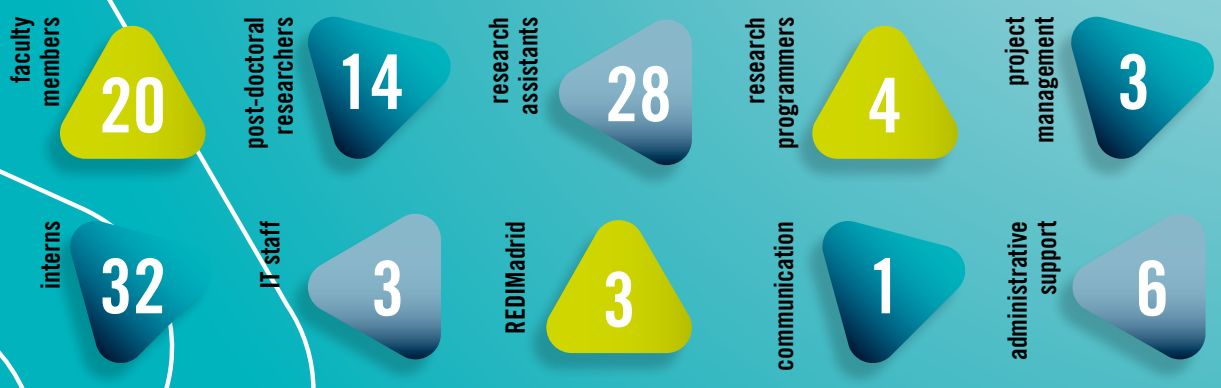
Hiring at the Institute follows internationally-standard open dissemination procedures with public, international calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and mailing 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.

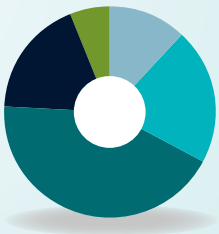
In addition to faculty positions, the Institute also has its own programs for visiting and staff researchers, post-docs, graduate scholarships, and internships. In all aspects related to human resources, the Institute follows the recommendations of the European Charter for Researchers and a Code of Conduct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

In 2020, the scientific staff of the Institute was composed of eleven senior faculty (full or associate professors, two part-time and one on leave), eight junior faculty (tenure-track or researchers), fourteen postdoctoral researchers, four research programmers, 28 research assistants (Ph.D. candidates, not counting visiting Ph.D. candidates) and 32 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 three project management staff, three system support staff, three REDIMadrid staff, six administrative support members, one communication and media manager, and one part-time administrative support that also gives general service to the rest of the IMDEA Institutes.

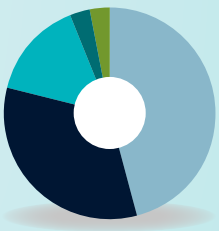
Figure 1 shows the ratio of each category at the end of 2020. Figure 2 summarizes where these researchers obtained their Ph.D. (by continents plus Spain), and Figure 3 shows the location where the Institute researchers were working before joining IMDEA. Finally, Figure 4 presents the nationalities of researchers at or above the Ph.D. level.





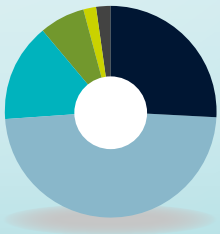
- 18% Senior Faculty
- 43% Research Assistant
- 12% Junior Faculty
- 6% Research Programmer
- 21% Postdocs

Figure 1
Type of position, all researchers



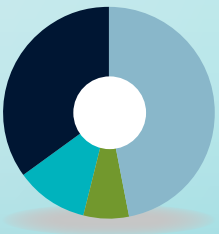
- 32% Spain
- 3% South America
- 47% Europe (ex. Spain)
- 2% Asia
- 16% North America

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



- 26% Spain
- 7% South America
- 48% Europe (ex. Spain)
- 2% Asia
- 15% North America
- 2% Australia

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



- 35% Spain
- 11% America
- 47% Europe (except Spain)
- 7% Asia

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 Europaea. 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.

Research Interests

Gilles' research is currently focused 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 of computational artifacts. 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.

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 foundamental problem arising in model-checking. He is interested in the application of abstract interpretation to decide those problems.

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.

Zsolt István
Assistant Research Professor

Zsolt received his PhD Degree in 2018 from ETH Zürich, Switzerland. His dissertation, entitled "Building Distributed Storage with Specialized Hardware", was awarded with the prestigious ETH Medal by the university. Before joining IMDEA Software as an Assistant Research Professor, he worked as a visiting researcher at IBM Rüschlikon, Switzerland. Prior to his doctoral studies, he completed the Master's degree in Computer Science (Distributed Systems) at ETH Zürich, Switzerland, in 2013, and the Bachelor's degree in Computer Science at UT Cluj-Napoca, Romania, in 2011.

Research Interests
Zsolt's research interests are in using specialized hardware to speed up distributed systems and databases without increasing their energy footprint, and to explore hybrid architectures for emerging data-intensive workloads. He uses field programmable gate arrays (FPGAs) as a vehicle for prototyping ideas.

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.

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.

faculty members on leave of absence

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.

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. Currently he is 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 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.

postdoctoral researchers

Antonio Faonio
Postdoctoral Researcher

Antonio received his Ph.D. degree in Computer Science from Sapienza University of Rome, Italy, where he was adviced by Giuseppe Ateniese. From 2014 to 2017 he was a postdoc researcher at Aarhus University, advised by Jesper Buus Nielsen. Starting from 2017, he is a postdoctoral researcher at IMDEA Software Institute where he works with Dario Fiore on cryptography.

Research Interests
Antonio's interest are in both theoretical and applied cryptography. He worked on leakage-resilient and tamper-resilient cryptography, non-malleability and controlled-malleability, re-randomizable cryptosystems and verifiable mixing networks, subversion resilient cryptography, zero-knowledge proofs, and password-based cryptography.

Ignacio Fábregas
Postdoctoral Researcher

Ignacio Fábregas received both his bachelor degree in Mathematics and Ph.D. in Computer Science in Universidad Complutense de Madrid (UCM). In 2017, he joined the IMDEA Software Institute as a post-doctoral researcher, where he works with Aleks Nanevski on the topic of Separation Logics for Concurrency. Before joining IMDEA Software he was a postdoc in Reykjavik University (Iceland), where he worked with Luca Aceto.

Research Interests
His current research interest are concurrency and logics. In particular, he is interested in separation logics, modal logics, category theory for computer science, and process semantics.

Avinash Sudhodanan
Postdoctoral Researcher

Avinash Sudhodanan received his Ph.D. in Information and Communication Technology from University of Trento (Italy). Prior to joining IMDEA Software Institute, he worked as an Early-Stage Researcher at Fondazione Bruno Kessler (Italy) and spent 18 months at SAP Labs France. Avinash received his Bachelors in Computer Science and Engineering and Masters in Cyber Security from Amrita Vishwa Vidyapeetham University, India.

Research Interests
Avinash's research interests primarily lie in the area of automatic detection of security vulnerabilities in web applications. His Ph.D. research led to the discovery of hundreds of serious security vulnerabilities affecting prominent web sites.

Yuri Meshman
Postdoctoral Researcher

Yuri Meshman obtained an M.Sc. and a Ph.D. at Technion Israel Institute of Technology, as well as a BSc in Mathematics and a BSc in Computer Science. During his BSc, he worked in an IBM Research group as a student software developer. During his Ph.D., he participated in the Fender project, an international research collaboration between Technion, Haifa and ETH, Zürich. Since March 2017, he is a postdoctoral researcher at the IMDEA Software Institute.

Research Interests
Yuri's current research interest are developing and verifying programs for systems with relaxed operational semantics.

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.

Matteo Campanelli
Postdoctoral Researcher

Matteo obtained his Ph.D. from the City University of New York in 2018 working at the intersection between decision theory, complexity, and cryptography. He was a visiting student at Aarhus University (2016) and at the Stanford Research Institute (2017). He joined IMDEA Software in 2018. Besides cryptographic research he has developed software for Libreoffice and machine learning models for ads quality at Google. He made the mistake of appearing on a few improv comedy stages in NYC; he was never able to surf.

Research Interests
Matteo's current research interests focus on the theory and practice of fast cryptographic protocols in general and on proof systems in particular.

Raphaelle Crubille
Postdoctoral Researcher

Raphaelle has a Master's degree in Computer Science from the Master Parisien de Recherche en Informatique and a PhD degree from Université Paris 7. She joined IMDEA Software Institute as a postdoctoral research in March 2019.

Research Interests
Raphaelle's research interests are in probabilistic (higher-order) computation, semantics of programming languages, and metrics for programs.

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's 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 the use of order theory, abstract interpretation, and compositionality.

Elena Gutiérrez
Postdoctoral Researcher

Elena Gutiérrez received her PhD. from Universidad Politécnica de Madrid while working as a researcher at IMDEA Software Institute with Pierre Ganty on the theory of automata and formal languages. During her PhD., she completed a 6-month internship in the National Institute of Informatics in Tokyo, advised by Ichiro Hasuo. After completing her PhD in september 2020, she became a postdoctoral researcher at the institute.

Research interests
Elena's research interests primarily lie in the theory of automata and grammars in the context of formal verification of software. She worked on the study of language-theoretical aspects of pushdown automata, automata minimization algorithms, residualization as well as tree automata minimization. She is also interested in the study of weighted automata and its applications on quantitative analysis of programs.

research programmers

Aliaksandr Hryzlou

Degree: M.Sc. University of Manheim, 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.

visiting and affiliate faculty

Patrick Cousot
Visiting Faculty
New York University.
Visiting during December 2019.

Roberto Giacobazzi
Affiliate Faculty

Anindya Banerjee
Affiliate Faculty

Boris Köpf
Affiliate Faculty

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.

Joaquín Arias
Research Assistant

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

Research: Design and implementation of advanced programming languages, including logic programming languages featuring constraints, tabling, and non-monotonic reasoning, and their application to reasoning over stream data and abstract interpretation.

Pepe Vila
Research Assistant

Degree: M.Sc. in Computer Engineering, Escuela de Ingeniería y Arquitectura de la Universidad de Zaragoza (EINA), Spain.

Research: Application security with emphasis on client-side web security and side channels. Micro-architectural attacks and countermeasures.

Alejandro Aguirre
Research Assistant

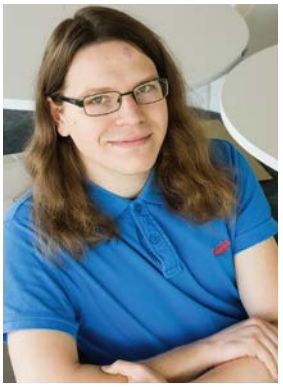
Degree: M.Sc. in Informatics, Université Paris Diderot (Paris 7), France.

Research: Formal methods fo rsoftware 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.

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.

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.

Pedro Valero
Research Assistant

Degree: Double BS in Computer Science and Mathematics, Universidad Autónoma de Madrid (UAM), Spain.

Research: Applications of quasiorders for solving problems from formal languages and automata theory.

Jesús Domínguez
Research Assistant

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

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

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.

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, meta-heuristics for fuzzing techniques.

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.

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.

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.

Kyveli Doveri
Research Assistant

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

Research: Formal languages of finite and infinite words.

Dimitris Kolonelos
Research Assistant

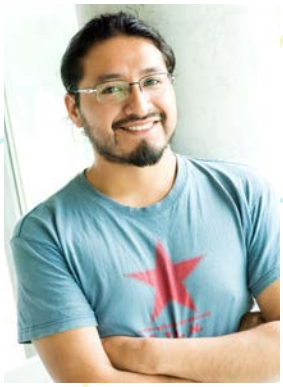
Degree: M.Sc. in Electrical And Computer Engineering, National Technical University of Athens, Greece.

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

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.



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 cyber-crime, 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.

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.

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.

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.

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 in termediate representation. Currently applying this technique to the study of gas consumption in Michelson smart contracts in the Tezos blockchain.

Zilong Wang
Research Assistant

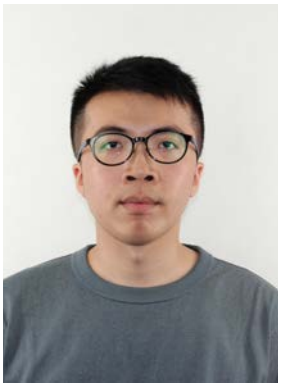
Degree: M.Sc. Universidad Autónoma de Madrid, Spain and The University of Science and Technology of China

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

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.



Man-Kit Sit
Research Assistant

Degree: M.Sc. in Engineering, Keio University, Japan

Research: Hardware Acceleration of Distributed Systems, Consensus Algorithms, Blockchains.

interns

Intern	Period	Nationality
Ignacio De Casso	04/18-09/20	Spain
David Munuera	09/19-05/20	Spain
Natalia Carpizo	09/19-06/20	Spain
Samuel García	09/19-05/20	Spain
Miguel Ángel Sánchez	09/19-12/20	Spain
Mohamed Ali	10/19-03/20	Egypt
Daniel Loscos	10/19-06/20	Spain
Stefan Malewski	11/19-03/20	Chile
Muhammad Laiq	11/19-03/20	India
Mustafa Hafidi	11/19-07/20	Morocco
S.M. Kumail Raza	11/19-03/20	Pakistan
Pablo Conde	02/20-04/20	Spain
Alexandre Bois	02/20-08/20	France
Margarita Capretto	02/20-08/20	Argentina
Eva Palandjian	03/20-09/20	France
Zachary Grannan	03/20-12/20	USA
Andoni Rodríguez	03/20-12/20	Spain
Aarti Kashyap	07/20-09/20	India
Maria Kokkou	07/20-09/20	Greece
Ashwin Nambiar	07/20-09/20	India
Paula Benedec	07/20-10/20	Romania
Andrei Tosa	07/20-10/20	Spain
Eli Guenzburger	08/20-10/20	Germany
Nicola Amadio	09/20-12/20	Italy
Aldana Ramírez	09/20-12/20	Argentina
Pablo Martínez de Leiva	09/20-12/20	Spain
Guillermo García	09/20-12/20	Spain
Alejandro De La Cruz	09/20-12/20	Spain
Elizaveta Vasilenko	10/20-12/20	Russia
Elena Ortiz	11/20-12/20	Spain
Daniel Jurjo	11/20-12/20	Spain
Juan Francisco García	11/20-12/20	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

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

Aiora Garalde
Project Assistant

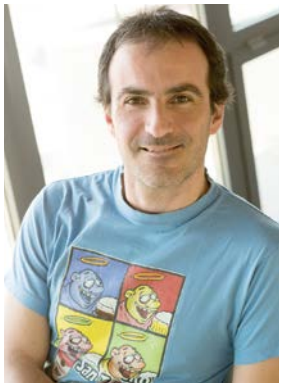
Degree: BS in Business Administration and Management, University of Alicante, Spain; National University of Distance Education, Spain.

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.

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.

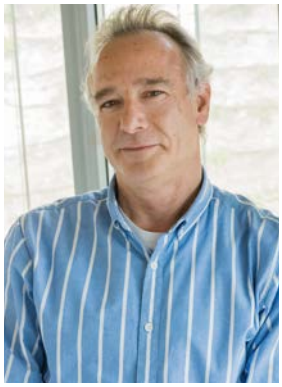
Andrea Iannetta
Human Resources Assistant

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

Ignacio Echaide
Human Resources Coordinator

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

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.

Communication

Blanca Gutiérrez
Communication Manager

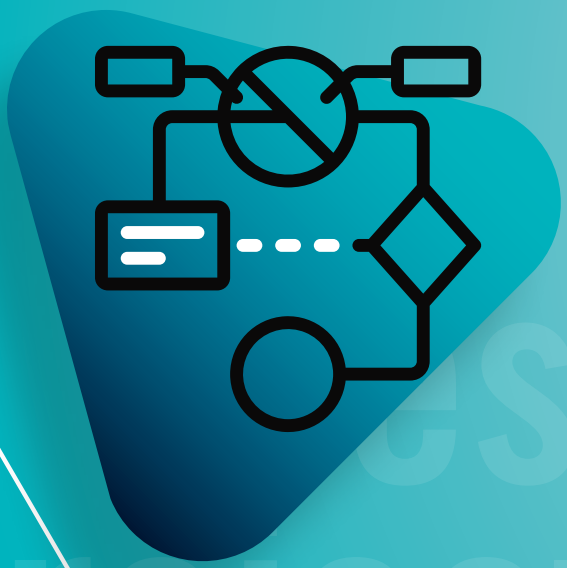
Degree: M.Sc. MS in Corporate Communication Management, EAE, OBS and University of Barcelona, Spain

common IMDEA services

Begoña Moreno
IMDEA Institutes' Coordination

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

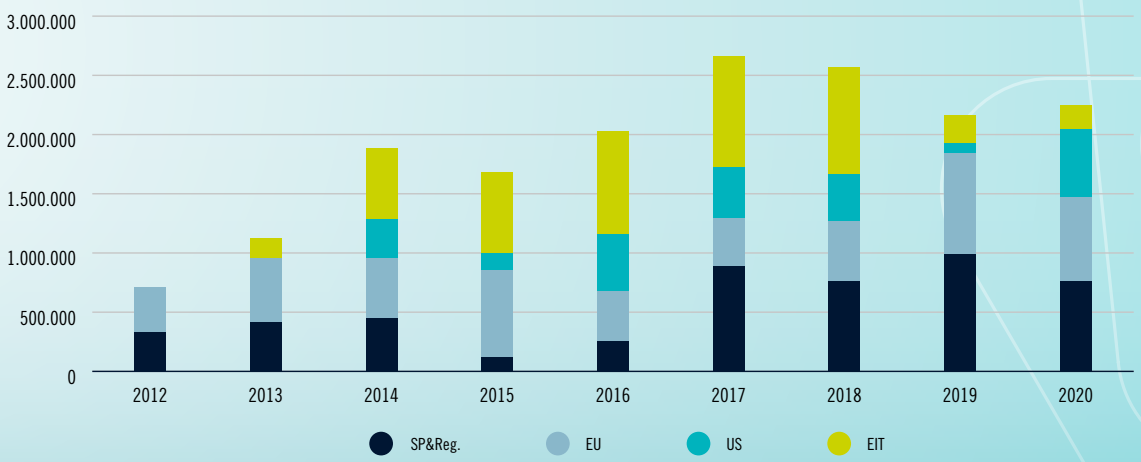
research projects and contracts



An important source of funding and technology transfer opportunities for the Institute are projects, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. During 2020, the Institute participated in a total of 24 funded research projects and contracts, of which ten of them (or almost 42%) involve collaboration with industry and eight of them have direct industrial funding. Of these 24 projects, twelve come from international sources (four funded by the European Union, one by the ONR-US agency, and seven by foreign companies), twelve have a national source, and funds for two come from regional sources, either through competitive calls or via contracts with companies. Figure 1 shows the origin of project funding.

The trend of external funding for the period 2012-2020 is shown in Figure 1. The amount of external funding for 2020 amounts to €2.2M, with the percentage of external funding for research and innovation w.r.t. the total Institute budget reaching 42%.

Figure 1
R&I External Income



projects running in 2020

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.

EIT Digital Spain
Coordination and Joint Activities

Funding: Spanish Ministry of Science, Innovation and Universities
Duration: 2018-2020
Principal Investigator: Assoc. Res. Prof. Juan Caballero

This project continues the action of its predecessor granted in 2015 and aims to boost the activities of the Spanish node of EIT Digital. The duties of IMDEA Software, as project beneficiary, focus on contributing to the progress of the network in collaboration with the members of the node with a twofold objective: on the one hand, to improve knowledge of the KIC possibilities in order to take maximal profit from the innovation program, and on the other hand to spread the activities of the KIC in the National ICT sector at all levels: large companies, SMEs, entrepreneurs, students, academia and researchers.

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.

MadridFlightOnChip

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

Funding: Regional Government of Madrid
Duration: 2019–2021
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 demostrator 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.

e-TUR2020

TUrismo & Retail

Funding: Spanish Ministry of Economy, Industry, and Competitiveness – CDTI
Duration: 2015-2020
Principal Investigator: Assoc. Res. Prof. Juan Caballero

e-TUR2020 is a four-year Spanish joint industrial research project funded by the Centre for the Development of Industrial Technology (CDTI). The aim of e-TUR2020 is to create a new on-line platform for the tourism sector that will enrich the sector's mobile applications with new services for tourists, tourist sector agents, and companies from other sectors. The e-TUR2020 project involves six industrial partners (Compartia, Eurona, Groupalia, SoluSoft, Tecnocom, Zemsania). The industrial partners subcontract parts of the work to 4 research and development centers (Eurecat, IMDEA Software Institute, PCT, and Universidad Carlos III de Madrid). Within e-TUR2020, the IMDEA Software Institute will manage the security aspects. To this end, the Institute will contribute to research and develop techniques to secure the information exchange.

TRACES

Technologies and tools for Resource-Aware, Correct, Efficient Software

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2020
Principal Investigators: Assoc. Res. Prof. Manuel Carro – Res. Prof. Manuel Hermenegildo

The TRACES project revolves around the need of change in the fundamental tools and approaches which underlie the software engineering techniques to be applied in the very near future. For this purpose TRACES includes three

main research lines: 1) Resource-aware computing: being able to determine safe (and maybe approximate) bounds for the resource consumption of software in a given hardware, and optimize it as much as possible, is necessary to ensure the correctness of embedded devices in terms which are more general than just functional correctness; 2) Advanced techniques to ensure functional correctness: these include not only infinite-state verification, but also debugging, synthesis of concurrent software, probabilistic / heuristic methods, and lean methods, such as testing and runtime / dynamic verification. These are necessary when, for example, the boundaries of a computer system are not well-known in advance, or the interactions with the outside world can only be probabilistically modeled; 3) New language technologies: new environments, tasks, and missions make it necessary to adapt existing languages to them or to create languages anew. Contrary to widespread belief, new languages and programming models are constantly created not only in academia but also in industry with the aim of either taking advantage of new devices or of performing tasks (e.g., knowledge-related) which would be too complex to write (and to ensure correct!) in traditional languages.

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 Complutense 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.

RACCOON

A Rigorous Approach to Consistency in Cloud Databases

Funding: European Union, European Research Council – H2020 Framework Program
Duration: 2017-2022
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 endusers 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.

ACCORD

Accelerated Ordering Service for Distributed Ledgers

Funding: European Union, Marie Curie Action (Individual Fellowship) – H2020 Framework Program
Duration: 2019-2020
Principal Investigator: Asst. Res. Prof. Zsolt István

The ACCORD project aims to increase distributed ledger throughput by at least an order of magnitude, while lowering latencies by a similar factor. To achieve this, the project focuses on the core component of DL systems, namely, distributed consensus, that is used to establish an absolute order of transactions. This ordering operation (service) is typically the main performance bottleneck in DLs. To fully exploit emerging network technologies and to overcome stagnating CPU performance, ACCORD will use hardware acceleration (i.e., FPGAs) to offload the steps required by the ordering service. The outcome of this project is a DL design with performance that allows it to be deployed in use-cases in which DLs are inadequate today (e.g., trading).

POST

Novel Constructions of Proof-of-Spacetime

Funding: Protocol Labs
Duration: 2018-2020
Principal Investigators: Assoc. Res. Prof. Dario Fiore – Post. Res. Matteo Campanelli

Proofs of Space Time (PoST) allow a user to show she has been storing a file for a certain amount of time. They are an important building block of the FileCoin protocol. Current constructions for PoST are based on the following paradigm: iterate a Proof of Replication (PoRep) and prove that all the repetitions are correct through a SNARK system. Unfortunately, applying even a state-of-the-art general purpose SNARK would result in PoST with impractical performances on the prover's side. The goal of this project is to design new PoST developing new SNARKs that are especially tailored to Proofs of Replication and their iteration.

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,

NEC Industrial Research Grant

Private Computation in Distributed Systems and Ledger Technologies

Funding: NEC Labs Europe
Duration: 2020
Principal Investigator: Assoc. Res. Prof. Dario Fiore

IMDEA researchers have started a research program funded by NEC to investigate how to reconcile required data sharing of distributed systems with privacy of data owners. This investigation is related to two main directions. On the one side, it touches on the problem of computing on private data in such a way that certain parties (i.e., data consumers) learn only the minimum amount of information that is needed. On the other hand, it aims to investigate consensus protocols—a fundamental building block of distributed ledgers—and its implication for privacy.

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.

BBVA

Research agreement with BBVA

Funding: BBVA
Duration: 2020
Principal Investigators: Assoc. Res. Prof. Dario Fiore – Post. Res. Antonio Faonio

Thanks to this agreement BBVA and the IMDEA Software Institute will explore the application of cryptographic techniques in the financial sector - techniques that make it possible for data to be shared and analyzed without exposing their content to third parties thanks to algorithms, protocols and encryption systems. Among various privacy-enhancing technologies, zero knowledge proofs (ZKP) is one that has the greatest potential, and it will be the main subject of this new team's study. This technology uses cryptographic algorithms to make it easier to verify the accuracy of information, without having to share the data that comprise it. This way, it can help create data-based solutions in which customers' sensitive data is not exposed to third parties (as it is not necessary to share the data with them to prove that they are accurate). The goal is for the research to translate into tangible advances that make it possible to transfer the benefits of this technology to the financial sector, the corporate world, the scientific community and society as a whole.

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 goals of the project are 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 together. The

specialized computations that our investigators aim to address will include set (non) membership, vector commitments, and digital signatures. The other goal of the project is to improve the state-of-the-art protocols for randomness generation, which are of vital relevance in proof-of-stake blockchains. The project will analyze the trade-offs between efficiency and corruption tolerance of current protocols, improve the communication and computation complexity of current proposals, and find more modular constructions that can be instantiated with diverse cryptographic tools, with special interest in post-quantum secure constructions.

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.

FAKULTÄT FÜR INFORMATIK
Faculty of Informatics

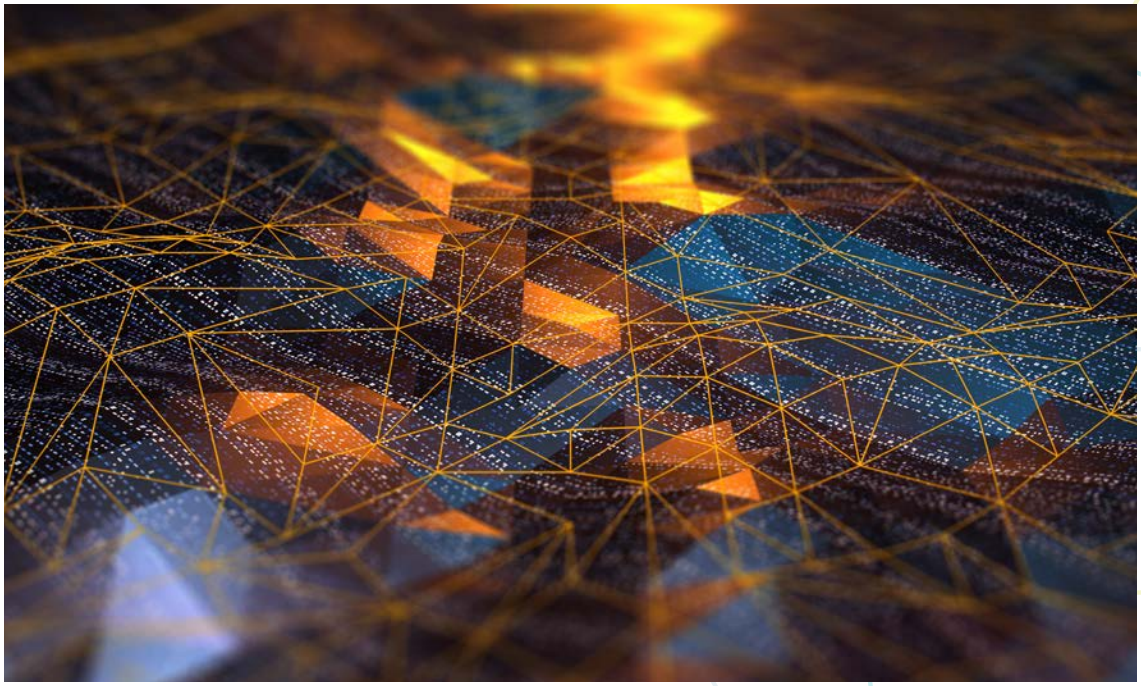
SLN

Scalability for the Lightning Network

Funding: Chaincode labs Inc. - Technical University of Wien 74
Duration: 2020–2021
Principal Investigator: Asst. Res. Prof. Pedro Moreno

The 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 the practical deployment.



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, Fraunhofer Gesellschaft, Pure-Systems Gmbh, STiftelsen Sintef, Autronica, Franders Mechatronics Technology Centre, Atego Systems, Teknologia Tutkimuskeskus VTT, Mobisoft, HIQ Finland, Softkinetic Sensors, Macq, Metso Automation.
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, Telefónica I+D, British TeleCom, Orange, Citycom, DIN Deutsches Institut für Normung, NPL Management, Thales, IXBLUE, Thales, MT Pelerini Group SA
ACCORD	H2020	IBM Research
AutoCrypt	ONR - Stanford University	SRI International
SynCrypt	ONR - Stanford University	SRI International
Contracts (BBVA)	BBVA	BBVA
Contracts (SLN)	Chaincode	Chaincode Labs Inc.
Contracts (Systematic Design of Blockchain Consensus Protocols)	Nomadic Labs	Tezos - Nomadic labs.
Contracts (Cost Analysis, Verification, and Optimization for Tezos via Parametric Resource Analysis)	Nomadic Labs	Tezos - Nomadic labs.
Contracts (Cryptographic Primitives for Randomness Generation and Privacy)	Nomadic Labs	Tezos - Nomadic labs.

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. *Juan de la Cierva grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2022 (**Manuel Bravo**).

4. *Juan de la Cierva grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2020 (**Zsolt István**).

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. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2020 (**Marco Guarnieri**).

8. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2020 (**Manuel Bravo**).

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

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 2020 and ending in 2024 (**Luís Miguel Danielsson**).

15. *Predoctoral Grant*, Protocol Labs, awarded in 2019 and ending in 2020 (**Dimitris Kolonelos**).

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

projects to start in 2021

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.

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.

NEC Industrial Research Grant

Secure Cloud Storage with Controlled Computation

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

Continuing with the research collaboration between IMDEA and NEC Labs since 2018, our researchers plan to start 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 is related to two main directions. First, it relates to the general problem of computation over encrypted data that allows to strike a balance between utility and privacy. Second, it relates to attestation, authentication and authorization mechanism for effective access control and data handling.


instituto
Idea software

communication and dissemination

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. *Manuel V. Hermenegildo*, *Pedro Lopez-Garcia*, Alberto Pettorossi, Maurizio Proietti. Preface, Fundamenta Informaticae, Special Issue on the 26th International Symposium on Logic-Based Program Synthesis and Transformation: LOPSTR 2016. Fundamenta Informaticae, Vol. 177, Num. 3–4, pages 1–3, IOS Press, December 2020.

2. Roberto Bruni, *Roberto Giacobazzi*, Roberta Gori, *Isabel Garcia-Contreras*, Dusko Pavlovic. Abstract Extensionality – On the Properties of Incomplete Abstract Interpretations. Proc. ACM Program. Lang., Vol. 4, Num. POPL, January 2020.

3. *Gilles Barthe*, Gustavo Betarte, Juan Diego Campo, Carlos Luna, David Pichardie. System-Level Non-interference of Constant-Time Cryptography. Part II: Verified Static Analysis and Stealth Memory. J. Autom. Reason., Vol. 64, Num. 8, pages 1685–1729, 2020.

4. *Gilles Barthe*, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert, Pierre-Yves Strub. Improved parallel mask refreshing algorithms: generic solutions with parametrized non-interference and automated optimizations. J. Cryptographic Engineering, Vol. 10, Num. 1, pages 17–26, 2020.

5. *Gilles Barthe*, Sandrine Blazy, Benjamin Grégoire, Rémi Hutin, *Vincent Laporte*, David Pichardie, Alix Trieu. Formal verification of a constant-time preserving C compiler. Proc. ACM Program. Lang., Vol. 4, Num. POPL, pages 1–30, 2020.

6. *Gilles Barthe*, Justin Hsu, Mingsheng Ying, Nengkun Yu, Li Zhou. Relational proofs for quantum programs. Proc. ACM Program. Lang., Vol. 4, Num. POPL, pages 1–29, 2020.

7. *Gilles Barthe*, Justin Hsu, Kevin Liao. A probabilistic separation logic. Proc. ACM Program. Lang., Vol. 4, Num. POPL, pages 1–30, 2020.

8. Yiyun Liu, James Parker, Patrick Redmond, Lindsey Kuper, Michael Hicks, *Niki Vazou*. Verifying replicated data types with typeclass refinements in Liquid Haskell. Proc. ACM Program. Lang., Vol. 4, Num. OOPSLA, pages 1–30, ACM, 2020.

9. Martin A. T. Handley, *Niki Vazou*, Graham Hutton. Liquidate your assets: reasoning about resource usage in liquid Haskell. Proc. ACM Program. Lang., Vol. 4, Num. POPL, pages 1–27, 2020.

10. Ray Neiheiser, Luciana Rech, *Manuel Bravo*, Luís E. T. Rodrigues, Miguel Correia. Fireplug: Efficient and Robust Geo-Replication of Graph Databases. IEEE Trans. Parallel Distributed Syst., Vol. 31, Num. 8, pages 1942–1953, 2020.

11. Torben Amtoft, *Anindya Banerjee*. A Theory of Slicing for Imperative Probabilistic Programs. ACM Trans. Program. Lang. Syst., Vol. 42, Num. 2, pages 1–71, 2020.

12. Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James R. Larus, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth G. Paterson, Srdjan Capkun, David A. Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel P. Smart, Aysajan Abidin, Seda Gurses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, *Dario Fiore*, Manuel Barbosa, Rui Oliveira, José Pereira. Decentralized Privacy-Preserving Proximity Tracing. IEEE Data Eng. Bull., Vol. 43, Num. 2, pages 36–66, 2020.

13. *Ignacio Cascudo*, Jaron Skovsted Gundersen, Diego Ruano. Squares of matrix-product codes. Finite Fields and Their Applications, Vol. 62, 2020.

14. Yotam M. Y. Feldman, Artem Khyzha, Constantin Enea, Adam Morrison, *Aleksandar Nanevski*, Noam Rinetzky, Sharon Shoham. Proving highly-concurrent traversals correct. Proc. ACM Program. Lang., Vol. 4, Num. OOPSLA, pages 1–29, 2020.

15. *Alejandro Aguirre*, Shin-ya Katsumata. Weakest Preconditions in Fibrations. Electronic Notes in Theoretical Computer Science, Vol. 352, pages 5–27, 2020. The 36th Mathematical Foundations of Programming Semantics Conference, 2020.

16. Martin Leucker, *César Sánchez*, Torben Scheffel, Malte Schmitz, Alexander Schramm. Runtime verification of real-time event streams under non-synchronized arrival. Softw. Qual. J., Vol. 28, Num. 2, pages 745–787, 2020.

17. Fabio Fioravanti, *John P. Gallagher*, Maurizio Proietti. Preface, Special Issue on LOPSTR 2017. Fundam. Inform., Vol. 173, Num. 4, 2020.

Conferences

1. José Bacelar Almeida, Manuel Barbosa, *Gilles Barthe*, *Vincent Laporte*, Tiago Oliveira. Certified Compilation for Cryptography: Extended x86 Instructions and Constant-Time Verification. 21st International Conference on Cryptology in India, INDOCRYPT 2020, Lecture Notes in Computer Science, Vol. 12578, pages 107–127, Springer, December 2020.

2. *Matteo Campanelli*, *Dario Fiore*, Nicola Grego, *Dimitris Kolonelos*, *Luca Nizzardo*. Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage. ASIACRYPT 2020: 26th Annual International Conference on the Theory and Applications of Cryptology and Information Security, LNCS, Vol. 12492, pages 3–35, Springer, December 2020.

3. *Ignacio Cascudo*, Bernardo David. ALBATROSS: Publicly AttestabLe BATched Randomness Based On Secret Sharing. Advances in Cryptology - ASIACRYPT 2020 -26th International Conference on the Theory and Application of Cryptology and Information Security, Part III, Lecture Notes in Computer Science, Vol. 12493, pages 311–341, Springer, December 2020.

4. *Ignacio Cascudo*, Jaron Skovsted Gundersen. A Secret-Sharing Based MPC Protocol for Boolean Circuits with Good Amortized Complexity. Theory of Cryptography- 18th International Conference, TCC 2020, Part II, Lecture Notes in Computer Science, Vol. 12551, pages 652–682, Springer, December 2020.

5. Martín Ceresa, *Felipe Gorostiaga*, *César Sánchez*. Declarative Stream Runtime Verification (hLola). Proc. of the 18th Asian Symposium on Programming Languages and Systems (APLAS'20), LNCS, Vol. 12470, pages 25–43, Springer, December 2020.

6. *Silvia Sebastián, Juan Caballero*. AVClass2: Massive Malware Tag Extraction from AV Labels. Proceedings of the 2020 Annual Computer Security Applications Conference, December 2020.

7. Fabio Gadducci, Hernán C. Melgratti, *Christian Roldán*, Matteo Sammartino. Implementation Correctness for Rep-

licated Data Types, Categorically. International Colloquium on Theoretical Aspects of Computing, ICTAC 2020, LNCS, Vol. 12545, pages 283–303, Springer, November 2020.

8. *Victor Perez-Carrasco*, *Maximiliano Klemen, Pedro Lopez-Garcia*, *Jose F. Morales*, *Manuel V. Hermenegildo*. Cost Analysis of Smart Contracts via Parametric Resource Analysis. Proceedings of the 27th Static Analysis Symposium (SAS 2020), LNCS, Vol. 12389, Springer-Verlag, November 2020.

9. *Silvia Sebastián, Juan Caballero*. *Towards Attribution in Mobile Markets: Identifying Developer Account Polymorphism.* Proceedings of the 27th ACM Conference on Computer and Communication Security, November 2020.

10. Nataliia Stulova, Arianna Blasi, *Alessandra Gorla*, Oscar Nierstrasz. Towards Detecting Inconsistent Comments in Java Source Code Automatically. 20th IEEE International Working Conference on Source Code Analysis and Manipulation, SCAM 2020, pages 65–69, IEEE, October 2020.

11. *Antonio Faonio*, *Dario Fiore*. Improving the Efficiency of Re-randomizable and Replayable CCA Secure Public Key Encryption. Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, LNCS, Vol. 12146, pages 271–291, Springer, October 2020.

12. *Felipe Gorostiaga*, *Luis Miguel Danielsson, César Sánchez*. Unifying the Time-Event Spectrum for Stream Runtime Verification. LNCS, Vol. 12399, pages 462–481, Springer, October 2020.

13. Mattia Fazzini, *Alessandra Gorla*, Alessandro Orso. A Framework for Automated Test Mocking of Mobile Apps. 35th IEEE/ACM International Conference on Automated Software Engineering, ASE 2020, pages 1204–1208, IEEE, September 2020.

14. *Frantisek Farka*. slepice: Towards a Verified Implementation of Type Theory in Type Theory. 30th International Symposium on Logic-Based Program Synthesis and Transformation, LOPSTR 2020, LNCS, Vol. 12561, pages 133–150, Springer, September 2020.

15. Amir-Hossein Karimi, *Gilles Barthe*, Borja Balle, Isabel Valera. Model-Agnostic Counterfactual Explanations for Consequential Decisions. The 23rd International Conference on Artificial Intelligence and Statistics, AISTATS 2020, Proceedings of Machine Learning Research, Vol. 108, pages 895–905, PMLR, August 2020.

16. Borja Balle, *Gilles Barthe*, Marco Gaboardi, Justin Hsu, Tetsuya Sato. Hypothesis Testing Interpretations and Renyi Differential Privacy. The 23rd International Conference on Artificial Intelligence and Statistics, AISTATS 2020, Proceedings of Machine Learning Research, Vol. 108, pages 2496–2506, PMLR, August 2020.

17. Nuno Afonso, *Manuel Bravo*, Luís Rodrigues. Combining High Throughput and Low Migration Latency for Consistent Data Storage on the Edge. 29th International Conference on Computer Communications and Networks, ICCCN 2020, pages 1–11, IEEE, August 2020.

18. Gianluca Brian, *Antonio Faonio*, Maciej Obremski, Mark Simkin, Daniele Venturi. Non-malleable Secret Sharing Against Bounded Joint-Tampering Attacks in the Plain Model. 40th Annual International Cryptology Conference, CRYPTO 2020, LNCS, Vol. 12172, pages 127–155, Springer, August 2020.

19. *Pierre Ganty*, *Elena Gutiérrez, Pedro Valero*. A Quasiorder-Based Perspective on Residual Automata. 45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020, LIPIcs, Vol. 170, pages 1–14, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, August 2020.

20. *Gilles Barthe*, Rohit Chadha, Vishal Jagannath, A. Prasad Sistla, Mahesh Viswanathan. Deciding Differential Privacy for Programs with Finite Inputs and Outputs. 35th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '20, pages 141–154, ACM, July 2020.

21. *Gilles Barthe*, Charlie Jacomme, Steve Kremer. Universal equivalence and majority of probabilistic programs over finite fields. 35th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '20, pages 155–166, ACM, July 2020.

22. Sunjay Cauligi, Craig Disselkoen, Klaus von Gleissenthall, Dean M. Tullsen, Deian Stefan, Tamara Rezk, *Gilles Barthe*. Constant-time foundations for the new spectre era. Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, pages 913–926, ACM, June 2020.

23. Paolo Calciati, Konstantin Kuznetsov, *Alessandra Gorla*, Andreas Zeller. Automatically Granted Permissions in Android apps: An Empirical Study on their Prevalence and on the Potential Threats for Privacy. MSR 2020: 17th International Conference on Mining Software Repositories, pages 114–124, ACM, June 2020.

24. Uwe Wolter, *Fernando Macías*, Adrian Rutle. *Multilevel Typed Graph Transformations*. Graph Transformation - 13th International Conference, ICGT 2020, LNCS, Vol. 12150, pages 163–182, Springer, June 2020.

25. *Pepe Vila, Pierre Ganty*, *Marco Guarnieri*, Boris Köpf. CacheQuery: Learning Replacement Policies from Hardware Caches. Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2020, pages 519–532, ACM, June 2020.

26. José Bacelar Almeida, Manuel Barbosa, *Gilles Barthe*, Benjamin Grégoire, Adrien Koutsos, *Vincent Laporte*, Tiago

Oliveira, Pierre-Yves Strub. The Last Mile: High-Assurance and High-Speed Cryptographic Implementations. 2020 IEEE Symposium on Security and Privacy, SP 2020, pages 965–982, IEEE, May 2020.

27. *Dario Fiore*, Anca Nitulescu, David Pointcheval. Boosting Verifiable Computation on Encrypted Data. 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2020, LNCS, Vol. 12111, pages 124–154, Springer, May 2020.

28. Dario Catalano, Mario Di Raimondo, *Dario Fiore*, Irene Giacomelli. MonZa: Fast Maliciously Secure Two Party Computation on Z2k. 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2020, LNCS, Vol. 12111, pages 357–386, Springer, May 2020.

29. Borzoo Bonakdarpour, Pavithra Prabhakar, *César Sánchez*. Model Checking Timed Hyperproperties in Discrete-Time Systems. NASA Formal Methods - 12th International Symposium, NFM'2020, LNCS, Vol. 12229, pages 311–328, Springer, May 2020.

30. *Gilles Barthe*, *Raphaëlle Crubillé*, Ugo Dal Lago, *Francesco Gavazzo*. On the Versatility of Open Logical Relations - Continuity, Automatic Differentiation, and a Containment Theorem. 29th European Symposium on Programming, ESOP 2020, Held as Part of ETAPS 2020, Lecture Notes in Computer Science, Vol. 12075, pages 56–83, Springer, April 2020.

31. *Ignacio Casso, Jose F. Morales*, *Pedro Lopez-Garcia*, *Roberto Giacobazzi*, *Manuel V. Hermenegildo*. *Computing Abstract Distances in Logic Programs.* Post-Proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), LNCS, Vol. 12042, Springer-Verlag, April 2020.

32. *Ignacio Casso, Jose F. Morales*, *Pedro Lopez-Garcia*, *Manuel V. Hermenegildo*. *An Integrated Approach to Assertion-Based Random Testing in Prolog.* Post-Proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), LNCS, Vol. 12042, pages 159–176, Springer-Verlag, April 2020.

33. *Maximiliano Klemen, Pedro Lopez-Garcia*, *John P. Gallagher*, *Jose F. Morales*, *Manuel V. Hermenegildo*. *A General Framework for Static Cost Analysis of Parallel Logic Programs.* Post-Proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), LNCS, Vol. 12042, pages 19–35, Springer-Verlag, April 2020.

34. *Avinash Sudhodanan*, Soheil Khodayari, *Juan Caballero*. Cross-Origin State Inference (COSI) Attacks: Leaking Web Site States through XS-Leaks. Network and Distributed Systems Security Symposium, February 2020.

35. *Marco Guarnieri*, Boris Köpf, *José F. Morales*, Jan Reineke, Andrés Sánchez. Spectector: Principled detection of speculative information

flows. Proceedings of the 41st IEEE Symposium on Security and Privacy, S&P 2020, IEEE, 2020.

36. Alvaro Feal, *Paolo Calciati*, Narseo Vallina-Rodriguez, Carmela Troncoso, *Alessandra Gorla*. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. The 20th Privacy Enhancing Technologies Symposium (PoPETs 2020.2), pages 314–335, 2020.

37. *Manuel Bravo*, Gregory Chockler, *Alexey Gotsman*. *Making Byzantine consensus live.* DISC'20: International Symposium on Distributed Computing, LIPICS, Vol. 179, Dagstuhl, 2020.

38. Vitor Enes, Carlos Baquero, Tuanir França Rezende, *Alexey Gotsman*, Matthieu Perrin, Pierre Sutra. *State-machine replication for planet-scale systems.* EuroSys'20: European Conference on Computer Systems, ACM, 2020.

39. *Isabel Garcia-Contreras, Jose F. Morales*, *Manuel V. Hermenegildo*. *Incremental Analysis of Logic Programs with Assertions and Open Predicates.* Proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), LNCS, pages 36–56, Springer-Verlag, 2020.

40. *Joaquín Arias*, Zhuo Chen, *Manuel Carro*, Gopal Gupta. Modeling and Reasoning in Event Calculus Using Goal-Directed Constraint Answer Set Programming. Post-Proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), LNCS, Vol. 12042, pages 139–155, Springer-Verlag, 2020.

41. Gordon J. Pace, *César Sánchez*, Gerardo Schneider. Reliable Smart Contracts. Proc. of the 9th Int'l Symp. on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'2020). Verification. Part III, LNCS, Vol. 12478, pages 3–8, Springer, 2020.

42. Xueliang Li, Yuming Yang, Yepang Liu, *John P. Gallagher*, Kaishun Wu. *Detecting and Diagnosing Energy Issues for Mobile Applications.* Proc. of the ACM SIGSOFT International Symposium on Software Testing and Analysis, ACM Press, 2020.

43. *John P. Gallagher*, Robert Glück. An Experiment Combining Specialization with Abstract Interpretation. Proceedings 8th International Workshop on Verification and Program Transformation and 7th Workshop on Horn Clauses for Verification and Synthesis, VPT/HCV (ETAPS) 2020, and 7th Workshop on Horn Clauses for Verification and Synthesis, EPTCS, Vol. 320, pages 155–158, 2020.

Workshops

1. *Ignacio Casso, Jose F. Morales, Pedro Lopez-Garcia, Manuel V. Hermenegildo. Testing Your (Static Analysis) Truths.* Pre-proceedings of the 30th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'20), September 2020.

2. *Juan José Moreno-Navarro. Industrial innovation and top ranked universities.* Academic Proceedings of the 2020 University-Industry Interaction Conference Series, June 2020.

3. *Joaquín Arias, Manuel Carro,* Zhuo Chen, Gopal Gupta. *Justifications for Goal-Directed Constraint Answer Set Programming.* Proceedings 36th International Conference on Logic Programming (Technical Communications), EPTCS, Vol. 325, pages 59–72, Open Publishing Association, 2020.

4. *John P. Gallagher, Manuel V. Hermenegildo,* Bishoksan Kafle, *Maximiliano Klemen, Pedro Lopez-Garcia, Jose F. Morales.* From big-step to small-step semantics and back with interpreter specialization (invited paper). Proceedings of the Eighth International Workshop on Verification and Program Transformation (VPT 2020), Electronic Proceedings in Theoretical Computer Science (EPTCS), pages 50–65, Open Publishing Association (OPA), 2020. Co-located with ETAPS 2020.

Edited Volumes

1. *Manuel V. Hermenegildo, Pedro Lopez-Garcia,* Alberto Pettorossi, Maurizio Proietti (Eds.). *Fundamenta Informaticae, Special Issue on the 26th International Symposium on Logic-Based Program Synthesis and Transformation: LOPSTR 2016.* Vol. 177, Num. 3–4, IOS Press, December 2020.

2. *Alexey Gotsman,* Ana Sokolova (Eds.). Proc. of Formal Techniques for Distributed Objects, Components, and Systems - 40th IFIP WG 6.1 International Conference, FORTE 2020, Held as Part of the 15th International Federated Conference on Distributed Computing Techniques, DisCoTec 2020. Lecture Notes in Computer Science, Vol. 12136, Springer, June 2020.

Doctoral, Master and Bachelor Theses

1. Jaron Skovsted Gundersen. *On the Interaction Between Linear Codes, Secret Sharing, and Multiparty Computation*. Ph.D. Thesis. Aalborg University. December 2020. Advisors: Ignacio Cascudo (IMDEA Software Institute), Diego Ruano, Horia Cornean and Olav Geil (Aalborg University).

2. Elena Gutiérrez Viedma. *New Perspectives on Classical Automata Constructions*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). September 2020. Advisor: Pierre Ganty (IMDEA Software Institute).

3. Pedro Valero Mejía. *On the Use of Quasiorders in Formal Language Theory*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2020. Advisor: Pierre Ganty (IMDEA Software Institute).

4. José Vila Bausili. *Learning secrets and models from execution time*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). June 2020. Advisor: Boris Köpf (IMDEA Software Institute).

5. Joaquín Arias. *Advanced Evaluation Techniques for (Non)-Monotonic Reasoning Using Rules with Constraints*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). February 2020. Advisor: Manuel Carro (IMDEA Software Institute and Technical University of Madrid).

6. Emanuele Giunta. *Auxiliary Oracle IOP and secure, fast reductions of R1CS over binary field*. Master Thesis. Università degli Studi di Catania. September 2020. Advisors: Dario Catalano (U. degli Studi di Catania) and Ignacio Cascudo (IMDEA Software Institute).

7. Francesco Parolini. *Simulation-based Inclusion Checking Algorithms for ω-Languages*. Master Thesis. Università degli Studi di Padova. July 2020. Advisors: Francesco Ranzato (U. degli Studi di Padova) and Pierre Ganty (IMDEA Software Institute).

8. Natalia Carpizo. *Mejora de un Sistema de Autodocumentación Basado en Comentarios Legibles Mecánicamente y Aserciones: LPDowner*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). June 2020. Advisors: Manuel Hermenegildo (IMDEA Software Institute and Technical University of Madrid) and José Francisco Morales (IMDEA Software Institute).

9. *Víctor Pérez-Carrasco*. *Analysis of Smart Contracts using Horn Clauses*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). June 2020. Advisors: Manuel Hermenegildo (IMDEA Software Institute and Technical University of Madrid), Pedro López (IMDEA Software Institute and CSIC) and José F. Morales (IMDEA Software Institute).

Invited Talks

Invited and Plenary Talks by IMDEA Scientists

1. *Juan Caballero*. Malware & PUP: Keep them separate, if you can. Invited talk at the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). October 2020.

2. *John Gallagher*. From Big-Step to Small-Step Semantics and Back with Interpreter Specialisation. Invited talk and proceedings article. VPT 2020, ETAPS workshop, Dublin, 2020.

3. *Alexey Gotsman*. Reasoning about consistency choices in modern distributed systems. Summer School on Practice and Theory of Distributed Computing. July 2020.

4. *Manuel Hermenegildo*. Cost Analysis of Smart Contracts via Parametric Resource Analysis. Invited plenary talk at the 27th Static Analysis Symposium (SAS 2020). Chicago, USA. November 2020.

5. *Pedro Moreno-Sanchez*. Security, Privacy and Interoperability in Payment-Channel Hubs. BIS: Workshop on Blockchain Interoperability and Sharding. October 2020.

Invited Seminars and Lectures by IMDEA Scientists

1. *Matteo Campanelli*. Techniques in efficient zero-knowledge. Hanyang University, Seoul, South Korea. February 2020.

2. *Matteo Campanelli*. Standard Proposal: Commit-and-Prove Zero-Knowledge Proof Systems. 3rd ZKProof Workshop. April 2020.

3. *Ignacio Cascudo*. On UC-secure homomorphic commitments. Cryptography Seminar, Universitat Politècnica de Catalunya, Barcelona, Spain. January 2020.

4. *Dario Fiore*. zkSNARKs: who, what, and... blockchains! Invited talk at the First IMDEA Software - Tezos Blockchain Workshop, Madrid, Spain. January 2020.

5. *Dario Fiore*. Boosting Verifiable Computation on Encrypted Data. Kookmin University, South Korea, August 2020.

6. *Pierre Ganty*. Deciding language inclusion problems using quasiorders. The 2nd Learning and Verification day, in LaBRI, Bordeaux, France, January 2020.

7. *Gibran Gomez*. Malicious TLS Traffic Detection using Unsupervised Machine Learning. XV Jornadas REDIMADRID 2020, Madrid, Spain. October 2020.

8. *Alexey Gotsman*. Making BFT Consensus Live. Tezos-IMDEA Workshop, IMDEA Software Institute, Madrid, January 2020.

9. *Alexey Gotsman*. Atomic Transactions for Modern Data Stores. University of Aarhus, Denmark, March 2020.

10. *Alexey Gotsman*. Making BFT Consensus Live. University of Aarhus, Denmark, March 2020.

11. *Alexey Gotsman*. Making Byzantine Consensus Live. Theory and Practice of Blockchains. June 2020.

12. *Marco Guarnieri*. Exorcising Spectres with Secure Compilers. Workshop on Principles of Secure Compilation (PRISC 2020). January 2020.

13. *Marco Guarnieri*. Spectector: Principled detection of speculative information flows. Italian Conference on CyberSecurity (ITASEC 2020). February 2020.

14. *Marco Guarnieri*. CacheQuery: Learning Replacement Policies from Hardware Caches. Microsoft Research Cambridge, Programming Language Seminar. February 2020.

15. *Marco Guarnieri*. Hardware-Software Contracts for Secure Speculation. Intel Side-channel Academic Program Tech talk. July 2020.

16. *Marco Guarnieri*. Hardware-Software Contracts for Secure Speculation. Intel Side-channel Academic Program Workshop. September 2020.

17. *Marco Guarnieri*. Spectector: Principled detection of speculative information flows. Invited lecture at Hardware Security course (D-ITET), ETH Zürich. November 2020.

18. *Elena Gutiérrez*. A Congruence-based Perspective on Automata Minimization Algorithms. Formal Methods Seminar at Laboratoire Bordelais de Recherche en Informatique (LaBRI). Bordeaux, France. June, 2020.

19. *Dimitris Kolonelos*. Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage. Protocol Labs Research Seminars. November 2020.

20. *Aleks Nanevski*. Type and Proof Structures for Concurrency. Boston University Programming Languages Seminar, Boston, US. May 2020.

21. *César Sánchez*. Temporal Verification of Hyperproperties. Universidad País Vasco, San Sebastián, Spain. January 2020.

22. *Ida Tucker*. Bandwidth efficient threshold ECDSA. Journées Codage et Cryptographie du GDR IM et du GDR Sécurité Informatique. IRISA, Rennes, France. November 2020.

23. *Niki Vazou*. Refinement Types & Functional Extensionality. IFIP Working Group 2.1. Otterlo, The Netherlands. January 2020.

Invited Speaker Series

During 2020, 21 external speakers were invited to give talks at IMDEA Software. Due to the pandemic, since March 2020 all the seminars have been given in videoconference, with 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. *Samira Briongos*. Postdoctoral researcher, UPM: RELOAD+REFRESH: Abusing Cache Replacement Policies to Perform Stealthy Cache Attacks.

2. *Ida Tucker*. PhD student, École Normale Supérieure de Lyon, France: Distributing the elliptic curve digital signature algorithm both securely and efficiently.

3. *Roberto Di Cosmo*. Research Professor, INRIA Paris, France: Archiving, assessing and attributing research software: towards software as a first class citizen in the scholarly world.

4. *Jaron Skvosted Gundersen*. PhD Student, Aalborg University, Denmark: Improved Bounds on the Threshold Gap in Ramp Secret Sharing.

5. *Carsten Baum*. Post-doctoral Researcher, Aarhus University, Denmark: Efficient Constant-Round MPC with Identifiable Abort and Public Verifiability.

6. *Borzoo Bonakdarpour*. Assistant Research Professor, Iowa State University, USA: Synthesis of Parametrized Distributed Self-stabilizing Protocols.

7. *Alberto Ros*. Associate Research Professor, Universidad de Murcia: Non-Speculative and Invisible Reordering of Memory Operations.

8. *Pedro Moreno Sánchez*. Post-doctoral Researcher, Vienna University of Technology, Austria: Security, Privacy and Scalability in Blockchain Technologies.

9. *Cristian-Alexandru Staicu*. Post-doctoral Researcher, TU Darmstadt, Germany: Code Reuse Gone Rogue: The Dangers of Overrelying on Third-Party JavaScript Code.

10. *Arpan Gujarati*. Post-doctoral Researcher, Max Planck Institute for Software Systems, Germany: Towards Ultra-Reliable Cyber-Physical Systems: Reliability Analysis of Distributed Real-Time Systems.

11. *Leonidas Lampropoulos*. Post-doctoral Researcher, U. of Maryland and U. of Pennsylvania, USA: Software Correctness at Scale through Testing and Verification.

12. *Aastha Mehta*. PhD Student, Max Planck Institute for Software Systems, Germany: Policy Compliance in Online Services.

13. *Stefania Dumbrava*. Assistant Research Professor, Ecole Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise (ENSIIE): Mechanically Verified Graph Query Processing.

14. *Michael Greenberg*. Assistant Professor, Pomona College: Executable Formal Semantics for the POSIX Shell.

15. *Manuel Rigger*. Post-doctoral Researcher, ETH Zürich, Switzerland: Three Tales on Finding Logic Bugs in Database Management Systems.

16. *Antonio Nappa*. Post-doctoral Researcher, Corelight Inc, USA: ScrambleSuit: A Tool for Testing Malware Analysis Sandboxes using PoW-based Side Channels Mechanism.

17. *Eduardo Soria Vázquez*. Post-doctoral Researcher, Aarhus University, Denmark: Secure and Verifiable Computation (over rings).

18. *Pedro Cabalar*. Associate Professor, University of A Coruña, Spain: Answer Set Programming and its Temporal Extension.

19. *Antonio Nappa*. Chief Technology Officer, BitCorp Intelligence Creative Labs, Italy: One ray to rule them all: Inducing soft-errors by gamma-ray emissions at ground level.

20. *Lydia Garms*. Post-doctoral Researcher, Royal Holloway, University of London (RHUL), United Kingdom: Group Signatures with Selective Linkability and Extensions.

21. *Juan Lastra Díaz*. Ad-honorem Researcher, National University of Distance Education, Spain: Reproducibility practices and initiative encouraged by Information Systems.

Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **10** seminars were given in 2020.

Scientific Service and Other Activities

Conference and Program Committee Chairmanship

Alexey Gotsman:

1. PC Co-Chair, International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE), 2020.

Bishoksan Kafle:

2. PC Co-chair of the 8th International Workshop on Horn Clauses for Verification and Synthesis (HCVS 2021).

Cesar Sanchez:

3. Co-organizer of the track "Reliable smart contracts" at the 9th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation.

Niki Vazou:

4. Chair of Student Research Competition, 47th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2020).

Editorial Boards and Conference Steering Committees

Gilles Barthe:

1. Editorial Board of the Journal of Automated Reasoning.
2. Editorial Board of the Journal of Computer Security.
3. Editorial board of Transactions on Dependable and Secure Computing.

Juan Caballero:

4. Steering committee of the Annual Computer Security Applications Conference (ACSAC).
5. Steering committee of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).
6. Steering Committee of the International Symposium on Engineering Secure Software and Systems (ESSoS).

Manuel Carro:

7. Area Editor, Theory and Practice of Logic Programming.

Dario Fiore:

8. Editorial Board of IET Information Security Journal.
9. Editor Board of the International Journal of Applied Cryptography.

John Gallagher:

10. Steering Committee. International Symposium on Functional and Logic Programming (FLOPS).

Pedro Lopez-Garcia:

11. Steering Committee of the International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR).

12. Guest editor of Fundamenta Informaticae, vol. 177 (3-4), December, 2020, IOS Press, Special Issue on the 26th International Symposium on Logic-Based Program Synthesis and Transformation: LOPSTR 2016.

Manuel Hermenegildo:

13. Steering Committee of the Conference on Compiler Construction (CC).
14. Steering Committee of the International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR).
15. Steering Committee of the International Symposium on Functional and Logic Programming (FLOPS).
16. Steering Committee of the ACM SIGPLAN Workshop/Symposium on Partial Evaluation and Program Manipulation (PEPM).
17. Editorial Advisor of "Theory and Practice of Logic Programming" (Cambridge U. Press).
18. Area editor, Algorithms in Programming Languages and Software Engineering, of the "Journal of the IGPL" (Oxford U press).
19. Area Editor, Logic and Constraint Logic Programming, of the "Journal of Applied Logics" (CP - IFCoLog Journal).

Niki Vazou:

20. Steering Committee of Haskell Symposium.
21. Steering Committee of ACM SIGSAC Workshop on Programming Languages and Analysis for Security (PLAS).
22. Steering Committee of Workshop on Type-driven Development (TyDe).

Participation in Program Committees

Alejandro Aguirre:

1. 25th International Conference in Functional Programming (ICFP 2020), Artifact Evaluation Committee.

Gilles Barthe:

2. 27th ACM Conference on Computer and Communications Security (CCS 2020).
3. 32nd International Conference on Computer-Aided Verification (CAV 2020).

Manuel Bravo:

4. 4th Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL 2020), co-located with Middleware 2020.

Juan Caballero:

5. 27th ACM Conference on Computer and Communications Security (CCS 2020).
6. 17th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2020).
7. 41st IEEE Symposium on Security & Privacy (IEEE S&P 2020).
8. 2020 Network and Distributed System Security Symposium (NDSS 2020).

Manuel Carro:

9. 36th International Conference on Logic Programming (ICLP 2020).
10. Declarative Problem Solving Workshop (DPSW 2020).
11. 2020 International Conference on Services Computing (SCC 2020).

Ignacio Cascudo:

12. 18th IACR Theory of Cryptography Conference (TCC 2020).

Antonio Faonio:

13. The 24th International Conference on Financial Cryptography and Data Security (FC 2020).
14. The 15th International Workshop on Security (IWSEC 2020).

Dario Fiore:

15. 23rd International Conference on Practice and Theory of Public-Key Cryptography (PKC 2020).

Pierre Ganty:

16. 14th International Conference on Reachability Problems (RP 2020).
17. 8th International Conference on Networked Systems (NETYS 2020).
18. 21st International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2020).

Alexey Gotsman:

19. 39th ACM Symposium on Principles of Distributed Computing (PODC 2020).
20. 47th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2020).

Marco Guarnieri:

21. 33rd IEEE Computer Security Foundations Symposium (CSF 2020).
22. 5th IEEE European Symposium on Security and Privacy (EuroS&P 2020).
23. 15th ACM SIGSAC Workshop on Programming Languages and Security (PLAS 2020).

Bishoksan Kafle:

24. 8th International Workshop on Verification and Program Transformation (VPT 2020).
25. 31st International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2021).
26. 21st International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI-AE 2020), Artifact evaluation committee.

Manuel Hermenegildo:

27. 37th International Conference on Logic Programming (ICLP 2020).
28. ACM SIGPLAN 2020 International Conference on Compiler Construction (CC 2020).
29. SPLASH 2020 Workshop on Logic and Practice of Programming (LPOP 2020).
30. 22nd International Symposium on Practical Aspects of Declarative Languages (PADL 2020).

Pedro Lopez-Garcia:

31. 1st Workshop on Energy Efficiency at the Edge (WEEE 2020), co-located with ACM e-Energy 2020.

Fernando Macías:

32. 7th International Workshop on Multi-Level Modelling (MULTI 2020).

César Sánchez:

33. 2nd Workshop on Formal Methods for Blockchains (FMBC2020).
34. 20th International Conference on Runtime Verification (RV'20).
35. 17th International Colloquium on Theoretical Aspects of Computing (ICTAC'20).

36. 7th Workshop on Reactive and Event-based Languages & Systems (REBLS'20), colocated with SPLASH'20.

Niki Vazou:

37. Workshop on Foundations of Computer Security 2020 (FCS'20).
38. 32nd International Conference on Computer-Aided Verification (CAV'20).

Association and Organization Committees

Manuel Carro:

39. Representative of IMDEA Software in Informatics Europe.
40. Member of the joint board of the Erasmus Mundos European Master in Software Engineering.
41. Representative of IMDEA Software in the Node Strategy Committee of EIT Digital Spain.
42. Representative of IMDEA Software at the General Assembly of EIT Digital.
43. Signed accession agreement to Alastria.
44. Member of the Transference committee of Alastria.

Manuel Hermenegildo:

45. President of the INRIA Scientific Council (Institut National de Recherche en Informatique et en Automatique, France).
46. Member of the Schloss Dagstuhl Scientific Advisory Board (Germany).
47. Member of the Executive Committee of the ACM Europe Technology Policy Committee.
48. Member of the Academia Europaea. Member of the Nomination Committee.
49. Member of the Jury for the 2020 SCIE-Fundación BBVA National Prizes in Informatics.
50. Member of the External Advisory Board of the NOVA LINCS Institute (Portugal).
51. Member of the IRILL Scientific Advisory Board (French Institute for Free Software).
52. Member of the Board Nomination Committee of Informatics Europe.
53. Secretary of the International Association for Logic Programming.
54. Member of the International Federation for Computational Logic (IFCoLog) Advisory Board.
55. Member of the Technical University of Madrid Consulting Council.
56. Member of the Technical University of Madrid Gallery of Distinguished Professors.

Niki Vazou:

57. Member of Visualization Committee in POPL'20.

Awards

Paper Awards:

1. *Dario Fiore*, Aikaterini Mitrokotsa, Luca Nizzardo, Elena Pagnin. Multi-Key Homomorphic Authenticators. IET Information Security, vol. 13, issue 6. **2020 Premium Award for Best Paper in the IET**.

Thesis Awards:

2. *Platon Kotzias*. A Systematic Empirical Analysis of Unwanted Software Abuse, Prevalence, Distribution, and Economics. **UPM extraordinary award 2018-2019 for PhD thesis**.

Other Awards:

3. *Ida Tucker*. 2020 L'Oréal-UNESCO France Rising Talent Award for Women in Science.
4. Daniel Benarroch, *Matteo Campanelli*, *Dario Fiore*. Commit-and-Prove Zero-Knowledge Proof Systems. 3rd ZKProof workshop. **Most impactful discussion**.

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 2020.

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*.

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:

munication

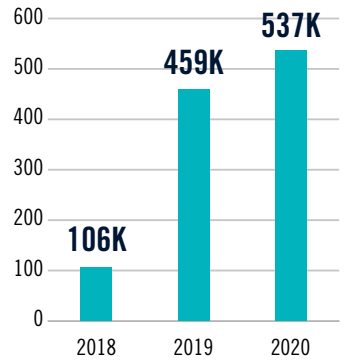
19 web news

6 press releases

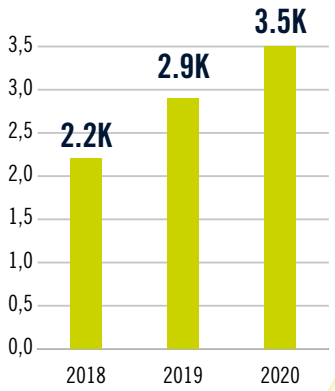
97 media impacts

558 social network posts

total impressions



total community



536,5K

impressions

453K	24.3K	8.7K	38K	12.5K

3,5K

community

1125	54	200	1758	321

Dissemination events

In 2020, researchers from the IMDEA Software Institute have participated in several events related to dissemination and the promotion of science. The majority of them have been virtual due to the COVID-19 pandemia.

Women and Girls in Science Day

'Breaking Codes: Women and Girls in Science'

February 11, 2020

IMDEA Software

5 researchers (3 from the Institute)

+100 school students

On the occasion of the International Day of Woman and Girl in Science, the IMDEA Software Institute organized the conference "Breaking Codes: Women and Girls in Science", with the support of researchers from the Institute as well as from other centres in the Campus, such as the Center for Biomedical Technology (CTB). Researchers from each center led a small workshop focused on their fields of expertise.

The contribution of the IMDEA Software Institute was focused on cryptography, with a workshop that was led by three researchers from the IMDEA Software Institute: Anaïs Querol, Elena Gutiérrez and Isabel García.

This was a great opportunity to bring science and research closer to young girls, to encourage STEM vocations, and to make it possible for the audience to interact with young and established researchers.

Video summary

Photo gallery

Virtual

3 researchers

50

Science and Innovation Week

The Roots of Software II

November 11, 2020

The IMDEA Software Institute joins once again the Science and Innovation Week organised by the Regional Ministry of Science, Universities and Innovation of the Madrid Regional Government, through the Fundación para el Conocimiento madrid+d.

The main objective of the event is attracting students at all levels to STEM careers and introducing young talents to research and innovation.

Research assistants at the Institute used this opportunity to present some basic concepts of several areas of Computer Science through challenges, games and videos.

Video of full event

European Researchers' Night

Great Women Researchers on the "Big Screen"

November 27, 2020

Eleven researchers from the nearly 750 who work in the seven IMDEA Institutes participated in this activity, presenting the life and work of women who have stood out in the world of science, as much as to deserve to star in great film hits.

Eugenia Nieto, Mónica Echeverry, Marta Liras, Natalia Martín, Sofía de Oliveira, Arturo Azcorra, Silvia Sebastián, Elena Gutiérrez, Abraham Esteve and Ana Ramírez de Molina, with Manuel Carro acting as conductor, showed us that together with Marie Curie, in her own right, other feminine names should be written, with other personal and scientific feats as surprising as those of Emily Roebling, Rita Levi-Montalcini, Lise Meitner, Hedy Lamarr, Lisbeth Salander, Margaret Hamilton, Lynn Margulis or Margarita Salas.

Residencia de Estudiantes and virtual

5 researchers
(3 from the Institute)

175

undécima noche europea de los investigadores madrid

La Noche Europea de los Investigadores e Investigadoras de Madrid es un proyecto de divulgación científica, promovido por la Consejería de Ciencia, Universidades e Innovación y coordinado por la Fundación madri+d. Este proyecto está financiado por la Unión Europea dentro del Programa Horizonte 2020 de investigación e innovación, bajo el acuerdo de subvención número 953.820.

Residencia de Estudiantes

FECYT

Video summary

Photo gallery

Research and technology related events

IMDEA Software Institute

10 researchers (6 from the Institute

100

First IMDEA Software Tezos Blockchain Workshop

January 16, 2020

Following the signature of the collaboration agreement between the IMDEA Software Institute and Nomadic Labs, the Institute organized the 'First IMDEA Software Tezos Blockchain Workshop'. It had the participation of some of the best representatives of the Institute, Nomadic Labs, and the Tezos ecosystem.

Video summary

ChainrEaction Hackathon

February 3-5, 2020

ChainrEaction was the first hackathon organized by the IMDEA Software Institute and EIT Digital. Its topic was the use of blockchain technology to develop sustainable solutions for the digital cities of the future and slow down climate change. It was the first blockchain hackathon for environmental action in Spain. Organizing this event is part of the commitment of both organizations to supporting the United Nations Sustainable Development Goals (SDG).

The two main objectives of the three-day hackathon were:

- Bring students closer to research and innovation in the area of blockchain.
- Contribute to the creation of novel solutions for a more sustainable future.

The student groups presented their solutions to a committee for evaluation. There were awards granted in three categories and sponsored by the Tezos Foundation:

1. Most impressive proof of concept implementation.
2. Most viable pitch and business model.
3. Most surprising use of blockchain technology for environmental action.

They were given to the winners in a ceremony at the end of the hackathon.

IMDEA Software Institute

26 from 10 different countries

9

Tezos Foundation

web

Video playlist

Photo gallery


blockchain hackathon
for environmental action
#chainrEaction
chainrEaction


Who is in charge of distributing the donated items?
Why masks are left in warehouse while doctors are in need?
Do donators have to pay the Postage?
How can we guarantee the outcome?
How to motivate individuals? How can we link a value to a social cause and ensure that our incentive maximizes this cause


idea
software
chainrEaction


Comment
Join the conversation
Participate
Spread the word
Use hashtag

Reflections on blockchain

February 5, 2020

"Reflections on Blockchain at chainrEaction" was a public event that took place on February 5th, 2020, as a continuation of the ChainrEaction hackathon.

After a three day-long hackathon, it only seemed right to end with an event to present long-term visions for the evolution and future of blockchain technologies. Hackathon participants and general public (attendance was also open to anyone interested) had the opportunity to learn about different perspectives of this technology through keynote talks by international blockchain experts from industry and academia.

After the insightful talks, the chainrEaction jury announced the winners of the three prizes, who collected their trophies and pitched their winning ideas to the public.

IMDEA Software Institute

100

6

Video summary

Photo gallery


winner
chainrEaction
blockchain hackathon for environmental action
3-5FEB2020
Tezos Foundation
Most surprising use of blockchain
1.500,00 # €
TRIPPIO


idea
software


chainrEaction


winner
chainrEaction
blockchain hackathon for environmental action
3-5FEB2020
Tezos Foundation
Most impressive proof of concept
1.500,00 # €


winner
chainrEaction
blockchain hackathon for environmental action
3-5FEB2020
Tezos Foundation
Most viable pitch and business model
1.500,00 # €
ENERGYCHAIN

REDIMadrid

October 20, 2020

Virtual event
80
11

Since its creation, REDIMadrid has been holding an annual workshop that works as a meeting point to share experiences among researchers and industry representatives on the use of advanced networks in their projects. Practitioners from the Madrid Region and elsewhere were invited to submit and, if selected, present their experiences on the use of the facilities offered by REDIMadrid and similar organizations.

This edition was held online due to the COVID-19 pandemia, but it notwithstanding allowed connected users to share experiences and broaden their knowledge on the use of REDIMadrid and related networks. It completely fulfilled its goals and served to exchange ideas and experiences on the application of network technologies, as well as proposals for new R&D activities centered on the network, its development, and its expansion.

Video of full event

Media impacts

The following is a selection of the greatest impacts on the Spanish media during 2020.

EL PAÍS

LA CRISIS DEL CORONAVIRUS ›

La guerra de la app de rastreo del virus: investigadores y gobiernos europeos compiten por su opción

Más de 300 académicos de todo el mundo firman una carta "preocupados" por la posible deriva hacia una "vigilancia sin precedentes" de la sociedad

servimedia
LÍDER EN INFORMACIÓN SOCIAL

CORONAVIRUS

BBVA y el Instituto Imdea Software se unen para desarrollar técnicas de criptografía avanzada

04 MAYO 2020 | 11:42H | MADRID

sinc
La ciencia es noticia

INNOVACIÓN

Manuel Carro, experto en 'apps' de rastreo de la COVID-19

"Las aplicaciones para detectar contagios son un experimento que vale la pena probar"

Ni panacea ni amenaza para la privacidad: las aplicaciones de seguimiento de interacciones, bien utilizadas, serán un complemento a los rastreadores humanos, según defiende el director del Instituto IMDEA Software. Este profesor de Informática en la UPM explica por qué están tardando en desarrollarse. "Quizá de haberlo hecho antes tendríamos menos rebrotes ahora", dice.

radio 5 rne

europa press

Google Play es responsable del 67% de instalaciones de apps maliciosas de Android

TeleMadrid

Home Semana de la Ciencia

Diez investigaciones "made in Madrid" de las que está pendiente todo el planeta ciencia

annual report 2020

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