AL09

Cryptography

Criptografía

Organizers **Organizadores** **Antolatzaileak**

David Balbás Gutiérrez
(IMDEA Software Institute)

Miguel Beltrá Vidal
(Universidad de Alicante)

Helena Martín Cruz
(IMAC & Universitat Jaume I)

Guillermo Pascual Pérez
(Inst. of Science and Technology Austria)

Description **Descripción** **Deskribapena**

Cryptography is the science and practice of designing computation and communication systems in the presence of adversaries. This session includes presentations on multiple aspects of state-of-the-art cryptography. On the one hand, it will cover mathematical advances on techniques underlying the design and cryptanalysis of cryptographic primitives and protocols. These techniques often rely on results from number theory, coding theory, algebraic geometry, and combinatorics. On the other hand, it will address problems and solutions that arise when applying these mathematical results to the real world, including protocol design, computationally hard problems, and provable security.

La criptografía es la ciencia que estudia la seguridad de la computación y de las comunicaciones en presencia de adversarios. Esta sesión incluye ponencias sobre múltiples aspectos de la criptografía actual. Por un lado, se tratarán avances matemáticos en técnicas que subyacen al diseño y criptoanálisis de primitivas y protocolos criptográficos. Estas técnicas frecuentemente se basan en resultados de teoría de números, teoría de códigos, geometría algebraica y combinatoria. Por otro lado, se plantearán problemas y soluciones que surgen al aplicar estos resultados matemáticos al mundo real, como el diseño de protocolos, los problemas computacionalmente difíciles, y la seguridad demostrable.

MSC Codes **Códigos MSC** **MSC Kodeak**

94-06

(primary)

94A15; 94A60; 94B05

(secondary)

Slots **Bloques** **Blokeak**

1.A (Aula 0.6); 1.B (Aula 0.6); 1.C (Aula 0.6)

QR Code **Código QR** **QR Kodea**

Session Schedule **Horario de la Sesión** **Saioaren Ordutegia**

L13 | 17:30-17:50 | 0.6
An alternative Commitment-based model for Authenticated Key Exchange protocols
Rodrigo Martín Sánchez-Ledesma (Universidad Complutense de Madrid & Indra Sistemas de Comunicaciones Seguras)

L13 | 18:00-18:20 | 0.6
Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via multiple local maps
Ginevra Giordani (Università degli Studi dell'Aquila)

L13 | 18:30-18:50 | 0.6
Group Key Progression: Strong Security for Persistent Data
David Balbás (IMDEA Software Institute, Universidad Politécnica de Madrid & NTT Social Informatics Laboratories)

L13 | 19:00-19:20 | 0.6
Secret Sharing Schemes for Approximated Weighted Threshold Access Structures
Miquel Guiot (Universitat Rovira i Virgili)

M14 | 15:00-15:20 | 0.6
Lower bounds on the Communication Cost of Multicast Encryption and Group Messaging
Miguel Cueto Noval (Institute of Science and Technology Austria)

M14 | 15:30-15:50 | 0.6
Formal Modelling and Analysis for Cryptographic Protocols
Arturo Hernández Sánchez (VRAIN, Universitat Politècnica de València)

M14 | 16:00-16:20 | 0.6
Lattice problems and Security
Miguel Ángel González de la Torre (Instituto de Tecnologías Físicas y de la Información-CSIC)

M14 | 16:30-16:50 | 0.6
A Critical Look into Threshold Homomorphic Encryption for Private Average Aggregation
Miguel Morona-Mínguez (Universidad de Vigo)

M14 | 17:30-17:50 | 0.6
Advancing Symmetric Cryptography: Cryptanalysis of Symmetric Techniques for Advanced Protocols (STAP)
Irati Manterola Ayala (Simula UiB)

M14 | 18:00-18:20 | 0.6
Advances in the Cryptanalysis of DME-minus signature scheme
Pilar Coscojuela (Universidad Complutense de Madrid)

M14 | 18:30-18:50 | 0.6
Security Analysis of a Code-based Cryptosystem Using Convolutional Codes
Miguel Beltrá Vidal (University of Alicante)

Monday 13	**Lunes 13**	**Astelehena 13**
17:30-17:50	**17:30-17:50**	**17:30-17:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

An alternative Commitment-based model for Authenticated Key Exchange protocols

Rodrigo Martín Sánchez-Ledesma
(Universidad Complutense de Madrid & Indra Sistemas de Comunicaciones Seguras)

In this talk we present an alternative Unauthenticated Model, intended to build a security framework to cover protocols whose specifics may not concur with those of already existing models for authenticated exchanges. This new model is constructed from the notion of commitment schemes, employing ephemeral information, therefore avoiding the exchange of long-term cryptographic material. From this model, we propose a number of key exchange protocols, formalizing their security under this model.

Joint work with David Domingo Martín and Iván Blanco Chacón.

Monday 13	**Lunes 13**	**Astelehena 13**
18:00-18:20	**18:00-18:20**	**18:00-18:20**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via multiple local maps

Ginevra Giordani
(Università degli Studi dell'Aquila)

The construction of invertible low-multiplicative non-linear layers over $\mathbb{F}_p^n$ is crucial for the design of symmetric primitives targeting Multi Party Computation, Zero-Knowledge proofs and Fully Homomorphic Encryption. We generalize a construction recently studied by constructing a shift invariant lifting over finite fields via multiple local maps of degree ≤ 2. We prove that if $n \geq 3$, then $\mathcal{S}_{\mathrm{F}_0,\mathrm{F}_1}$ is never invertible unless it is a Type-II Feistel scheme.

Joint work with Lorenzo Grassi, Silvia Onofri and Marco Pedicini.

Monday 13	**Lunes 13**	**Astelehena 13**
18:30-18:50	**18:30-18:50**	**18:30-18:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Group Key Progression: Strong Security for Persistent Data

David Balbás

(IMDEA Software Institute, Universidad Politécnica de Madrid & NTT Social Informatics Laboratories)

We study how to extend strong end-to-end security for data in transit to shared data at rest, such as for message backups and file sharing. We introduce Group Key Progression (GKP), a primitive which enables a (dynamic) group of users to agree on a persistent sequence of keys efficiently. Our construction Grappa satisfies post-compromise security and interval access control, a new notion that describes how group changes translate into access to keys in the sequence.

Joint work with Matilda Backendal and Miro Haller.

Monday 13	**Lunes 13**	**Astelehena 13**
19:00-19:20	**19:00-19:20**	**19:00-19:20**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Secret Sharing Schemes for Approximated Weighted Threshold Access Structures

Miquel Guiot

(Universitat Rovira i Virgili)

In weighted threshold access structures, each party has a weight, and subsets are authorized if their combined weight reaches a threshold. For these access structures, existing secret sharing schemes result in large shares that scale linearly with the weights. To improve efficiency, the access structure can be approximated. This talk focuses on balancing efficiency and accuracy in such approximations by using techniques based on the Chow parameters

Joint work with Oriol Farràs.

eprint.iacr.org/2024/772

Tuesday 14	**Martes 14**	**Asteartea 14**
15:00-15:20	**15:00-15:20**	**15:00-15:20**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Lower bounds on the Communication Cost of Multicast Encryption and Group Messaging

Miguel Cueto Noval
(Institute of Science and Technology Austria)

We prove lower bounds on the communication cost of maintaining a shared key among a group of users and consider primitives like multicast encryption (ME) and continuous group-key agreement (CGKA). These are round-based primitives in which users can be added or removed from the group and its members in a given round agree on a key that should not be possible to derive by non-members. We prove our results in a combinatorial model that also implies lower bounds in a symbolic model for ME and CGKA.

Joint work with Michael Anastos, Benedikt Auerbach, Mirza Ahad Baig, Matthew Kwan, Guillermo Pascual-Perez and Krzysztof Pietrzak.

eprint.iacr.org/2024/1097
eprint.iacr.org/2023/1123

Tuesday 14	**Martes 14**	**Asteartea 14**
15:30-15:50	**15:30-15:50**	**15:30-15:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Formal Modelling and Analysis for Cryptographic Protocols

Arturo Hernández Sánchez
(VRAIN, Universitat Politècnica de València)

Formal modeling uses computational logic to verify software systems. In the context of cryptographic protocols, it is used to determine whether an intruder can gain some knowledge from the exchange of information between participants by reasoning about the algebraic properties of their cryptographic primitives. In this talk, we will give an overview of how these models can be used to detect vulnerabilities in cryptographic protocols and how their analysis can be automated with Maude-NPA.

Joint work with Santiago Escobar.

Tuesday 14	**Martes 14**	**Asteartea 14**
16:00-16:20	**16:00-16:20**	**16:00-16:20**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Lattice problems and Security

Miguel Ángel González de la Torre
(Instituto de Tecnologías Físicas y de la Información-CSIC)

Lattice-based cryptography is currently one of the most relevant fields of development in terms of public key cryptosystems. The security of these cryptosystems (like ML-KEM or Frodo-KEM) is based on the difficulty of solving hard lattice problems (LWE or SVP). The relationship between the parameters, the derived lattice problem and the security derived from these assumptions are the topics considered for this conference.

Tuesday 14	**Martes 14**	**Asteartea 14**
16:30-16:50	**16:30-16:50**	**16:30-16:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

A Critical Look into Threshold Homomorphic Encryption for Private Average Aggregation

Miguel Morona-Mínguez
(Universidad de Vigo)

Threshold Homomorphic Encryption is a good fit for private federated average aggregation, a key operation in Federated Learning. Despite its potential, recent studies show that threshold schemes in mainstream HE libraries can introduce security vulnerabilities if an adversary has access to a restricted decryption oracle. We survey the use of threshold RLWE-based HE for federated average aggregation and examine the performance impact of using smudging noise with large variance as countermeasure.

Tuesday 14	**Martes 14**	**Asteartea 14**
17:30-17:50	**17:30-17:50**	**17:30-17:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Advancing Symmetric Cryptography: Cryptanalysis of Symmetric Techniques for Advanced Protocols (STAP)

Irati Manterola Ayala
(Simula UiB)

We explore advancements in symmetric cryptography, focusing on Symmetric Techniques for Advanced Protocols (STAP). STAPs are ciphers designed for improving efficiency in cryptographic protocols such as ZK-proofs, FHE, and MPC. We evaluate the security of new STAPs against algebraic attacks, including a key recovery attack on the Rubato cipher family, and efficient Gröbner basis attacks for solving polynomial equations in primitives like Arion, Griffin, and Anemoi.

Tuesday 14	**Martes 14**	**Asteartea 14**
18:00-18:20	**18:00-18:20**	**18:00-18:20**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Advances in the Cryptanalysis of DME-minus signature scheme

Pilar Coscojuela
(Universidad Complutense de Madrid)

Following the attack on the DME scheme by D. Smith-Tone et al., we are working to determine whether it can be adapted to DME-minus, a variant of the DME where only the even-indexed components of the public key are available. The resulting system of equations for recovering an equivalent last round is similar to that of DME but with half the number of equations. This talk will focus on studying the complexity of solving such a system.

Joint work with I. Luengo and M. Avendaño.

Tuesday 14	**Martes 14**	**Asteartea 14**
18:30-18:50	**18:30-18:50**	**18:30-18:50**
[Room 0.6]	**[Aula 0.6]**	**[Gela 0.6]**

Security Analysis of a Code-based Cryptosystem Using Convolutional Codes

Miguel Beltrá Vidal
(University of Alicante)

We study some security notions of a McEliece cryptosystem based on convolutional codes: Indistinguishability under Chosen-Plaintext Attacks (IND-CPA), Indistinguishability under Adaptive Chosen-Ciphertext Attacks (IND-CCA2), Non-Malleability under Adaptive Chosen-Ciphertext Attacks (NM-CCA2), and Indistinguishability of Keys under Chosen-Plaintext Attacks (IK-CPA). We show that they are not satisfied. Thus, the cryptosystem should not be used in practice unless proper conversions are applied.

Joint work with Paulo Almeida and Diego Napp.