Ministero dell'Università e della Ricerca | FIS | UNIVERSITÀ DI TRENTO

Università di Trento

Dipartimento di Matematica

Borsa di studio/Scholarship

A	**Titolo:** Singular structures in the geometry of measures: decompositions, rigidity and rectifiability/Strutture singolari nella geometria delle misure: decomposizioni, rigidità e rettificabilità

Project Code: MUR FIS2 CUP E53C25001800001 - FIS-2023-02725

CUP: E53C25001800001

Topic: Mathematical Analysis - Geometric Measure Theory, Optimal Transport and Calculus of Variations

Project Manager: Andrea Marchese

Contact: andrea.marchese@unitn.it

Synthetic description of the activity and expected research outcome

The project lies at the interface of Geometric Measure Theory and Optimal Transport, and aims at developing tools to describe measures and variational objects concentrated on irregular, lower-dimensional or fractal-like sets. Particular attention will be devoted to the fine structure of singular measures, rectifiability criteria and rigidity properties arising in geometric variational problems.

The expected research outcome is the development of new analytical and geometric methods for the study of singular measures and related structures. The goal is to combine Geometric Measure Theory and Optimal Transport to uncover hidden structures of singularities and address open problems including Besicovitch-type density questions, metric currents, vanishing-mass phenomena and rigidity of measures.

In addition to the standard PhD research budget and the generous travel funds provided by the PhD programme in Trento, the project will provide substantial extra funding for conferences, research visits, and other scientific travel.

References:

-Alberti, Marchese, On the differentiability of Lipschitz functions with respect to measures in the Euclidean space, Geom. Funct. Anal. (2016).
-Besicovitch, On the fundamental geometrical properties of linearly measurable plane sets of points (II), Math. Ann. (1938).
-Brenier, Polar factorization and monotone rearrangement of vector-valued functions, Comm. Pure Appl. Math. (1991)
-Colombo, De Rosa, Marchese, On the well-posedness of branched transportation, Comm. Pure Appl. Math. (2021).
-De Philippis, Rindler, On the structure of A-free measures and applications, Ann. of Math. (2016).
-Preiss, Geometry of measures in R^n: distribution, rectifiability, and densities, Ann. of Math. (1987).

Ideal candidate (skills and competencies)

The ideal candidate has a strong background in Mathematical Analysis, with solid knowledge of measure theory, functional analysis and variational methods. Experience in Geometric Measure Theory (rectifiability, currents, singular measures), Optimal Transport, or related topics in Geometric Analysis is desirable. The candidate should be able to work independently and interact with the research group.

UNIVERSITÀ DI TRENTO

Università di Verona

Borsa di studio/Scholarship

B	**Titolo:** Next-Generation high order moving mesh methods for hyperbolic equations

Project Code: ERC-STG AlcHyMiA, Grant Agreement Project 101114995

CUP: B33C23001120006

Topic: Numerical Analysis, Scientific Computing, High order numerical methods for Hyperbolic equations

Project Manager: Elena Gaburro (UniVR)

Contact: elena.gaburro@univr.it

Synthetic description of the activity and expected research outcome

The research activity funded by this scholarship will be carried out in the context of the ERC Starting Grant ALcHyMiA: "Advanced Structure Preserving Lagrangian schemes for novel first order Hyperbolic Models: toward General Relativistic Astrophysics" (GA 101114995).

The PhD student will work on the development and validation of novel numerical methods, of Finite Volume and Discontinuous Galerkin type, of high order of accuracy, for solving systems of nonlinear hyperbolic equations with an improved efficiency and robustness.

These methods will be developed on polygonal and polyhedral meshes moving together with the fluid flow in the context of cutting-edge Arbitrary-Lagrangian-Eulerian techniques, that involve a novel challenging integration over space-time 3d and 4d control volumes (which can be also degenerate).

The following topics could be also object of study: i) algorithms for grid generation and optimization, ii) the parallelization of the developed codes, iii) introduction of structure preserving techniques to increase accuracy and robustness, iv) introduction of novel non linear limiting techniques, v) the developments of routines for visualization.

The resulting methods will be applied in the field of computational fluid dynamics (e.g. Euler equations, multiphase models ...) and/or computational astrophysics (Euler-Einstein equations).

References:

Professor's website: https://www.elenagaburro.it, https://elenagaburro.it/publications

Project's website: https://www.elenagaburro.it/ALcHyMiA.

A simple paper: *High-order Arbitrary-Lagrangian-Eulerian schemes on crazy moving Voronoi meshes*, Springer 2023, link: https://arxiv.org/pdf/2208.02092.

Ideal candidate (skills and competencies)

The ideal candidate holds a Master's degree in Mathematics, Physics, Engineering, or Informatics and has experience in the analysis or implementation of numerical methods for PDEs. Familiarity with Finite Element and/or Finite Volume methods, mesh generation, or hyperbolic equations is valued. Good programming skills are also appreciated; candidates should highlight these competencies by citing relevant courses, projects, or thesis work.

We also look for a candidate capable of writing clear and interesting scientific English with a personal and independent style. The applicant's writing should reflect their own reasoning, moving beyond the use of AI-generated text. The Statement of Purpose and Research Project will be used to attest to this ability.

UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borsa di studio/Scholarship

C	**Cryptanalysis of Post-Quantum Cryptosystems**

Topic: Cryptography and Quantum Information

Project Manager: Alessandro Tomasi

Contact: altomasi@fbk.eu

Synthetic description of the activity and expected research outcome

Quantum computing allows the invention of some algorithms that are much more efficient than classical algorithms at solving specific problems. In particular, Shor's algorithm [Shor97] allows a sufficiently powerful quantum computer to recover private keys from public keys for legacy cryptosystems, by factoring RSA public moduli [Ekerå21] and breaking the (EC)DLP [RNSL17].

The security of post-quantum cryptosystems remains a subject of interest in order to establish safe parameter sets, particularly for concrete instances - rather than asymptotic estimates - for the more recent problems in so-called lattice-based cryptography [APS15]. This is not only relevant to standardized primitives, but especially for cryptosystems that are still under development for advanced applications, such as threshold signatures, functional encryption, multiparty computation, and homomorphic encryption.

The candidate's research will focus on an assessment of the level of security of concrete instances of post-quantum cryptosystems, through cryptanalytic techniques as well as practical software simulation of quantum information algorithms [LM21][PBP21].

References:

[APS15] Martin R. Albrecht, Rachel Player and Sam Scott. On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169–203, ISSN (Online) 1862-2984, ISSN (Print) 1862-2976 DOI: https://doi.org/10.1515/jmc-2015-0016, October 2015. https://eprint.iacr.org/2015/046. https://github.com/malb/lattice-estimator

[Ekerå21] Ekerå, M. (2021). On completely factoring any integer efficiently in a single run of an order-finding algorithm. Quantum Information Processing, 20(6). https://doi.org/10.1007/s11128-021-03069-1

[LM21] Li, B., Micciancio, D. (2021). On the Security of Homomorphic Encryption on Approximate Numbers. In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science(), vol 12696. Springer, Cham. https://doi.org/10.1007/978-3-030-77870-5_23. https://eprint.iacr.org/2020/1533.

[PBP21] Perriello, S., Barenghi, A., Pelosi, G. (2021). A Quantum Circuit to Speed-Up the Cryptanalysis of Code-Based Cryptosystems. In: Garcia-Alfaro, J., Li, S., Poovendran, R., Debar, H., Yung, M. (eds) Security and Privacy in Communication Networks. SecureComm 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-90022-9_25

[RNSL17] Roetteler, M., Naehrig, M., Svore, K. M., and Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. Cryptology ePrint Archive, Paper 2017/598. https://eprint.iacr.org/2017/598

[Shor97] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/s0097539795293172

Ideal candidate (skills and competencies)

MSc in Mathematics or Computer Science with a focus on the mathematics of cryptography

Software development skills, preferably in Rust or Python. Prior knowledge of Qiskit would be helpful.

Good knowledge and proficiency of the English language

Expertise on one or more of the scientific topics in the call description above.

UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borsa di studio/Scholarship

D	**Applications of Zero-Knowledge Proofs**

Topic: Applied Cryptography

Project Manager: Alessandro Tomasi

Contact: altomasi@fbk.eu

Synthetic description of the activity and expected research outcome

Zero-knowledge proofs are a central field of study in modern cryptography, enabling a prover to convince a verifier that a statement is true without revealing any other information. Over the last decade, they have moved from being mostly theoretical protocols to practical tools.

Despite recent progress, efficient real-world deployment remains challenging. Proving can be computationally demanding, memory can easily become a bottleneck, and seemingly minor algebraic design decisions can have major performance consequences. The choice of elliptic curve, scalar field, and polynomial representation of constraints directly influences the scalability of the system. In particular, whether computations are native to the proving field, or they must be emulated in a non-native field, can significantly affect the circuit size and hence, proving cost. A classical example of this problem is encoding cryptographic hash functions in arithmetic circuits [GKRRS19]. This leaves a considerable gap between what is possible in theory and what is practical in deployed systems.

This PhD project aims to study zero-knowledge proof systems from both an algebraic and an implementation-oriented perspective. The candidate will investigate how structural choices, like curve selection, field compatibility, and the embedding of primitives, influence prover and verifier complexity. Circuit design, arithmetization, and parameter selection are also studied trying to assess trade-offs between prover time, verifier time, proof size, and memory usage.

The scope also includes the potential design of new or adapted proof constructions when current approaches prove inadequate for specific constraints. The primary aim is to let practical bottlenecks and deployment requirements guide the design process to improve on existing schemes.

Digital identity infrastructures form the main application context, since they combine strong privacy requirements with demanding usability and efficiency constraints. In such systems, holders of credentials should be able to prove assertions about themselves for e.g., age verification or entitlement to voting rights, without disclosing more information than strictly necessary [LKWL25][FS24]. Additional scenarios, such as end-to-end verifiable electronic voting [HKLR24], content provenance [DCB24], and verifiable machine learning inference [XLFWZJSZ25] serve as test cases to expose different measures of performance limitation. Electronic voting poses large-scale verification and aggregation challenges, while machine learning inference stresses circuit size and proving cost.

Overall, the goal is to connect algebraic structure with practical performance and to develop optimization strategies that make zero-knowledge proofs efficient and deployable in real-world systems.

References

[DCB24] VerITAS: Verifying Image Transformations at Scale. Trisha Datta, Binyi Chen, Dan Boneh. Cryptology ePrint Archive, Paper 2024/1066. https://eprint.iacr.org/2024/1066

[FS24] Anonymous credentials from ECDSA. Matteo Frigo, abhi shelat. Cryptology ePrint Archive, Paper 2024/2010. https://eprint.iacr.org/2024/2010

[GKRRS19] Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, Markus Schofnegger. Cryptology ePrint Archive, Paper 2019/458. https://eprint.iacr.org/2019/458.pdf

[HKLR24] ZK-SNARKs for Ballot Validity: A Feasibility Study. Nicolas Huber, Ralf Kuesters, Julian Liedtke, Daniel Rausch. Cryptology ePrint Archive, Paper 2024/1902. https://eprint.iacr.org/2024/1902

[LKWL25] The BBS Signature Scheme. Tobias Looker, Vasilis Kalos, Andrew Whitehead, Mike Lodder. 7 July 2025. https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html

[XLFWZJSZ25] zkPyTorch: A Hierarchical Optimized Compiler for Zero-Knowledge Machine Learning. Tiancheng Xie, Tao Lu, Zhiyong Fang, Siqi Wang, Zhenfei Zhang, Yongzheng Jia, Dawn Song, Jiaheng Zhang. Cryptology ePrint Archive, Paper 2025/535. https://eprint.iacr.org/2025/535

Ideal candidate (skills and competencies)

MSc in Mathematics or Computer Science with a focus on the mathematics of cryptography

Software development skills, preferably in Rust or Python. Prior knowledge and development experience of libraries for zero knowledge proofs would be helpful.

Good knowledge and proficiency of the English language

Expertise on one or more of the scientific topics in the call description above.