Winter Doctoral Day Program – 21st January 2025
Morning Session

Date and time: 8:50. Tuesday 21st January.
Venue: Facultad de Matemáticas. Sala de Grados. 2ª Planta

08:50-09:00 - Welcome
Antonio Prados Montaño, Academic Program Coordinator, Universidad de Sevilla

09:00-10:00 Opening Talk. Dr. Sol H. Jacobsen
Presenting: Dr. Diego Frustaglia, Dept. Física Aplicada II

10:00-14.40. – Students talks

Into the Light:
Towards unified quantum optics and condensed matter computation

Sol H. Jacobsen
Department of Physics, NTNU, Gløshaugen. Norwegian University of Science and Technology

Abstract:

Quantum spintronics aims to reduce the energy cost of condensed matter computation by utilizing the spin degree of freedom of electrons in addition to their charge. Superconducting spintronics marries this aim with the resistance-free currents of superconductivity, and is also fertile ground for investigating the coexistence of competing phases of matter. The field shows great potential for developing the next generation of low-dissipation, condensed matter computation. A separate branch of physics investigates light-matter coupling in order to hybridize matter degrees of freedom with optical ones and communicate this information over long distances. This talk will look at my contribution to these research directions and discuss their potential for a unified future.

Sol Jacobsen short CV:

Her research interests are in fundamental quantum physics, with particular focus on superconductors and magnetic systems. Her background also covers quantum error correction, entanglement, optimal state preservation, integrable systems and quantum optics. She received a joint honours degree in Physics with Philosophy from the University of York, U.K., where she was awarded the university's Goodwin Prize for Physics. She went on to do a Ph.D. at the University of Tasmania, Australia, under the guidance of Peter Jarvis, and then a postdoc at the Freiburg Institute for Advanced Studies, Germany. Since then she has been at NTNU and QuSpin, first as a postdoc with Jacob Linder and then as an independent researcher. In 2019, she won a grant from the Norwegian Research Council to establish her own group, and was awarded Outstanding Academic Fellow at NTNU.

More details can be found in: *https://sites.google.com/view/soljacobsen/team/sol-h-jacobsen* and her X account to chat about work and life as a *@SpintronicMum*

Morning session

Venue: Facultad de Matemáticas. Sala de Grados. 2ª Planta

8:50 – 9:00	Welcome Opening talk
9:00 – 10:00	Sol H. Jacobsen

STUDENTS PRESENTATION

10:00 – 10:20	Chamorro Burgos, Miguel Ángel
10:20 – 10:40	Ríos Monje, Carlos
10:40 – 11:00	Rodríguez Fernández, Eusebio
11:00 – 11:20	Fernández Peramo, Pablo
11:20 – 11:40	Palomeque Mangut, Sergio
11:40 – 12:10	COFFEE BREAK
12:10 – 12:30	Román Hajderek, Roberto
12:30 – 12:50	Rubio Barbero, Francisco
12:50 – 13:10	Vegas Díaz, Alejandro
13:10 – 13:30	Jiménez Cómez, Marina
13:30 – 14:40	*FLASH TALKS*

Abstracts Students' presentations
LONG TALKS

10:00-10:20.- Chamorro Burgos, Miguel Ángel

"Compressible hydrodynamic interactions"

It is well-established that the same degrees of freedom can evolve differently depending on whether they operate in one, two, or three spatial dimensions. In a colloidal monolayer at the interface between two fluids, particles behave as a two-dimensional system within the plane, but hydrodynamic interactions propagate in three dimensions. This hybrid case is ideal for studying dimensional transitions.

Recent predictions identified a characteristic behavior of two-dimensional collective diffusion in this configuration, distinct from the "pure" cases of two or three dimensions. This phenomenon was experimentally verified, inspiring studies of similar setups, such as thick layers, membranes, and self-propelled active particles.
Active matter, which drives systems out of equilibrium by violating conservation laws, has spurred numerous theoretical and numerical models emphasizing propulsion mechanisms. Our work focuses on the dynamics of active colloids in this hybrid configuration, introducing a novel concept: "shakers." These particles do not self-propel but actively generate flows in the surrounding medium. When confined to a fluid interface, they exhibit unique collective behaviors, such as macroscopic structures due to compressibility or the stabilization of collapse caused by capillary interactions from interface deformations.

10:20-10:40.- Ríos Monje, Carlos

"Optimal synchronisation to a limit cycle: the Van der Pol oscillator"

The Van der Pol oscillator is a prototypical model for synchronisation phenomena. In the absence of external forcing, all its trajectories on the phase plane tend to a closed, periodic, trajectory—the limit cycle—after infinite time. We are interested in minimising the non-conservative contribution to the work when driving the system from a given initial point on the phase plane to any final point belonging to the limit cycle in a finite time. To this end, we resort to optimal control theory, which has been recently exploited in the context of statistical mechanics. The minimization of the work without any restriction is solved by applying calculus of variations theory, and the results can be extended to the general framework of the Liénard equation. Beyond the unrestricted case, we consider a non-holonomic constraint that bounds the possible values of the driving force to a finite range. Pontryagin's Principle is needed to address this problem, leading to an optimal protocol, that alternates between bang and Euler-Lagrange pieces.

10:40-11:00.- Rodríguez Fernández, Eusebio

"Quantum Spin Dynamics In Curved Circuits"

"Spin carriers propagating along quantum circuits gather quantum spin phases depending on the circuit's size, shape, and spin-orbit coupling (SOC) strength.
In this work, we study the effects abrupt changes of curvature has on the quatum spin dynamics on mesoscopic flat circuits. We find that the abrupt change of curvature when using polygonal

interferometers leaves an imprint on the quantum conductance and the topological phases of the system, opening up the use of these features as control tools in spintronics circuits.
Here we present the case for three different SOCs, Rashba and Dresselhaus [001] which, although belonging to different symmetry classes, produce field textures coplanar to the plane of the circuit and Dresselhaus [110] which, contrary to the previously mentioned variant, produces orthogonal field textures.

11:00-11:20.- Fernández Peramo, Pablo

"A Photovoltaic Receptor for Event-Based Sensors"

A Dynamic Vision Sensor (DVS) proof-of-concept chip employing an unconventional photo-transduction front end has been designed. Instead of the conventional logarithmic transducer comprising a photodiode and a nonlinear load, the proposed pixel architecture uses a single diode operating in the photovoltaic regime. This operation regime, the same as employed for solar cells, features a voltage-current characteristic that endows the sensor with remarkable sensitivity to transient illumination variations, particularly in low light conditions. Also, the lack of resistive loads benefits compactness and decreases static power consumption. Experimental results with the sensor demonstrate advantages over previous art regarding noise and latency.

11:20-11:40.- Palomeque Mangut, Sergio

"Low-Light Challengues in a PFM Digital Pixel Sensor - Leakage and Quantization"

CMOS image sensors (CIS) come in all shapes and sizes. One such is the digital pixel sensor (DPS), a family of architectures in which the analog-to-digital conversion (ADC) takes place within each pixel. In this presentation, we present a comprehensive analysis and simulation of reset leakage currents and quantization errors in pulse frequency modulation (PFM) DPS. PFM imagers encode absolute light intensity in the rate of pulses, or spikes, using a comparator and an asynchronous self-reset feedback, initiating a new integration cycle each time the voltage reference is reached. We showcase the benefits of using an NMOS reset switch in mitigating leakage currents and reducing fixed pattern noise (FPN), particularly in low-light conditions, where PMOS reset implementations often fail to sustain proper photocurrent integration. By characterizing leakage mechanisms, including subthreshold, gate-induced drain leakage, and reverse-bias junction currents, we derive their influence on photodiode operation and propose methods to optimize pixel design for enhanced sensitivity. Furthermore, quantization error caused by residual charge

is analyzed, highlighting its impact on dynamic range and performance. We validate the theoretical insight with simulation results from an advanced CMOS technology, demonstrating improved lowlight performance and reduced error using the NMOS reset. These findings provide a framework for designing high-performance PFM-DPS pixels for future imaging applications.

11:40-12:10.- COFEE BREAK

12:10-12:30.- Roberto Roman Hajderek

"A quantum-safe authentication scheme for IoT devices using homomorphic encryption and weak physical unclonable functions with no helper data"

Physical Unclonable Functions (PUFs) are widely used to authenticate electronic devices. Therefore, each device can be uniquely identified and counterfeit devices can be detected. Weak PUFs, which support a relatively small number of challenge- response pairs (CRPs), are simple and easy to construct. Device authentication with weak PUFs typically uses helper data to obfuscate and recover a cryptographic key that is then required by a cryptographic authentication scheme. However, these schemes are vulnerable to helper-data attacks and many of them do not protect conveniently the PUF responses, which are sensitive data, as well as are not resistant to attacks performed by quantum computers. This paper proposes an authentication scheme that avoids the aforementioned weaknesses by not using helper data, protecting the PUF response with a quantum-safe homomorphic encryption, and by using a two- server setup. Specifically, the CRYSTALS-Kyber is used for its quantum resistance and suitability for resource-constrained Internet-of-Things (IoT) devices. The practicality of the proposal was tested on an ESP32 microcontroller using its internal SRAM as a SRAM PUF.

12:30-12:50.- Rubio Barbero, Francisco

"Unlocking Unpredictability: Random Telegraph Noise for Secure Hardware"

"Nowadays, when data safety is becoming crucial with each innovation step, using the inherent unpredictability of physical phenomena opens new ways for evermore secured hardware. This talk delves into describing the use of Random Telegraph Noise (RTN) as a basic entropy source for designing both True Random Number Generators and Physical Unclonable Functions. The latter design already proposed, this talk introduces key new modifications that make this feasible

for high-quality TRNG applications. With a common entropy extraction metric, it will be demonstrated the feasibility of achieving such stable yet unpredictable bitstreams, we also address key random metrics such bit balance, minimal autocorrelation, and randomness validation tests based on the industry-grade NIST SP 800-22 test suite.
This presentation will outline some of the main issues—and the main challenges from the RTN physical layer constrains (defect capture and emission) to ""a high entropy biasless output"". First results show the feasibility of the architecture; in particular, the promise it holds out for IoT devices and other applications in power-constrained environments. Future work will look into the analysis of the impact of introducing post-processing algorithms on the generated bitstreams and the extension of this methodology to multi-defect RTN , laying the foundation for a silicon integration.

12:50-13:10.- Vegas Díaz, Alejandro

"Nuclear reactions studies at experimental Basic Nuclear Physics line at CNA: the case of 6Li+12C reaction"

The study of nuclear reactions involving different ions and light targets at low energies provides crucial information for the development and corroboration of different theories and models applied to astrophysical environments. The experimental Basic Nuclear Physics (FNB) line of National Accelerators Center (CNA), is being adapted and prepared with the aim of studding these reactions, taking advantage of the target development and characterization provided at the CNA and collaborating facilities. As a first step, the reaction of 6Li+12C at different energies around the Coulomb barrier, covering a wide angular range, has been measured.
In this talk, the experimental setup employed for the 6Li+12C reaction measurement at CNA will be detailed and the preliminary results of the data analysis carried out will be presented and discussed. Finally, the perspectives of the future work related to the experimental setup for other nuclear reactions studies at the FBN experimental line will be presented.

13:10-13:30.- Jiménez Cómez, Marina

"Hybrid kinetic-MHD simulation of Edge Localized Mode and Alfvén Waves in ASDEX Upgrade Tokamak with MEGA code"

The population of fast ions is a great concern in tokamaks since they can interact with plasma fluctuations such as Alfvén Waves (AWs) and lose their confinement. Various experimental [1]

and numerical [2] results on the ASDEX Upgrade tokamak demonstrated an interaction between Edge localized modes (ELMs) and fast ions. To better understand the underlying physics, nonlinear hybrid kinetic-MHD simulations were performed using the MEGA code [3].
An abrupt ELM crash of an ASDEX Upgrade NBI heated plasma was simulated self consistently with fast-ions kinetic effects. Simulations reveal that, in the presence of Alfvén modes the ballooning mode prior to the ELM is affected by the AWs. The edge perturbation amplitude oscillates at the AW frequency (~150 kHz). An interaction region rotating at the AW frequency has been identified radially separating both modes. Likewise, in the presence of the ELM, the growth rate of the AW increases by a factor of ~2 . A fast-ion redistribution analysis is done to understand the impact of fast ions in the dynamics of the instabilities.

FLASH TALKS

13:30-13:35.- Auñón Fernández, Gabriel

"Test measurement of the 27Al(alpha,n) reaction at CNA HiSPANoS"

The neutrons produced in nuclear reactions following the absorption of alpha particles play a crucial role in several fields of research: production of new elements in astrophysics, neutron background in underground dark matter experiments, or nuclear materials interrogation, for instance.
To study this type of reaction, members of the Spanish nuclear physics community have established the MANY Collaboration (Measurement of Alpha Neutron Yields). Corresponding experiments will be carried out at two laboratories, one of them being the Centro Nacional de Aceleradores (CNA) of Universidad de Sevilla. There, alpha beams up to 9 MeV can be produced in both continuous and pulsed mode. The facility is well suited for alpha-activation measurements and thus the 27Al(alpha,n) has been studied by looking at the decay of the corresponding 30P reaction products. Unfortunately, the current pulsing system is inefficient for alpha beams because it was designed for hydrogen beams, but a test experiment for the 27Al(alpha,n) and the registered time-of-flight distributions using a single MONSTER neutron detector module are promising.
The preliminary results of the activation and time-of-flight measurements will be presented together with the recently funded facility upgrades for an improved production and pulsing of the alpha beams.

13:35-13:40.- Bartolomé Sarsa, Jesús

"Thermal neutrons at HiSPANoS: Proposal for a moderating system"

The use of thermal neutron radiation is widespread across numerous fields and its use is a core component of many different experiments, including the study of fission and fusion, archeology, astrophysics, medicine or research applications. Such experiments are mostly carried out in nuclear reactors, which are the most intense thermal neutron source. This makes measuring in research reactors highly demanded, but many experiments do not require such high neutron fluxes and can be conducted in alternative thermal neutron facilities. In this context, Compact Accelerator Neutron Sources (CANS) produce neutrons via nuclear reactions triggered by energetic ion beams. One of such CANS is HiSPANoS, hosted at the Centro Nacional de Aceleradores (CNA).

HiSPANoS is commissioned and open to users as a fast and epithermal neutron source. Aiming at expanding its capabilities to provide thermal neutrons, a neutron moderator has been designed via Monte Carlo simulations using the Geant4 toolkit. The proposed set-up takes into consideration the particularities of HiSPANoS in terms of ion beam energies and possible neutron production reactions, as well in terms of space limitations in the experimental hall. The characteristics of the expected thermal neutron beams and fields will be presented together with the measurement plan for the eventual commissioning.

13:40-13:45.- López Rodríguez, Álvaro

"Novel method for 210Po and 210Pb low level measurements in seawater"

The Ocean is the largest carbon sink on Earth. With the Biological Carbon Pump as one of the main mechanisms to transport the organic carbon synthesized in the surface by the phytoplankton to the deep ocean, where it remains stored. Evaluating this process and the organic carbon flux from surface to depth is essential to accurately quantify the gigatons of carbon stored. To indirectly calculate this flux, the measurement of the disequilibrium found in depth between the naturally occurring radioactive pair 210Pb-210Po is widely used. To measure 210Po and 210Pb, a radiochemical procedure is applied to isolate 210Po. 209Po is added as internal tracer to determine the chemical yield of the procedure and hence 210Po losses. Therefore, it is necessary that both Po-isotopes behave chemically identically and are extracted in equal proportion from the seawater matrix. However, the most used method for Po-isotope isolation extracts 209Po more efficiently than 210Po when those procedures are followed, this leads to inaccuracies in the measured activity of 210Po. In response to the need for new methods to accurately determine 210Po activity in seawater, we propose a new robust, easy-to-apply procedure. This method consists of co-precipitating polonium isotopes with Fe(OH)2 and it has been successfully employed in various water matrices. It is concluded that i) the radiochemical yield is slightly lower than that of traditional methods, but ii) the change of the oxidation state of Fe to II guarantees the correct extraction of tracer and 210Po from the matrix.

13:45-13:50.- González González, Beatriz

"Developing machine learning algorithms to quantify Th-234 export fluxes in the ocean"

The biological pump (BP) is one of the main mechanisms by which the ocean captures carbon from the atmosphere and transports it to the deep ocean. The downward flux of photosynthetically produced particulate organic carbon (POC flux) is one of the most important parameters of the BP. Quantifying the POC flux is essential to understand the marine carbon cycle and the impact of the BP on global carbon cycle. POC flux in the ocean presents challenges for observing and modeling its functioning and influencing parameters. The disequilibrium of the radioactive pair Th-234 - U-238 due to the sinking particles allows the determination of Th-234 flux, which is used to estimate POC flux. In this study, we used machine learning techniques to predict Th-234 fluxes globally, as a proxy for POC flux in the ocean. For that, Two ML models, Random Forest and Extreme Gradient Boosting, were applied using seven input variables, including location, year, and other biophysical characteristics derived from satellite data. The results demonstrate the models ability to predict Th-234 fluxes with a high degree of accuracy. This approach provides a viable method for estimating Th-234 fluxes along the five oceans, with the advantage of not requiring in-situ measurements.

13:50-13:55.- López Cansino, Ramón

"2D maps of ion temperatures, impurity velocity flows and densities with Coherence Imaging Charge Exchange Recombination Spectroscopy at Wendelstein 7-X"

Well-established diagnostics used in the field of plasma physics and nuclear fusion typically provide its measurements as 1D radial profiles. In this work, a diagnostic based on the Coherence Imaging Spectroscopy technique is developed. Optimized for the measurement of radiation generated after charge exchange reactions between impurities present in the plasma and neutral particles injected by the neutral beam injector, this novel application enables the derivation of 2D measurements of relevant plasma parameters such as the ion temperature, impurity velocity flows or densities in the core region of Wendelstein 7-X plasmas. These measurements constitute a substantial upgrade to the already existing data because of the higher spatial resolution provided and the possibility to identify 2D structures such as magnetic islands. The resulting measurements are shown and finally validated against standard diagnostic results.

13:55-14:00.- Reyner Vignolas, Alex

"Characterization of fast ion losses with FILD diagnostics"

"In tokamak plasmas fast ions are produced as a product of fusion reactions and the different heating mechanisms. A good confinement of these fast ions is necessary to ensure good performance and keep the structural integrity of the machine. Understanding the mechanisms responsible for fast ion losses is then critical for the success of future magnetically confined fusion power plants. The Fast Ion Loss Detector (FILD) [1] is a key diagnostic for the characterization of fast ion losses in a tokamak. When the probe head is inserted into the vessel, the lost ions enter the diagnostic through a collimator and hit a scintillator plate that we are recording with a camera. This allows us to measure the energy and pitch of the ions. The geometry of the detector varies depending on the conditions and target ions of each machine. In this work we will present the results from the double collimator FILD in ASDEX, and the design of the ITER FILD collimator, optimized to measure the alpha particles product of the deuterium-tritium reaction.
[1] M. Garcia-Muñoz et al., Rev. Sci. Instrum. 87 11D829 (2016)".

14:00-14:05.- Torres Muñoz, Carmen

"Commissioning of a High-Temperature Furnace for the Nuclear Microprobe at the CNA"

This work presents the commissioning of a high-temperature furnace integrated into the nuclear microprobe beamline at the Centro Nacional de Aceleradores (CNA). The furnace enables in-situ studies of material behavior under controlled thermal conditions while subjected to ion beam analysis. Major developments include mounting the furnace on a heat shield, testing the system under high vacuum conditions and integrating the system into the microprobe chamber.
Initial tests demonstrate the furnace's capacity to reach temperatures up to 500°C, maintaining stability suitable for advanced material characterization with a accuracy of 1ºC. These upgrades expand the capabilities of the microprobe, in particular it will be used for characterisation of silicon carbide detectors (using IBIC technique) at high temperatures (from room temperature up to 400 ºC)

14:05-14:10.- Ruíz Martín, Mateo

"Packed-Bed Plasma Reactors for Hydrogen Production"

Hydrogen is emerging as one of the primary alternatives to fossil fuels due to its high energy density and status as a clean energy source. However, for hydrogen to serve as an efficient fuel, it is imperative for it to be easily transportable and storable in large quantities. To address these challenges, instead of directly storing hydrogen, a hydrogen carrier can be employed. Among several options, ammonia stands out due to several advantages, leading to the process known as ammonia-to-hydrogen. This talk focuses on the use of atmospheric cold plasma technologies to carry out this process in-situ. The plasma reactor consists of a special type of dielectric barrier discharge, a packed-bed reactor. These

types of reactors are specifically chosen for their numerous advantages in enhancing the efficiency of plasma chemical processes. The reactors operate at room temperature and atmospheric pressure, reducing the need for extensive cooling and vacuum systems. Their scalability and cost-effectiveness also make them suitable for on-site generation, ensuring that the technology can be easily distributed. Additionally, it can be directly fed with renewable energy, contributing to the electrification of the industry.

14:10-14:15.- Delgado Lozano, Ignacio

"Dual-band dual-polarization microstrip patch antenna"

Standard microstrip patch antennas are normally used for simple single-band single-polarization cases presenting a reduced bandwidth around 5 %. However, modifying and complicating the design of this type of antennas, it is possible to obtain much more advanced configurations as differential feeding, circular polarization or ultrawide bandwidths. In this work, the authors propose a dual-band dual-polarization microstrip patch antenna, made by coupling the patch resonance with the ones from Chebyshev second-order filters of a diplexer. The ultimate goal is to design a filtering antenna ('filtenna'), which is an emergent device able to act as a conventional antenna while rejecting undesired frequency components.

14:15-14:20.- Cheng, Yufeng

"Molecular Dynamics simulation on electrical conduction of room temperature ionic liquids under strong electric field"

Room temperature Ionic liquids (RTILs) are a kind of room temperature molten salt completely composed of ions. With the advantages of high conductivity, nonvolatile, chemical stability or wide electrochemical windows. RTILs have been applied in batteries, fuel cells, electrospray thrusters. Recent research classified the RTILs as dilute electrolyte since only a few of ions, called 'free ions', contribute to the electrical conductivity and the formation of electrical double layer. In addition, it was found that the number of free ions and, consequently, the conductivity increased with temperature. We use the open-source Molecular Dynamics (MD) code LAMMPS to investigate the electrical conduction of RTILs in strong electric filed (~ 1 V/nm). A modified open-source Python-based post-processor PyLAT is used for data processing. Some studies suggest that the ions tend to exist in a free state, a behavior comparable to that observed with increasing temperature. However, the impacts of elevated temperature and applied electric fields on properties such as energy profiles, radial distribution functions (RDFs), and ion mobility differ significantly. While the two-state model has effectively elucidated the influence of temperature on the electrical conductivity of RTILs, a comprehensive understanding of how electric fields enhance their electrical conduction remains to be achieved.

14:20-14:25.- Hidalgo Zamora, Francisco

"Equivalent Circuit Model of a Frequency Selective Surface"

An Equivalent Circuit Model of a Frequency Selective Surface (FSS) is a circuit which models the behaviour of the FSS. In this flash talk the structure of a FSS will be explained and a procedure to model this FSS using a circuit based on passive lumped and distributed elements, will be shown

14:25-14:30.- Misas Arcos, Mario

"Spacetime paradoxes"

General relativity represents our most advanced effort to understand the nature of gravity and spacetime itself. However, it also predicts some of the most counter-intuitive phenomena in physics, giving rise to several paradoxes. This talk will attempt to show how a mathematical approach can be key in resolving these puzzles, or at least approaching a solution. By employing semi-Riemannian geometry, we will examine scenarios such as the twin paradox, the information paradox, and other perplexing scenarios, including the existence of wormholes and exotic spacetimes.

14:30-14:35.- Casado Galán, Alejandro

"Design Proposal for Configurable Hybrid-PUF – TERORO"

c) Phisically Unclonable Functions (PUF) are a very useful cryptographic primitive used in the field of hardware security. A good PUF provides a robust and secure autenthication procedure for circuits in the Internet of Things (IoT). It works as a digital fingerprint for identifying a circuit and preventing malicious spoofing attacks by extracting information from a physical source of entropy, in integrated circuits, this is typically the variation in the silicon substrate. Typical structures for designing PUFs in silicon circuits are Ring-Oscillators (RO) and Transient Effect Ring-Oscillators (TERO). In this work I present a way of combining the two in one mixed structure called "TERORO", where it has a configuration input to choose the type of oscillator, either TERO or RO. Also, because of its intrinsic architecture, the amount of inverting stages is also configurable, introducing the posibility of changing the frequency of oscillation.

14:35-14:40.- Navarro Torrero, Pablo

"Design of a Karatsuba Multiplier to Accelerate Digital Signature Schemes on Embedded Systems"

This flash talk summarizes the design and implementation of a Karatsuba multiplier to accelerate digital signature schemes on embedded systems. The Karatsuba algorithm is integrated into hardware accelerators for RSA and EdDSA, representing a fundamental component of contemporary, state-of-the-art implementations. A hardware/software co-design methodology is employed, implementing the architectures on a System-on-Chip platform that combines

programmable logic with an ARM processor. The results showcase enhanced resource consumption and timing performance for both signature generation and verification, confirming the superiority of EdDSA over RSA when utilizing the same Karatsuba multiplier core and coding techniques.

Attendees (not presenting)

- Daniel Lopez Aires
- Pedro Punta De La Herran
- Jose Luis Garcia Leon
- Jesus Gonzalez Rosa
- Alfonso Rodriguez Gonzalez
- Jose Antonio Pavon Rodriguez
- Daniel Jimenez Flores
- Gabriel Auñon Fernandez
- Andres Rodriguez Galan
- Maria Laura Olivera Atencio
- Mateo Ruiz Martin
- Unai Abascal Ruiz
- Antonio Jesus Lopez Fuentes
- Servando Marin Meana
- Fernando Puentes Del Pozo
- Gregorio Garcia Valladares
- Daniil Kabirov Leontieva
- Jesus Salas Suarez Barcena
- Alvaro Saiz Castillo
- Kiera Anne Mckay
- Apurba Karmakar
- Manuel Martinez Rojas
- Demetrio H. Saucedo Cuberes
- Amir Khan
- Ivan Diez De Los Rios Luis
- Apurba Karmakar