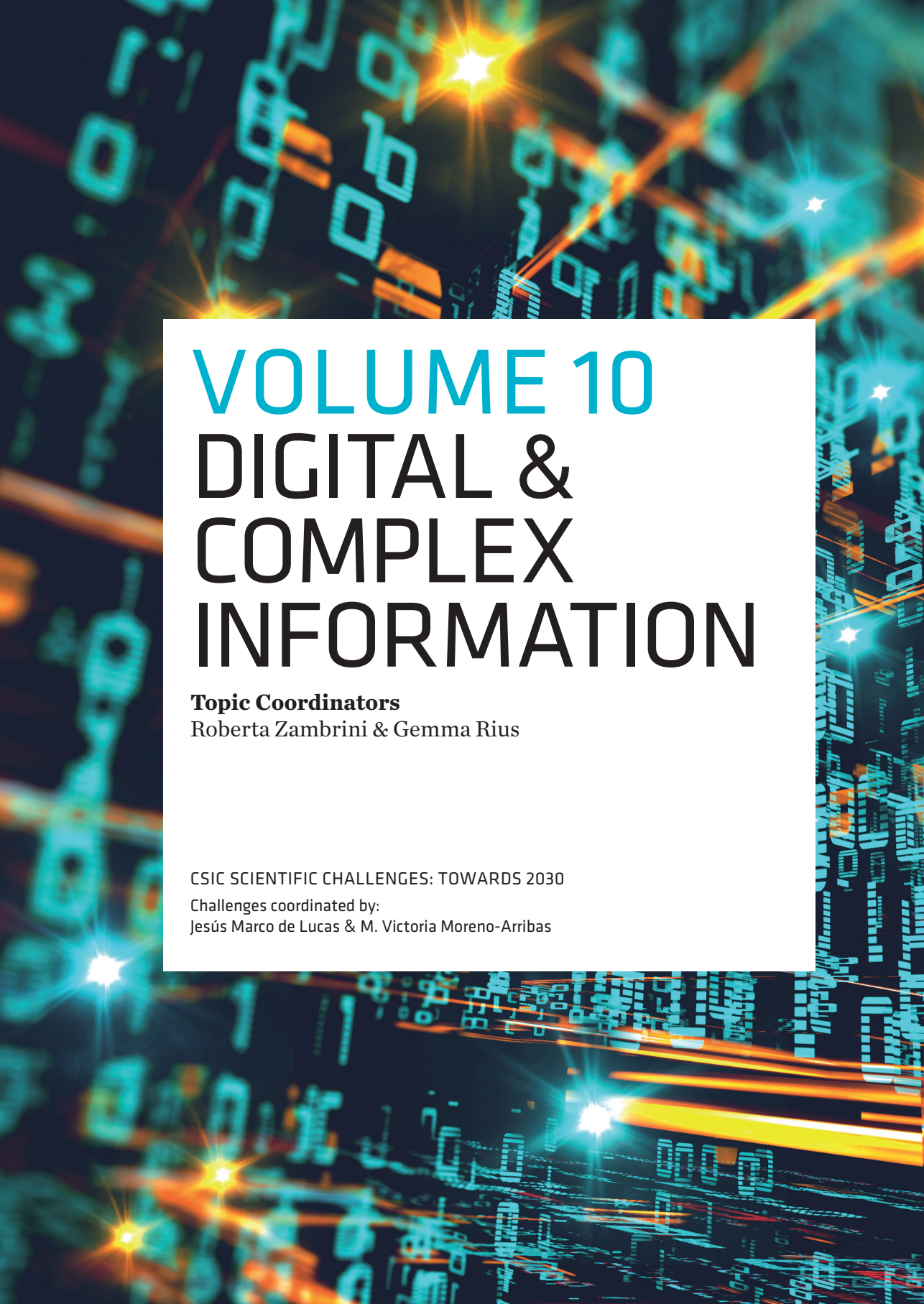


VOLUME 10
DIGITAL & COMPLEX INFORMATION

Topic Coordinators
Roberta Zambrini & Gemma Rius

CSIC SCIENTIFIC CHALLENGES: TOWARDS 2030
Challenges coordinated by:
Jesús Marco de Lucas & M. Victoria Moreno-Arribas

VOLUME 10

DIGITAL & COMPLEX INFORMATION

Catálogo de publicaciones de la Administración General del Estado:
https://cpage.mpr.gob.es

Editorial CSIC:
http://editorial.csic.es (correo: *publ@csic.es*)

ISBN Vol. 10: 978-84-00-10756-7
ISBN O.C.: 978-84-00-10736-9
e-ISBN Vol. 10: 978-84-00-10757-4
e-ISBN O.C.: 978-84-00-10734-5
NIPO: 833-21-140-5
e-NIPO: 833-21-137-1
DL: M-2426-2021

Diseño y maquetación: gráfica futura

CSIC SCIENTIFIC CHALLENGES: TOWARDS 2030

VOLUME 10
DIGITAL & COMPLEX INFORMATION

Topic Coordinators
Roberta Zambrini & Gemma Rius

CSIC SCIENTIFIC CHALLENGES: TOWARDS 2030

What are the major scientific challenges of the first half of the 21st century? Can we establish the priorities for the future? How should the scientific community tackle them?

This book presents the reflections of the Spanish National Research Council (CSIC) on 14 strategic themes established on the basis of their scientific impact and social importance.

Fundamental questions are addressed, including the origin of life, the exploration of the universe, artificial intelligence, the development of clean, safe and efficient energy or the understanding of brain function. The document identifies complex challenges in areas such as health and social sciences and the selected strategic themes cover both basic issues and potential applications of knowledge. Nearly 1,100 researchers from more than 100 CSIC centres and other institutions (public research organisations, universities, etc.) have participated in this analysis. All agree on the need for a multidisciplinary approach and the promotion of collaborative research to enable the implementation of ambitious projects focused on specific topics.

These 14 "White Papers", designed to serve as a frame of reference for the development of the institution's scientific strategy, will provide an insight into the research currently being accomplished at the CSIC, and at the same time, build a global vision of what will be the key scientific challenges over the next decade.

VOLUMES THAT MAKE UP THE WORK

1 *New Foundations for a Sustainable Global Society*
2 *Origins, (Co)Evolution, Diversity and Synthesis of Life*
3 *Genome & Epigenetics*
4 *Challenges in Biomedicine and Health*
5 *Brain, Mind & Behaviour*
6 *Sustainable Primary Production*
7 *Global Change Impacts*
8 *Clean, Safe and Efficient Energy*
9 *Understanding the Basic Components of the Universe, its Structure and Evolution*
10 *Digital and Complex Information*
11 *Artificial Intelligence, Robotics and Data Science*
12 *Our Future? Space, Colonization and Exploration*
13 *Ocean Science Challenges for 2030*
14 *Dynamic Earth: Probing the Past, Preparing for the Future*

CSIC scientific challenges: towards 2030
Challenges coordinated by:
Jesús Marco de Lucas & M. Victoria Moreno-Arribas

Volume 10
Digital & Complex Information

Topic Coordinators
Roberta Zambrini (IFISC, CSIC – UIB) and Gemma Rius (IMB-CNM, CSIC)

Challenges Coordinators
Agnès Ponsati (URICI, CSIC), Alberto Corsín Jiménez (ILLA, CSIC), Antonio Lafuente (IH, CSIC), Astrid Wagner (IFS, CSIC), David Zueco (ICMA, CSIC-UNIZAR), Diego Porras (IFF, CSIC), Fernando Aguilar (IFCA, CSIC-UC), Gabriela Cembrano (IRII, CSIC-UPC), Javier Aizpurua Iriazabal (CFM, CSIC), Joan Bausells (IMB-CNM, CSIC), Judith Farré (ILLA, CSIC), Luis Hernández Encinas (ITEFI, CSIC), Miguel Cornelles Soriano (IFISC, CSIC-UIB), Óscar Martínez Graullera (ITEFI, CSIC), Ricardo Martínez Martínez (IMB-CNM, CSIC) and Rodolfo Haber (CAR, CSIC-UPM)

Participant CSIC-Centers
Centro de Astrobiología (CAB, CSIC-INTA)
Centro de Automática y Robótica (CAR, CSIC-UPM)
Centro Nacional de Investigaciones Metalúrgicas (CENIM, CSIC)
Centro de Física de Materiales (CFM, CSIC-UPV/EHU)
Instituto de Instrumentación para Imagen Molecular (I3M, CSIC-UPV)
Instituto de Astrofísica de Andalucía (IAA, CSIC)
Instituto de Análisis Económico (IAE, CSIC)
Instituto de Agricultura Sostenible (IAS, CSIC)
Instituto de Agroquímica y Tecnología de Alimentos (IATA, CSIC)
Instituto de Nanociencia y Materiales de Aragón (INMA, CSIC)
Instituto de Ciencia de Materiales de Barcelona (ICMAB, CSIC)
Instituto de Ciencias Matemáticas (ICMAT, CSIC-UCM-UAM-UC3M)
Instituto de Ciencia de Materiales de Madrid (ICMM, CSIC)
Instituto de Ciencia de Materiales de Sevilla (ICMS, CSIC-US)
Centro de Investigación en Nanociencia y Nanotecnología (ICN2, CSIC-UAB-Generalitat-Fundación)
Instituto de Economía, Geografía y Demografía (IEGD, CSIC)
Instituto de Estructura de la Materia (IEM, CSIC)
Instituto de Física de Cantabria (IFCA, CSIC-UC)
Instituto de Física Fundamental (IFF, CSIC)
Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC, CSIC-UIB)
Instituto de Filosofía (IFS, CSIC)
Instituto de Historia (IH)
Instituto de Investigación en Inteligencia Artificial (IIIA, CSIC)
Instituto de Lenguas y Culturas del Mediterráneo y Oriente Próximo (ILC, CSIC)
Instituto de Lengua, Literatura y Antropología (ILLA, CSIC)
Instituto de Microelectrónica de Barcelona (IMB-CNM, CSIC)
Institución Milá y Fontanals (IMF, CSIC)
Instituto de de Micro y Nanotech de Madrid (IMN-CNM, CSIC)
Instituto de Microelectrónica de Sevilla (IMSE-CNM, CSIC-US)
Instituto de Ciencias del Patrimonio (INCIPIT, CSIC)
Instituto de Gestión de la Innovación y del Conocimiento (INGENIO, CSIC-UPV)
Instituto de Óptica Daza de Valdés (IO, CSIC)
Instituto de Políticas y Bienes Públicos (IPP, CSIC)
Instituto de Química Física Rocasolano (IQFR, CSIC)
Instituto de Robótica e Informática Industrial (IRII, CSIC-UPC)
Instituto de Tecnologías Físicas y de la Información Leonardo Torres Quevedo (ITEFI, CSIC)
Unidad de Recursos de Información Científica para la Investigación (URICI, CSIC)
Unidad de Sistemas de Información Geográfica del Centro de Ciencias Humanas y Sociales (USIG-CCHS, CSIC)

VOLUME 10 **SUMMARY**

ABSTRACT

Information, gathered, stored, processed and transmitted, is the cornerstone of the present era and shapes every aspect our daily life, thus permeating cultural and social deep changes. A multi and cross-disciplinary approach is needed to cover all present challenges of the Information Age, ranging from both the more technological aspects to the social ones. This duality is reflected in the title of this volume, Digital and Complex Information. The current Digital Transformation is enabled by developments in physics and engineering and entails several fields including electronics, optics, material science, and quantum technologies. Nowadays challenges include sustainable and energy efficient electronics, integrated photonics with new functionalities, quantum computing and machine learning, and operation within the Internet of Things. Nonetheless the Digital world generates an ever-increasing amount of data in which security and trust play a critical role. The advances in digital technologies call for a new scientific research approach: an Open Science, reproducible, interoperable and accessible. New avenues are open in how we deal with Humanities and with individual/social security and rights, within digital citizenship. This is the broad spectrum of challenges that drives research across about the 40 CSIC institutes in line with the latest developments in digitalization worldwide.

CHALLENGE 5

ABSTRACT

The popularization of Internet has meant a disruptive change in our way of life: from our social and professional activities to the mechanisms for generating and exchanging information. Despite this being generally beneficial, it has also implied an increased number of risks and threats from a security and privacy point of view. One of the great challenges of our society is the generation of trust and security in the management of digital information that we share and use daily.

KEYWORDS

confidentiality, integrity and availability of information and data

hardware devices | internet of things

lightweight cryptography

microelectronics developments of secure computing systems

post-quantum cryptography

quantum computing

quantum key distribution | RISC-V

secure computation

trustworthy and secure digital society

CHALLENGE 5

TRUST AND SECURITY IN THE DIGITAL INFORMATION

Coordinators

Luis Hernández Encinas
(ITEFI, CSIC, Coordinator)

Ricardo Martínez Martínez
(IMB-CNM, CSIC, Adjunct Coordinator)

Participant researchers and centers

Iluminada Baturone Castillo
(IMSE-CNM, CSIC-US)

Verónica Fernández Mármol
(ITEFI, CSIC)

Agustín Martín Muñoz
(ITEFI, CSIC)

Santiago Sánchez Solano
(IMSE-CNM, CSIC – US)

Lluis Terés Terés
(IMB-CNM, CSIC)

1. EXECUTIVE SUMMARY

The exponential deployment and popularization of Internet access (the so-called democratization of Internet access) facilitated by the proliferation of the technological devices with connecting capabilities, has driven to the growth of the cyberspace, which has changed our society dramatically. Although this change has provided a large number of benefits, it has also generated a number of risks and threats that often go unnoticed. An obvious challenge would be minimizing such risks and threats through scientific research in order to improve the security of the digital information, thus contributing to enhance users' trust in the digital society.

Research will be carried out on the design of methods for ensuring the confidentiality, integrity and availability of information, as transversal requirements for digital security. Key challenging points are identified regarding the storage of data, the communication of information over networks, and the processing of data on hardware devices. To secure the storage of data, cryptographic protocols and algorithms will be developed taking into account fundamental aspects of authentication, lightweight cryptography and post-quantum cryptography. To guarantee the security of communications over networks, dodging the threat of quantum computing, quantum key distribution will be improved by means of new protocols and technological developments. For the secure processing of data on hardware devices,

microelectronics developments of secure computing systems and hardware roots of trust will be investigated, looking for a European technological sovereignty.

Addressing this challenge and achieving its goals will ensure that digital applications will be used in a trustworthy and secure way.

The experience and previous achievements of the groups involved in this challenge show their ability to succeed in reaching results which will contribute to the progress of basic science, and to the development of new technologies and novel applications which will have a remarkable impact in many aspects of our society.

2. INTRODUCTION AND GENERAL DESCRIPTION

This chapter, in short, tries to contribute to the promotion of a trustworthy and secure digital society, considering the technological aspects of risks and threats and moreover, understanding their repercussions on the uses and actions of citizens. Information security is needed to preserve the defense of constitutional and democratic values, the citizens' fundamental rights, their personal data and its relation to General Data Protection Regulation, etc., and requires a multidisciplinary approach. In fact, digital security constitutes one of the main challenges of our society, which is not only the information society, but also the *data society*. The later term comes from the massive use of devices, which are continuously and ubiquitously connected to the Internet.

Along this chapter, the terms *trust*, *trustworthy*, and *trustworthiness* describe something which a person can believe in, that is, something that is completely reliable. Properties that something trustworthy must possess are: authenticity, accuracy, consistency, integrity, etc. The concept of *security* is typically applied referred to acts of an intentional nature. Security-related risks are often related to the actions of an intentional opponent or attacker, such as sabotage, theft, or other explicit attacks. This term also applies to something that is protected and resilient against failures or errors, malfunctions, whether caused or not.

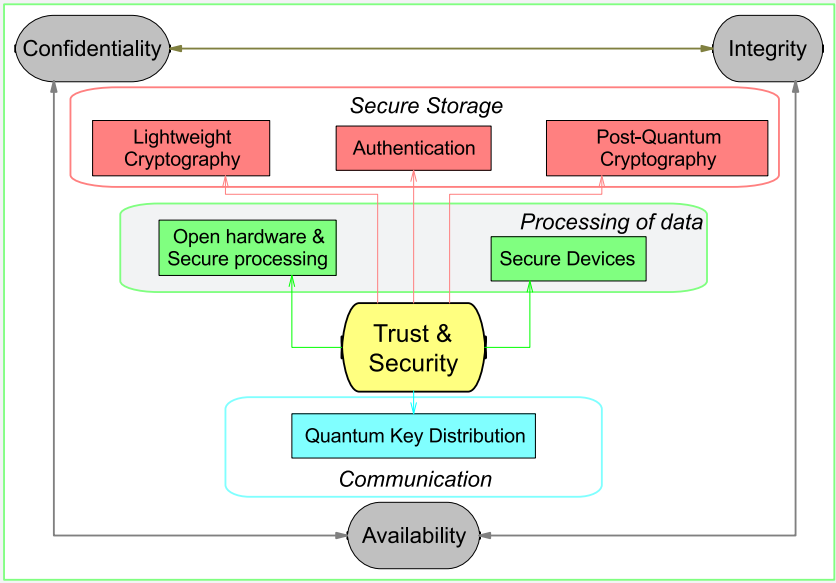
Reports issued by relevant authorities, such as the National –Spanish– Security Strategy [Gobierno de España, 2017], the Annual National –Spanish– Security Report, the European Security Strategy [European Council, 2009], the NIS (Network and Information Systems) Directive [European Union, 2020],

the Cybersecurity Act [European Union (b), 2020] from the European Union, and the Horizon Europe Cluster about Civil Security for Society, as well as the Digital Europe Program, stress the role of *Information Security* as a priority objective to ensure national security and create a *Trust-based digital society*. There are also of interest the international calls made by the National Institute of Standards and Technology (NIST) from USA. These calls are aimed to foster research to find new cryptographic algorithms, primitives and protocols which can contribute to improve the trustworthiness and security of digital information. Among them, it is worth to mention those related to the lightweight cryptography and the post-quantum cryptography.

Ensuring the **confidentiality, integrity and availability (CIA) of information and data**, either transmitted by networks or processed and stored in electronic devices (computers, smartphones, etc.) is nowadays a strong challenge, since users, organizations and companies must be sure that such assets are always available and cannot be accessed or modified by other entities or even by malicious users without the corresponding permission. In order to achieve this challenge and to reach the transversal objective of ensuring CIA of information and data (see Figure 5.1) by the design and implementation of cryptographic protocols and secure applications (transparent to the entities), three types of actions can be developed capable of ensuring: 1) Secure storage of data (authentication, lightweight cryptography and post-quantum cryptography), 2) Quantum safe communications (quantum key distribution), and 3) Secure processing of data on hardware devices (secure devices, open hardware, etc.). The benefits of such actions will permit to protect the entities from many threats and weaknesses like the (massive) password theft, phishing, ransomware and other malware attacks, and to provide to the users a real trustability in the management of digital information, methods for a secure generation of keys, and trusted hardware executing trustworthy computation.

The **protection of store data** can be addressed by considering several aspects related to the improvement of cryptographic protocols and algorithms. In this sense, *authentication* is a property of information security that allows users to confirm their identities and those of their devices, and thus avoids impersonation attacks by which impostors assume the identity of legitimate users. Moreover, *lightweight cryptography* addresses the security demands in resource-constrained hardware and software scenarios such as sensor networks, RFID tags, smart-home appliances and mainly Internet of Things (IoT)

FIGURE 5.1–Challenges for obtaining Trust & Security of data



devices. Lightweight cryptography denotes a wide range of cryptographic algorithms with different properties and diverse use cases. In fact, the only unifying constraint of all of them is the low computing power of the devices intended to run them. Under such conditions, specially designed algorithms are necessary. *Post-quantum cryptography (PQC)* refers to the design and implementation of new cryptographic protocols and algorithms which can be considered secure against the power of the quantum computation. The threat of quantum computing, in terms of security, is the possibility that in the medium-to-long term a universal quantum computer with sufficient computing capacity will be ready as to implement quantum algorithms capable of breaking the cryptographic algorithms currently used. The PQC concept was born after the publication of several quantum algorithms (Shor, Grover and Simon algorithms, mainly), which will break the main symmetric and asymmetric cryptosystems used today, if a quantum computer with sufficient computing capacity is developed. Indeed, the mathematical problems on which their security is based (integer factorization and discrete logarithms in the case of asymmetric cryptosystems) could be solved in just a few hours.

Quantum safe communications The aforementioned quantum computing threat is being considered internationally by agencies and governing bodies. It is therefore mandatory, in order to fulfil the national and international security agendas, to continuously evaluate the risks associated with the irruption of said technology, and to study alternatives to make the exchange of information feasible through confidential and secure channels capable of providing quantum safe communications to the general public. In this sense, it is worth to mention the *Quantum Key Distribution (QKD)*, a quantum technology that uses the principles and tools of Quantum Mechanics for the secure exchange of information. This is of enormous importance in information security since it enables the sharing of cryptographic keys among users with information-theoretic security, i.e., with security independent of the computational power of an adversary. It is therefore secure against a quantum computer attack and hence, the name quantum-safe.

In relation to the **Processing of data on hardware devices**, it is clear that microelectronics plays a fundamental role in the context of trust and security in digital data, both for being the Key Enabling Technology for the construction of the information processing and transmission elements that support cryptographic protocols executed in software, and for being increasingly used for *hardware implementation of specific devices* that allow to improve performance and security of the device itself, and reduce size and energy consumption of cryptosystems. Secure interconnection of devices and systems in different application domains is an open research challenge. So, new microelectronic solutions must be explored in order to provide efficient mechanisms to verify the identity of hardware devices and users, as well as to establish hardware roots of trust to store, communicate, and process sensitive information. Moreover, it is also necessary to ensure the security of devices against side-channel implementation attacks, particularly fault injection and power analysis attacks, and to develop countermeasures that allow implementing components and algorithms providing security together with efficient features of size, power consumption and operation speed.

Another aspect pertaining to security is the necessity of obtaining the European sovereignty in all aspects related to the development of trusted and secure technology, in particular, in the *development of secure computing systems*. In this sense, the challenge is to increase the technological autonomy by promoting a national (and European) industrial base of cybersecurity, R&D&I and the management of technological talent (European and National

–Spanish– Cybersecurity Strategy [European Commission, 2013]). Europe is technologically vulnerable due to the lack of control in the main technologies that process digital and complex information. These uncovered technologies range from advanced nanometric technologies to the design of complex digital intellectual property blocks and processor cores. The challenge is being able to reduce this gap through the concept of trusted chips creating the necessary hardware blocks needed to ensure the chip authenticity and the support of cryptographic algorithms based on open and known Hw/Sw processing systems.

3. IMPACT IN BASIC SCIENCE PANORAMA AND POTENTIAL APPLICATIONS

The research needed for securing digital information and for reaching users' trust on the technology and applications will produce a relevant impact in both basic science panorama and worldwide economy, and will lead to the development of applications which will have a strong social impact. Some examples of this technology and applications are: protection of citizens' personal information; biometric recognition of citizens; new materials, components and developments for the construction of hardware devices and photonic; generalization and implementations of remote e-voting systems, etc. A more detailed explanation about the impact of this challenge is provided in the following paragraphs.

In relation to the transversal objective associated to *CIA of stored and transmitted information*, the design and development of new protocols and algorithms will obviously impact in many fields of science and technology, since the management of information is more and more a requirement in complex systems and advanced applications. The historical evolution of cryptography, as a basic tool related to trust and security, teaches us, among other things, that after some (supposed) secure algorithms are proposed and accepted for their use, the researchers study such algorithms with the goal to develop new attacks. When some weaknesses have been found, modifications of the accepted algorithms or new algorithms must be developed. With this perspective in mind, it is not easy to determine what topics will have an impact in the short and medium term or in the long term. Taking into account that achieving trust and security in digital data is a *very long-distance race*, most of all topics can be considered as long-term challenges, though some of them (as, for example several algorithms) could produce results with impact in the short or medium term.

One of the main impacts that this challenge will have is the protection of citizens' personal information in a way that avoids the traceability of their movements and the knowledge of their interests and hobbies, the safeguards their medical data from access by unauthorized third parties, the right to be forgotten on the Internet, etc. Protecting the information managed in everyday commercial and industrial activities will have an strong impact in the economy of any country, since corporate espionage and global threats will be avoided or mitigated allowing the proper development of banking, pharmaceutical, telecommunication companies, etc., as well as the correct functioning of critical infrastructures and services as security forces and bodies, nuclear, electrical and gas installations, transportation systems, hospitals, etc. Here, the development of post-quantum cryptography will have an important impact in the proposal of new security protocols. To get such impact, new algorithms based on specific mathematical problems will be needed, such as considered in the PQC call by the NIST: lattices, error correcting codes, multivariate quadratic polynomials, isogenies over elliptic curves, hashes, etc. Most of its results should be in the short-medium term since the objective is to protect the information against the quantum threat.

Another great impact of this challenge will be a relevant improvement of the biometric recognition of citizens. This type of recognition is widespread in certain areas and is usually used by the security forces to identify users or to access to certain buildings or parts of them. The improvements in biometric recognition techniques will have a clear economic and social impact, in a short-medium term, since they will allow the access to personal or private data only to those who have the right to know it. The owner of the data will be able to access such data without employing intrusive methods, the access grant being completely transparent to the user. Health authorities and state security agencies, etc. will also have access to this data. The new results of biometrics will impact on the used today features and traits for identifying users. Thus, in addition to use fingerprints, irises, voice, hand and vein geometry, etc., for which it will be necessary to improve their efficiency and effectiveness, in a short-medium term new identification features will be proposed; especially those based on the sensors of the smart devices like gyroscope, GPS, accelerometer, etc. These improvements will allow, in a long term, the use of personal devices with added guarantee of privacy, not only in the phase of access or initiation of such devices, but also through continuous authentication protocols that guarantee that whoever is using it at all times is its legitimate owner. An important impact of these new results related to biometry will be guaranteeing the safety and security of

implantable medical devices (IMD). So, it would be possible to avoid attacks of an adversary for knowing the possible illness of a sick person (which is against your privacy) and, furthermore, to prevent someone from manipulating such IMD by altering the dose of the insulin pump, the pace of a pacemaker, etc.

This challenge will also have an impact on certain aspects related to digital citizenship (Chapter 8) such as electronic voting (e-voting). It is about generalizing the democratic uses of all citizens in electoral processes. This is another one of those issues for which solutions are known, but none of them, at the moment, offer enough security to be implemented in a generalized and efficient way. E-voting proposals will allow secure voting though Internet by using any mobile device (laptop, smartphone, tablet, etc.) and, at the same time, consider the possibility that each citizen may vote several times in the same electoral process as a possible measure to avoid coercion when exercising the right to vote. It must be considered that e-voting requires very special characteristics, which go beyond the vote cast in a ballot box. It is about guaranteeing that, as usual, only registered voters can vote, that the vote must be cast freely, be valid, be secret and recorded in the option chosen by the voter; but in addition, it is required that each voter, at the end of the process, be able to verify that his vote was accounted for the option he chose, maintaining the confidentiality of the vote at all times.

Improving security and increasing trustworthiness in new technologies will impact, in a short-medium term, in the development and generalization of IoT devices.

Moreover, their applications will be closer to the users and their popularity will be increased even more. At the same time, these improvements, will extend in a long term, their use in fields such as home automation, smart cities, smart meters, etc. It is a widely accepted fact that IoT devices were not designed with their security in mind. In this sense, the development of lightweight cryptographic algorithms will provide a bigger security to IoT devices (see Chapter 4). These developments will take into account their limited computation and storage capabilities.

Another aspect on which this challenge will have a great impact will be the development of international standards, in a short-medium term, in each and every one of the aspects considered so far. This will guarantee that the new developments will be compatible, available and interoperable at international level with an obvious positive economic impact.

Regarding Quantum Safe Communications, the expected short-term impact is extending the operability of current QKD systems to the demands of communication networks, which implies longer range, higher speeds and lower deployment costs. Consequently, the expected impact will be a wider use of these technologies by the society in general, governments, corporations, banks, defense sectors, etc. Security risks will thus be reduced and therefore, will not expose sensitive information from these sectors, which will have a positive effect on the economy. Moreover, secure interconnection of QKD nodes independently of their nature will impact in the applied science, in a medium term. Specifically, the development of hybrid networks where free-space and optical fiber QKD links coexist, will increase the flexibility and versatility of these networks and will better address the user needs. On the other hand, wireless networks are proliferating with the increasing use of smartphones, drones, autonomous cars, etc. Adequate confidentiality of these channels is mandatory, in the short term, to ensure the user's information. For this matter, the development of efficient free-space to optical fiber interfaces capable of counteracting atmospheric effects and relative movement is necessary. These solutions, which require, not only technological advances, but also increased knowledge of theoretical aspects, such as atmospheric turbulence and beam propagation, will also impact basic science.

Regarding longer-term impacts of quantum safe communications, within basic and applied science, are the development of QKD applications, including space applications that will enable long-distance ultra-secure links. This will benefit citizens and governments, as their data could be secure globally. Exploring the development of different types of QKD protocols better suited to different applications (whether the channel is free space or optical fiber, requires a high or lower bandwidth connection, it is mobile or stationary), will impact the society by providing a better choice to the users' needs. In addition, the development of the Quantum Communications Infrastructure (QCI) will allow public use of confidential channels to protect user's sensitive information. Potential applications will include the use of these links for critical infrastructures such as the energy, transport, telecommunications or water supply networks. In this sense, the foreseen impact will include the development of new solutions suitable to be deployed in this infrastructure, such as robust, compact and cost-effective systems, that could be easily integrated in standard technology; along with new hybrid encryption schemes including quantum and non-quantum cryptographic primitives.

The use of secure devices and secure computing systems in different application domains will impact in the applied science, in a short-term. For example, the efficient hardware implementations of circuitry for security, i.e., symmetric, asymmetric and post-quantum and lightweight cryptographic and biometric algorithms as well as primitives like ciphers, hash functions, etc., will spread the range of devices that are secure currently to cover wearable and implantable devices. The new microelectronic solutions will provide efficient mechanisms to verify the identity of hardware devices and users, as well as to establish hardware roots of trust to store and communicate sensitive information. Furthermore, the new results will ensure the security of devices against attacks to the implementations of cryptosystems in physical devices, particularly fault injection and side-channel attacks, and that their security will remain over time in spite of aging. Detecting not only counterfeiting but also tampering, that is, that a legitimate device has been manipulated with the objective of carrying out an unauthorized operation, is crucial in many applications. In addition, the fraudulent copy of hardware designs must be avoided among other reasons by their important economic consequences. In this sense, it is demanded the development of white-box cryptography and code obfuscation. In summary, as the citizens need to use certified devices from a safety point of view, new metrics have to be proposed and new methodologies have to be developed to certify the embedded systems and programming techniques from a security point of view.

Our society demands transparency and secure computing systems should also be transparent. Hence, the generalization of Open Intellectual Properties (IPs) will have a big impact to grow the universe of fundamental blocks for its usage on an open hardware environment such as RISC-V, and independent verifications and benchmarking for RISC-V implementations or for any open-IP. The development of on-chip strategies and utilities will help, in a short-medium term, end users to protect the different levels of Hw/Sw from the core processor up to the application software (Physically Unclonable Functions or PUFs, cryptographic coprocessors or accelerators, etc.).

Spain, in particular, and Europe, in general, need to have a secure electronic technology which makes it possible the design and fabrication from System on Chips till microprocessors that enable the secure implementation of cryptosystems in the devices of our daily life. In this sense, it is fundamental to guarantee, in a long term, the growth of the open RISC-V ecosystem and its application in many different application domains, from High Performance

Computing to Ambient Intelligence, IoT, Edge Computing, etc. The efficient generation of tools for the very large scale integration (VLSI) circuit design as well as the implementation of secure systems and IP modules on FPGAS and ASICs are strategic for the electronic technology in Spain and Europe.

4. KEY CHALLENGING POINTS

Besides those related to military, diplomatic, and governmental, there are other environments where it is very important to protect the information and data. Some of them affect to institutions and their relationship with citizens. For example, the necessity of enhancing the security of the personal identification devices like passports, ID cards, etc., in order to avoid impersonation of identities (see Chapter 8). It is also evident the need of guaranteeing the secure communications between the companies and their clients (bank transactions, cloud computing, access to databases, IoT devices, etc.), as well as the security of IMD in order to avoid patient data theft, therapy manipulation, etc.

The best way to guarantee the transversal objective of **Confidentiality, Integrity and Availability of information and data** is to develop cryptographic protocols and algorithms which fulfill the security requirements established by the international organisms and associations. In fact, the development/evolution of our digital society requires to guarantee the CIA of the information managed, for example, in the contexts of smart cities (by smart meters or autonomous cars), or e-governance (electronic administration, remote electronic voting, etc.).

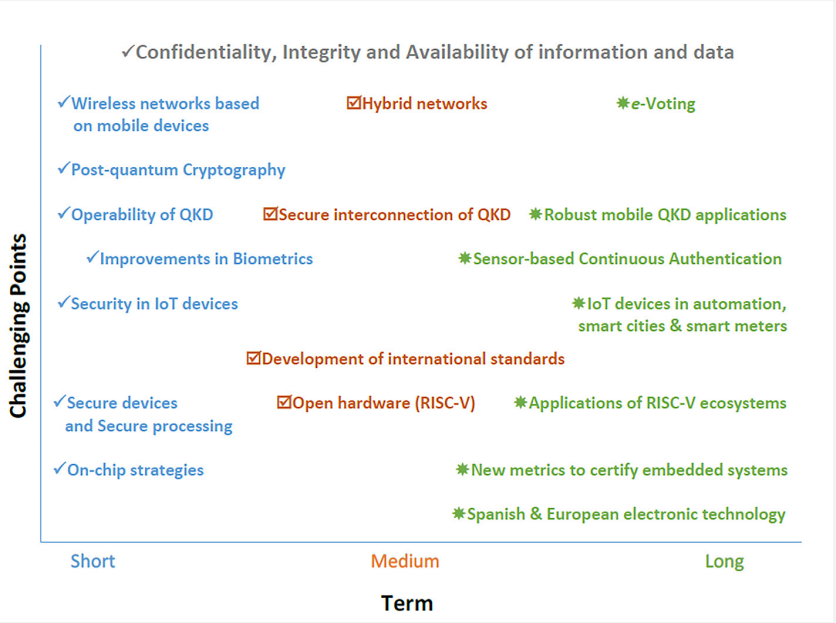
In the following, descriptions of the key challenging points to achieve effective trust and security in the digital information are provided. Figure 5.2 shows a scheme of the foreseen terms to achieve the different challenging points.

4.1. Guaranteeing secure data storage

Authentication

Several European regulations impose trust and security norms concerning the electronic identification of subjects making transactions within the European Economic Area: General Data Protection Regulation (GDPR, EU Regulation No. 679/2016), The Strong Customer Authentication (which came into force on September 2019), and U.S. regulations follow similar issues: Digital Identity Guidelines from NIST establish that the highest Authenticator

FIGURE 5.2–Timeline of the challenges by term



Assurance Level is based on a) proof of possession of a key through a cryptographic protocol, and b) use of a hardware-based authenticator and an authenticator that provide verifier impersonation resistance by using biometrics. In order to be authenticated, claimants shall prove possession and control of two distinct authentication factors using approved cryptographic techniques. Moreover, many applications require that genuine individuals prove with their physical presence that they are associated with the origin and storage of information. In this sense, Biometrics authenticates the physical presence of the user through physical features (fingerprint, iris, etc.), physiological characteristics (heart or brain signals, etc.) or behavioral traits (gait, handwritten signatures, etc.).

The adequate combination of cryptographic and biometric techniques into crypto-biometric systems is demanded not only by economic applications but also for e-health, e-government, e-learning, digital rights management, etc. Some of the tools to be improved for solving the identification of users based on the sensors of smart devices (gyroscope, accelerometer, etc.) and for

guaranteeing the safety of IMD, are those related to cryptography for encryption and user authentication, template protection, data storage, secure and multi-party computing, etc. The fusion of multiple sources of information (fingerprint, face, voice, etc.) is employed by multi-modal biometric systems to achieve higher performance in individual recognition. Implementations of crypto-biometric and multi-modal biometric systems into trusted hardware-based devices as well as the development of efficient template protection techniques are two challenges to be achieved.

In the case of e-voting, cryptographic protocols are necessary to be developed and improved, at least in security matters. Among other primitives, it is worth mentioning digital signature, homomorphic encryption, sharing of secrets, proofs of zero knowledge, etc. The new proposals in this aspect will improve the democratic aspects of our society and the interaction between citizens and administrations in a context of e-governance (see Chapter 8).

Lightweight cryptography

Lightweightness does not mean less security. The challenge in lightweight cryptography is to keep the same level of security as that of conventional cryptography but to perform it with lower resources. In fact, the topic is to achieve the best trade-off between security protection against attacks (avoiding vulnerabilities), cost (area, memory, energy) and performance (latency, throughput, power). Lightweight cryptography is currently split into ultra-lightweight cryptography (that provides one function with high performance on one platform) and ubiquitous cryptography (that is concerned with more versatile algorithms in terms of functionality or implementation). Low-cost IoT devices are not only characterized by their constraints in processing power, memory, chip size, and energy consumption but also by their minimal or non-existent security. Combining this lack of security with their network dependency, they become the perfect gateway to attack or compromise the whole network. It is thus obvious that developing new and more secure and efficient lightweight cryptoalgorithms is a key challenge regarding the storage of data. This is the reason why 5G technology deployment or specific calls such as that of NIST for lightweight cryptography address the topic of lightweight algorithm design.

Post-quantum cryptography

From a cryptographical point of view, the principal method to avoid the quantum computation threat is the development of the *post-quantum cryptography*, also referred to as quantum-resistant cryptography, i.e., the design and

implementation of robust cryptographic primitives, using Mathematics or Computer Science, against the quantum algorithms that threaten the security of cryptography as we know today.

Due to the quantum threat to the protection of information, the NIST has launched an international call to select new quantum-resistant cryptographic algorithms. Their security will be based on specific mathematical problems founded in lattices, error correction codes, quadratic multivariate polynomials, hashes, etc., so that this cryptography be invulnerable to quantum computers, no matter how much computing power they have. The key challenging points of PQC are to develop this type of algorithms and protocols in order to increase the security of the methods to be used for protecting the information in the post-quantum era.

4.2. Quantum-safe communications

Quantum key distribution

Quantum communications consist in the transport of quantum states from one location to another. This can be achieved through quantum communication protocols, such as Quantum Teleportation or QKD. The latter has an interesting application in information security since it enables the exchange of cryptographic keys with unconditional security. Quantum communications will take part in future quantum networks, where different quantum technologies will work in parallel. The end nodes, consisting of quantum processors, will perform certain computational tasks, and will be connected to each other by communication lines. These lines, or physical layer, will consist of optical fiber or free-space channels. In the final stage, quantum repeaters will extend communication over nodes to, in principle, arbitrary long distances.

Although all these technologies are experimenting great progress, the final horizon of a Quantum Internet remains a considerable challenge. Therefore, intermediate steps, outlined by the Quantum Technologies Flagship, are to be taken by European stakeholders to progressively advance towards the final goal. Initial stages of implementation of quantum networks will be through a trusted-node approach that may involve the use of satellites to reach long distances. Communication protocols will implement QKD using Quantum Random Number generators, which, in conjunction with the One Time Pad enable unconditional secure encryption. This approach suits well the protection of critical infrastructures, for instance, whose information is highly sensitive.

A practical case of a quantum communication network will presumably be the QCI, whose agreement was signed by sixteen European Union member states, including Spain, in 2019. The plan is to build a pan-European network with the mission of protecting Europe and its critical infrastructures from global cyber threats. Several European cities will be connected through QKD links by both ground and space-based transmission channels. In later stages, other cryptographic primitives such as authentication, digital signatures, and secret sharing protocols, are planned to be added to the network. These are key challenging points that require a hybrid approach to information security involving a classical and quantum perspective that the groups involved in this challenge can provide.

Other key challenging points remain increasing the range and speed, the robustness, integration, scalability, etc., of QKD systems. In this sense, through our expertise in fast free-space QKD and enabling technologies, we believe we are in position of tackling these challenges successfully. Other open questions in this field, that we are planning to study theoretically and experimentally, are novel protocols capable of closing security loopholes, such as Measurement Device Independent or Twin-Field protocols, novel technologies for polarization tracking in mobile platforms and continuous-variables QKD systems in free-space channels.

Finally, space QKD applications are also driving considerable interest of many research laboratories worldwide. Key challenging points remain inter-satellite quantum communications. Our previous experience and knowledge of experimental QKD protocols place us in a good position to tackle these issues in collaboration with other research institution specialized in space applications such as the National Institute of Aerospatiale Techniques (INTA).

4.3. Hardware devices for secure data processing

The advent of edge computer technology has led to the development of new Internet connected devices to support innovative and important services for citizens and industrial sectors. Most of these embedded systems, usually encompassed in the IoT paradigm, combine specific and general purpose processing elements that were developed without taking security aspects into consideration, which can seriously compromise their functionality and, therefore, their capability to lay the foundations of trust on which the future development of digital administration and electronic commerce should be based. The development of secure devices and secure processing systems will therefore constitute the two main topics that will be considered in this challenge.

Secure devices

Obtaining efficient hardware realizations of the primitives necessary to guarantee the trust and security in the processing and transmission of digital information, and ensuring that these implementations do not present vulnerabilities that can facilitate the execution of attacks by a possible adversary, are, regarding computation on hardware devices, two challenges that should be addressed in the coming years.

The new cryptographic schemes resulting from the standardization processes currently launched by NIST for lightweight and post-quantum cryptography will undoubtedly be the main candidates to attract the attention of cryptographic hardware designers in the short and medium term. In order to combine the high-performance provided by hardware and the flexibility of software implementations, many of these new security primitives will be developed following a Hw/Sw co-design methodology. This kind of hybrid realizations with enhanced security at both hardware and software levels will be also excellent platforms to evaluate possible vulnerabilities, as well as to explore hardware, software and mixed countermeasures during the design phase of a cryptographic system.

The massive use of devices connected to communication networks for the exchange of information among administrations, service providers and citizens, raises a number of open issues related to security. System hardware is the first link in the chain of trust that must be established to provide a secure environment for users. For this purpose, electronic devices must provide a Root of Trust (RoT) based on the confidence on their fabrication and resistant to device impersonation attacks. PUFs and True Random Number Generators (TRNGs) are the key components of a silicon-based RoT. PUFs have been used in recent years as a mechanism to provide unique and non-transferable identities to hardware devices. PUFs should be easily evaluable and repeatable functions so their associated hardware can prove its identity by repeating the function evaluation, whereas another identical device (a possible impostor) is not able to generate the correct output for the same input. PUFs must generate responses with sufficient entropy to not reveal device secret information. On the other hand, Silicon-based TRNGs, which use a source of entropy such as thermal noise to generate unpredictable and statistically uncorrelated sequences of bits that allow generating secure and unreproducible keys and challenges, are a must for trusted and secure implementations.

A reduction of entropy leads to system vulnerabilities. In this regard, a crucial issue is device aging due to different mechanisms (such as BTI-Bias Temperature Instability or HCI-Hot Carrier Injection), which degrade the performances of circuits over their lifetime, and therefore can seriously compromise security in hardware implementations. Furthermore, aging affects not only the PUF but also the other elements of the security chain. It is therefore essential to study and analyze the effects of aging on the whole security chain, paying particular attention to whether these effects are accumulative, and whether and how these effects can be mitigated when the security level is fatally compromised.

Most of the applications mentioned above which use cryptosystems (identification, authentication, digital signatures, etc.) are embedded in smart cards, smartphones, tablets, IoT devices, etc. Hence, many cryptographic devices are physically reachable and might be within adversary's grasp. Regarding this fact, the challenge to be faced is twofold: on the one hand, improving attack techniques (leakage detection, higher-order attacks and protection circuit edition), which will allow improved security evaluations of the devices that citizens will use; on the other, to design new countermeasures capable of guaranteeing that the devices are resilient against increasingly sophisticated attacks. Examples of such countermeasures can be the automatic logic power balancing, the generation of passive and active top metal shielding to prevent focused ion beam circuit edition and microprobing, the integration of light sensors for the detection of die decapsulation, substrate thickness monitoring to identify possible backside attacks, passive layout camouflage based on near-equal layout gate libraries, active hardware obfuscation by means of synthesizing dummy finite-state machines, physical redundancy of protection flags, etc.

Secure processing

As mentioned above, besides secure transmission and storage of information, digital information origin should be authenticated. Avoiding counterfeiting is very important because fake devices do not meet usually the required quality provided by legitimate devices and can be the trapdoor for espionage. In addition, the European technological dependence on companies outside Europe affects many aspects of our digital society as most devices used by citizens every day (smartphones, tablets, smartcards, etc.) employ a technology closed under the control of a few number of non-European companies.

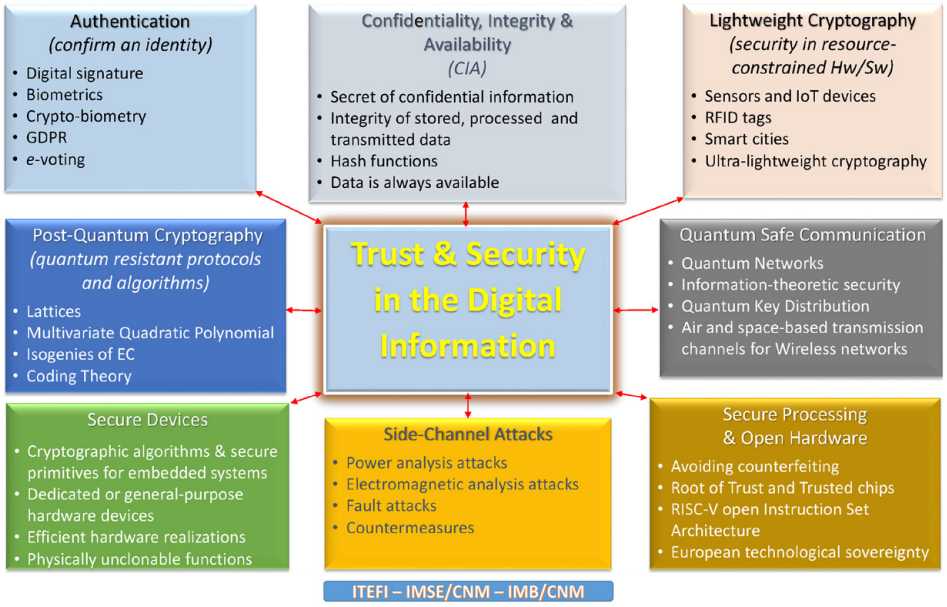
The EU has financed (with around 80M euros), the EPI project within a program that has the heading "H2020-EU.2.1.1.2. – Next generation computing: Advanced and secure computing systems and technologies, including cloud computing". This project has as one of its missions "Developing the first generation of technologies through a co-design approach (IPs for general-purpose High-Power Computation or HPC processors, for accelerators, for trusted chips, software stacks and boards)".

In this sense, "trusted chip" is the keyword and it is evident that Europe, and Spain in particular, need a certain level of technological control that they do not currently have. This challenge is not only the design of a European processor but also includes topics ranging from secure communications protocols that cover the entire range of applications, from broadband to IoT, until the control of manufacturing technologies. However, even in the case of fully European secure computing systems, there is still the need for auditing such a "trusted chip" to detect possible hardware trojans introduced either at the design house or at the semiconductor foundry. Hence, the second challenge here is the automated reverse engineering of full IC designs containing hundreds of thousands of equivalent gates. This hardware trust and assurance verification at chip level requires the physical extraction of the entire mask design and the bottom-up analysis of the resulting layout up to the architectural and functional description levels of the full chip.

Security by obscurity is discouraged and not recommended by standards bodies since the last century. Open technology is preferred. A possible solution to this situation is the RISC-V ISA (Instruction Set Architecture), which is free of royalties for any company and can mimic the path initiated by Linux years ago. In deep, the EU has chosen this architecture as a reference for the future European microprocessors. In fact, it is expected that this RISC-V open ISA will help to start and grow the open-hardware developments and market as happened years ago with Linux open operating system, which ten years later resulted in a large community of open software developers while reducing the costs of software developments. The RISC-V Foundation includes the Security Standing Committee to agree in the best security practices and include them in RISC-V based implementations. Nowadays, academic and industrial sectors are working on developing from cryptographic IP modules to complete Trusted Execution environments based on RISC-V. In addition, in order to have "compliant" RISC-V devices, a complete set of standard compliance test cases, methods and tools have to be provided to the developers allowing the detection of possible errors, security flaws or backdoors.

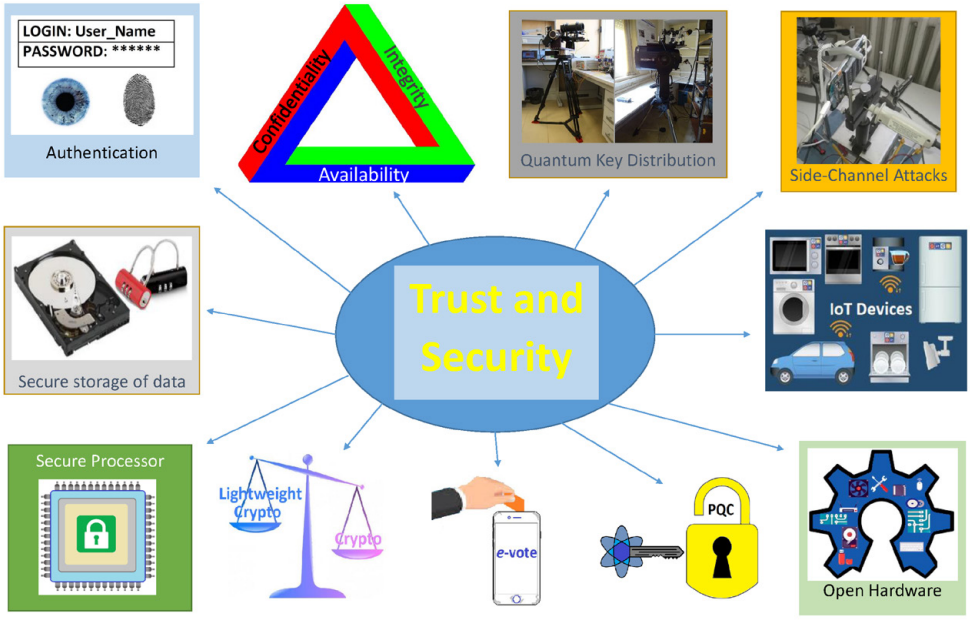
ANNEX: ONE SLIDE SUMMARY FOR EXPERTS

FIGURE 5.3–Trust and Security for experts



ANNEX: ONE SLIDE SUMMARY FOR THE GENERAL PUBLIC

FIGURE 5.4–Trust and Security for the general public



VOLUME 10 REFERENCES

Aeneas, Artemis-IA and EPoS (2021). Strategic research agenda for electronic components and systems 2021. Technical report. Accessible at: https://ecscollaborationtool.eu/publication/download/2021-01-11-ecs-sria2021-final.pdf

Baker, M. and Penny, D. (2016). Is there a reproducibility crisis?

Baquero-Arribas, M., Dorado, L. and Bernal, I. (2019). Open access routes dichotomy and opportunities: Consolidation, analysis and trends at the Spanish national research council. *Publications*, 7(3):49.

Bechhofer, S., De Roure, D., Gamble, M. et al. (2010). Research Objects: Towards Exchange and Reuse of Digital Knowledge. *Nature Precedings*: 1–1.

Bernal, I. and Román-Molina, J. (2018). Informe de la encuesta sobre evaluación por pares y el módulo "Open Peer Review" de DIGITAL.CSIC. Technical report.

Braun, T. (2010). How to improve the use of metrics. *Nature*. 465, 870–872. Accessible at: https://www.nature.com/articles/465870a

Castaño, F., Strzelczak, S., Villalonga, A., Haber, R. E. and Kossakowska, J. (2019). Sensor reliability in cyber-physical systems using internet-of-things data: A review and case study. *Remote Sensing*, 11(19):2252.

Centre National De La Recherche Scientifique (2019). CNRS roadmap for open science. Accessible at: https://www.science-ouverte.cnrs.fr/wp-content/uploads/2019/11/CNRS_Roadmap_Open_Science_ 18nov2019.pdf

Coalition S. (2020). Plan S. Accessible at: http://https://www.coalition-s.org/

COAR (2020). Building a sustainable, global knowledge commons. Accessible at: https://www.coar-repositories.org/

Coretrustseal (2020). Core Trustworthy Data Repositories. Accessible at: http://https://www.coretrustseal.org/

CSIC Divulgación (2020). Webs de Divulgación | Consejo Superior de Investigaciones Científicas – CSIC. Accessible at: csic.es.

ECSEL JTI. (2020). From IoT to system of systems: Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS. Technical report, ARTEMIS Industry Association.

ESFRI (2020). European Strategy Forum on Research Infrastructures. Accessible at: https://www.esfri.eu/

European Commission (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace. Accessible at: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission (2020). European Commission awards contract for setting up an open access publishing platform. Accessible at: https://ec.europa.eu/info/news/european-commission-awards-contract-setting-open-access-publishing-platform-2020-mar-20_en#:~:text=The%20European%20Commission%20has%20awarded,is%20planned%20for%20early%202021.

European Commission (2020). Horizon Europe. Accessible at: http://https://ec.europa.eu/info/horizon-europe_en

European Commission (2019). Orientations towards the first Strategic Plan for Horizon Europe. Accessible at: https://ec.europa.eu/research/pdf/horizon-europe/ec_rtd_orientations-towards-the-strategic-planning.pdf

European Council (2009). European security strategy – a secure Europe in a better world. Accessible at: https://www.consilium. europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/

European Parliament and Council (2019). Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the re-use of public sector information.

European Parliament, European Council, Council, European Economic and Social Committee and Committee Of The Regions (2020). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A New Industrial Strategy for Europe. COM/2020/102. Accessible at: https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en. pdf

European Technology Platform Photonics 21 (2019). Multiannual Strategic Roadmap 2021–2027. Accessible at: https://www.photonics21.org/download/ppp-services/photonics-downloads/Europes-age-of-light-Photonics-Roadmap-C1.pdf

European Union (2020). Network and Information Systems Directive. Accessible at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Union (b). Cybersecurity Act, 2020. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

Fesabid (2020). Grupo de Trabajo Copyright. Accessible at: http://www.fesabid.org/bpi/grupo-bpi-bibliotecas-y-propiedad-intelectual

Fundación Acción Pro Derechos Humanos (2020). ARTÍCULO 44 de la Constitución Española - Acceso a la cultura y promoción de la ciencia. Accessible at: https://www.derechoshumanos.net/constitucion/articulo44CE.htm

Gobierno De España (2017). Estrategia de Seguridad Nacional. Accessible at: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017.

Greer, C., Burns, M., Wollman, D. and Griffor, E. (2019). Cyber-physical systems and internet of things. *NIST Special Publication*, 202:52.

Griffor, E. R., Greer, C., Wollman, D. A. and Burns, M. J. (2017). Framework for cyber-physical systems: Volume 1, overview. Technical report.

IEA (2020). Data Centres and Data Transmission Networks, International Energy Agency, Paris. Accessible at: https://www.iea.org/reports/data-centres-and-data-transmission-networks

Institute Of Electrical and Electronics Engineers (2020). International roadmap for devices and systems 2020. Technical report. Accessible at: https://irds.ieee.org

Ishwarappa and Anuradha, J. (2015). A brief introduction on big data 5Vs characteristics and hadoop technology. In *Procedia Computer Science*, 48: 319–324. Elsevier B. V.

IX EPSCYT (2018). Informe De Resultados. Technical report. v261118. Accessible at: https://icono.fecyt.es/sites/default/files/filepublicaciones/20/epscyt2018_informe.pdf

Mckinsey Digital (2020). A game plan for quantum computing. Accessible at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing

Netherlands (2017). National plan open science. Accessible at: https:// www.openscience.nl/en/national-platform-open-science/ national-plan-open-science

Open Access 2020 (2020). Open Access 2020 Initiative. Accessible at: http://https://oa2020.org/

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79.

Quantum Flagship Initiative (2020). Strategic Research Agenda. Accessible at: https://qt.eu//app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf

Quantum Flagship Initiative, Mishina Et al. (2019). Strategic Agenda Summary: Education for QT. Accessible at: https://qt.eu/app/uploads/2019/03/Strategic-Agenda-Summary-Education-for-QT_19.03.19.pdf

Raymer, M. G. and Monroe, C. (2019). The US national quantum initiative. *Quantum Science and Technology*, 4(2):020504.

Red De Bibliotecas Y Archivos Del CSIC (2020). Apoyo para la publicación en acceso abierto para los investigadores CSIC. Accessible at: http://http://bibliotecas.csic.es/publicacion-en-acceso-abierto

Riedel, M. F., Binosi, D., Thew, R. and Calarco, T. (2017). The European quantum technologies flagship programme. *Quantum Science and Technology*, 2(3):030501.

UN General Assembly (2015). Transforming our world: the 2030 agenda for sustainable development. Resolution A/RES/70/1. Accessible at: https://www.refworld.org/docid/57b6e3e44

United Nations (2020). About the Sustainable Development Goals - United Nations Sustainable Development. Accessible at: https://www.un.org/sustainabledevelopment/development-agenda/

Van Lier, B. (2018). Cyber-physical systems of systems and complexity science: The whole is more than the sum of individual and autonomous cyber-physical systems. *Cybernetics and Systems*, 49(7-8):538–565.

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J. et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, 3:160018.

Wouters, et al. P (2019). Indicator frameworks for fostering open knowledge practices in science and scholarship. Accessible at: https://op.europa.eu/en/publication-detail/-/publication/b69944d4-01f3-11ea-8c1f-01aa75ed71a1

Information, gathered, stored, processed and transmitted, is the cornerstone of the present era and shapes every aspect our daily life, thus permeating cultural and social deep changes. A multi- and cross-disciplinary approach is needed to cover all present challenges of the Information age, ranging from both the more technological aspects to the social ones. This duality is reflected in the title of this volume, Digital and Complex Information. The current Digital Transformation is enabled by developments in physics and engineering and entails several fields including electronics, optics, material science, and quantum technologies. Nowadays challenges include sustainable and energy efficient electronics, integrated photonics with new functionalities, quantum computing and machine learning, and operation within the Internet of Things. Nonetheless the Digital world generates an ever-increasing amount of data in which security and trust play a critical role. The advances in digital technologies call for a new scientific research approach: an Open Science, reproducible, interoperable and accessible. New avenues are open in how we deal with Humanities and with individual/social security and rights, within digital citizenship. This is the broad spectrum of challenges that drives research across about the 40 CSIC institutes in line with the latest developments in digitalization worldwide.

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
CSIC
Consejo Superior de Investigaciones Científicas
EDITORIAL CSIC