BOOK OF ABSTRACTS

SS40 - New Trends in Cryptography

2nd Joint Meeting Brazil-Italy in Mathematics

September 10, 2026

Messina, Italy

Organizers:

Carina Alves, São Paulo State University
Marialaura Noce, University of Salerno

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

A Geometric Characterization of Maximal Unrefinable Partitions

Riccardo Aragona , Lorenzo Campioni, Roberto Civino
Department of Information Engineering, Computer Science and Mathematics, University of L'Aquila

Integer partitions into distinct parts may appear in several areas of mathematics, sometimes unexpectedly. In particular, they have been recently shown to be linked to translation subgroups in the symmetric group with 2^n elements and generating sets of groups in a group-theoretical problem related to algebraic cryptography [3,5]. Triggered by this problem, Aragona et al. showed that the generators of a given group are linked to partitions into distinct parts which satisfy a condition of *non-refinability* [4] together with a condition on the minimal excludant. This motivates us to investigate some combinatorial aspects of *unrefinable partitions*, i.e. those in which no part can be written as the sum of two different integers which do not belong to the partition (cf. the On-Line Encyclopedia of Integer Sequences for the first values [6, `https://oeis.org/A179009`]).

In this talk, we investigate the combinatorial structure of unrefinable partitions through their correspondence with numerical sets and Young diagrams. Building on the bijection introduced by Keith and Nath, we apply a general geometric criterion that links the unrefinability of a partition directly to the hook lengths of its associated Young diagram. This criterion provides a structural method for the characterization of any unrefinable partition.

Using this general framework, we revisit the correspondence results between *maximal* unrefinable partitions and partitions into distinct parts, previously established using enumerative methods [1]. We provide alternative and purely combinatorial proofs of these bijections, focusing on the rigid symmetry structures of the Young diagrams. In the triangular weight case, we show that the corresponding diagrams are quasi-symmetric, i.e. symmetric up to a single extra column. We extend this analysis to the nontriangular case, showing that the diagrams either exhibit this same quasi-symmetric structure or are perfectly self-conjugate, depending on the maximal part.
This is a joint work with Campioni and Civino [2].

References

[1] R. Aragona, L. Campioni, and R. Civino, *The number of maximal unrefinable partitions*, Ramanujan J. 69 (2026), 57.

[2] R. Aragona, L. Campioni, and R. Civino, *A Geometric Characterization of Maximal Unrefinable Partitions via the Keith-Nath Transformation and Young Diagrams*, arXiv preprint, arXiv:2602.01281 (2026).

[3] R. Aragona, R. Civino, N. Gavioli, and C. M. Scoppola, *Regular subgroups with large intersection*, Ann. Mat. Pura Appl. (4) 198 (2019), no. 6, 2043–2057.

[4] R. Aragona, R. Civino, N. Gavioli, and C. M. Scoppola, *Unrefinable partitionsinto distinct parts in a normalizer chain.* Discrete Math. Lett. 8 (2022), 72–77.

[5] R. Civino, C. Blondeau, and M. Sala, *Differential attacks: using alternative operations.* Des. Codes Cryptogr. 87 (2019), no. 2-3, 225–247.

[6] *The On-Line Encyclopedia of Integer Sequences*, Published electronically at `https://oeis.org`.

E–mail: `riccardo.aragona@univaq.it`.

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

Eidolon: A Post-Quantum Signature Scheme Based on k-Colorability in the Age of Graph Neural Networks

Asmaa Cherkaoui [1]
Laboratory of Mathematical Analysis, Algebra and Applications (LAM2A), Faculty of Sciences Ain Chock (FSAC), University Hassan II, Casablanca, Morocco

Ramon Flores
Department of Geometry and Topology, Faculty of Mathematics, University of Seville, Seville, Spain

Delaram Kahrobaei
Departments of Computer Science and Mathematics, Queens College, City University of New York, USA
and PhD Program in Mathematics, and Initiative for the Theoretical Sciences, Graduate Center, City University of New York, USA
and Department of Computer Science and Engineering, Tandon School of Engineering, New York University, USA
and Department of Computer Science, University of York, United Kingdom

Richard C. Wilson
Department of Computer Science, University of York, United Kingdom

We propose Eidolon, a post-quantum digital signature scheme based on the NP-complete problem of graph k-colorability. The construction generalizes the classical zero-knowledge identification protocol of Goldreich, Micali and Wigderson from 3-colorability to arbitrary k-colorability, and then applies the Fiat–Shamir transform to obtain a non-interactive signature scheme.

The public key is a graph generated with a planted valid k-coloring, while the secret key is the corresponding coloring. The graph is constructed so that the secret coloring is known to the signer but remains hidden inside an instance whose statistical behavior is close to that of a random graph. This point is important because worst-case NP-hardness alone is not sufficient for cryptographic security: concrete graph instances may still be vulnerable to heuristic solvers.

To reduce signature size, Eidolon uses Merkle-tree commitments. Instead of including all vertex commitments in every Fiat–Shamir round, the signer publishes Merkle roots and reveals only the authentication paths required by the verifier. This compresses the signature size from asymptotically O(tn) to O(t log n), where n is the number of vertices and t is the number of Fiat–Shamir rounds.

We also present an empirical security analysis against classical and learning-based attacks. In particular, we evaluate exact coloring methods, the DSatur heuristic, and a graph neural network attacker inspired by recent work on combinatorial optimization with GNNs. The experiments indicate that, for the tested parameter ranges, neither DSatur nor the GNN-based approach is able to recover the planted coloring for sufficiently large graphs. These results suggest that carefully generated k-colorability instances can resist the considered classical and machine-learning-based cryptanalytic approaches.

References

[1] A. Cherkaoui, R. Flores, D. Kahrobaei, and R. C. Wilson, *Eidolon: A Post-Quantum Signature Scheme Based on k-Colorability in the Age of Graph Neural Networks*, in *International Workshop on the Arithmetic of Finite Fields*, pp. 32–51, Springer Nature Switzerland, Cham, 2026.

[1]The authors acknowledge the support from the Institut Henri Poincare and LabEx CARMIN.
E–mail: esma1maysan@gmail.com.

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

A New Algebraic Diffie–Hellman Key-Exchange

Massimiliano Di Matteo
Department of Mathematics and Physics, University of Campania "Luigi Vanvitelli"
Ramón Esteban-Romero
Department of Mathematics, University of Valencia
Maria Ferrara
Department of Engineering, Pegaso University

We introduce a Diffie–Hellman key-exchange protocol built upon a novel algebraic structure, providing a new approach to secure key establishment.

E–mail: maria.ferrara1@unipegaso.it.

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

A group-based Functional Encryption scheme

Delaram Kahrobaei
The City University of New York, Queens College and Graduate Center - New York, USA
Carmine Mirra, Antonio Tortora
Dipartimento di Matematica e Fisica, Università della Campania "Luigi Vanvitelli" - Caserta, Italy
Maria Tota
Dipartimento di Matematica, Università di Salerno - Fisciano (SA), Italy

Functional Encryption is an extension of public-key cryptography that enables the receiver to learn a specific function of the encrypted data without revealing any additional information about the plaintext [3]. Motivated by [1], we present a functional encryption scheme for the inner product whose security relies on the Learning Homomorphism with Noise problem [2], a group-based variant of the Learning With Errors problem. Furthermore, we analyze the security of the scheme.

This contribution was partially supported by an INdAM-GNSAGA project (CUP E53C25002010001).

References

[1] M. Abdalla, F. Bourse, A. De Caro and D. Pointcheval, *Simple functional encryption schemes for inner products.* In IACR International Workshop on Public Key Cryptography, pages 733-751, 2015.

[2] G. Baumslag, N. Fazio, A. Nicolosi, V. Shpilrain and W.E. Skeith, *Generalized Learning Problems and Applications to Non-commutative Cryptography.* In Proc. ProvSec '11, volume 6980 of LNCS, pages 324–339, 2011.

[3] D. Boneh, A. Sahai and B. Waters, *Functional encryption: Definitions and challenges.* In Theory of Cryptography Conference (pp. 253-273). Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

E–mail: carmine.mirra@unicampania.it.

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

Graphs associated with groups and cryptographic applications

Carmine Monetta
Department of Mathematics, University of Salerno

Graph-theoretic methods play an important role in modern cryptography and information security. Several cryptographic primitives and secret-sharing schemes have been proposed using graph-based constructions, whose security relies on the computational hardness of classical graph problems such as Clique, Coloring, Dominating Set, and Hamiltonian Cycle. This connection motivates the study of graph families in which such problems become tractable, as understanding the underlying structural reasons for this behavior may help identify both suitable and unsuitable candidates for cryptographic applications.

In this talk, we focus on graphs naturally associated with groups, including power graphs, commuting graphs, and related constructions. These graphs provide a rich interaction between algebraic and combinatorial properties, often exhibiting a highly constrained structure inherited from the underlying group. We present recent results showing that, for broad classes of group-associated graphs, certain graph-theoretic properties force strong algebraic restrictions. As a consequence, some graph families that might initially appear suitable for hardness-based applications can be ruled out.

E–mail: cmonetta@unisa.it.

2nd Joint Meeting Brazil-Italy
in Mathematics
Messina, 7–11 September 2026

SS40

Cryptographic techniques for secure data aggregation

Delaram Kahrobaei
The City University of New York, Queens College and Graduate Center - New York, USA
Carmine Mirra, Antonio Tortora
Dipartimento di Matematica e Fisica, Università della Campania "Luigi Vanvitelli" - Caserta, Italy
Maria Tota
Dipartimento di Matematica, Università di Salerno - Fisciano (SA), Italy

There are three main cryptographic approaches used to build secure aggregation protocols: masking, additively homomorphic encryption, and functional encryption. We review these approaches and discuss how each enables secure data aggregation.

This contribution was partially supported by an INdAM-GNSAGA project (CUP E53C250020 10001).

E–mail: antonio.tortora@unicampania.it.