Roberta Cimorelli Belfiore

✉ r.cimorellibelfio@studenti.unimol.it • 🌐 robertacimorelli.github.io
Date of birth: 04/06/1997 Citizenship: Italian

Education and Training

University of Molise **Pesche, Italy**
PhD in Computer Science *2023–Current*
Supervisor: Prof. Anna Lisa Ferrara
Link to Doctoral School

University of Molise **Pesche, Italy**
Master's Degree in Software Systems Security *2021–2023*
Cum Laude
Thesis: *Identity-Based Matchmaking Encryption: A Generic Construction and Instantiations from Standard Lattice Assumptions*

University of Molise **Pesche, Italy**
Bachelor's Degree in Computer Science *2019–2021*

Visiting Research Experience

Fondazione Bruno Kessler (FBK) **Trento, Italy**
PhD Visiting Researcher (planned) *Sep 2025 – Mar 2026*
Planned six-month research stay at FBK under the supervision of Prof. Silvio Ranise. The activity will focus on applied cryptography and access control for protected data, with the goal of integrating theoretical aspects of my PhD into practical scenarios.

Newcastle University — CryptoLab **Newcastle, UK**
PhD Visiting Researcher *Feb 2025 – Aug 2025*
Research within the CryptoLab, supervised by Dr. Essam Ghadafi, on the design of cryptographic primitives for access control over encrypted data, with a focus on efficient post-quantum constructions.

Newcastle University **Newcastle, UK**
Short-term Visit *Jul 2024*

- Engaged in research discussions and explored collaborative opportunities.

University Activities

University of Molise **Isernia, Italy**
Teaching Assistant *Feb 2023 – May 2023*

- Conducted ongoing tutoring activities aimed at guiding and assisting students.
- Provided tutoring for working students who could not regularly attend classes.
- Offered tutoring for students with learning disabilities (D.S.A.).
- Supported students enrolled in bachelor's and master's degree programs with administrative tasks.
- Provided academic support to students.

Research Interests

My research combines theoretical cryptographic foundations with practical applications, focusing on privacy-preserving authentication, anonymous access control, and quantum-resilient protocols. My recent work has explored variants of cryptographic primitives such as Identity-Based Matchmaking Encryption, Access Control Encryption, and Hierarchical Key Assignment Schemes, aiming to strengthen privacy and security in identity-centric systems.

Professional Activities

Web Chair, 38th IFIP WG 11.3 DBSEC 2024

Sub-reviewer, 38th IFIP WG 11.3 DBSEC 2024

Reviewer, IEEE Transactions on Dependable and Secure Computing

Conferences and Seminars

Invited Talk: *Analyzing Access Control Policies in Smart Environments*
Newcastle University, Newcastle upon Tyne, UK, 25 Jul 2024.

Conference Talk: *Identity-Based Matchmaking Encryption from Standard Lattice Assumptions*
22nd International Conference on Applied Cryptography and Network Security (ACNS '24), Abu Dhabi, UAE, 05-08 Mar 2024

Conference Talk: *Security Analysis of Access Control Policies for Smart Homes*
28th ACM Symposium on Access Control Models and Technologies (SACMAT '23), Trento, Italy, 07-09 Jun 2023

Awards

Sep 2024: **CLUSIT Thesis Award**
Honored with the CLUSIT Thesis Award at the 19th edition.
Link

Feb 2025: **"Prof. Mario Massimo Petrone" Study Award**
Awarded for the most meritorious Master's Degree thesis in Software Systems Security (LM-66), discussed during the academic year 2023-2024.
Link

Jan 2024: **2024 ACNS Student Travel Grant**
Honored with the 2024 ACNS Student Travel Grant at the 22nd International Conference on Applied Cryptography and Network Security.

Funded Research Projects

Verifica di proprietà di sicurezza nello sviluppo del software
Team member of the research project coordinated by Prof. Anna Lisa Ferrara, as part of the Departmental Research Projects – Start-up 2023 Call of the University of Molise (UNIMOL).

INdAM-GNCS Project 2025 – CUP_E53C24001950001
Team member of the research project coordinated by Prof. Manuela Flores, funded by INdAM GNCS.

Research Groups

Program Analysis in the Clouds Lab (PAC Lab)
Member of the research group coordinated by Prof. Gennaro Parlato and Prof. Anna Lisa Ferrara at the University of Molise.

CryptoLab
Member of the research group lead by Dr. Essam Ghadafi within the CryptoLab at the School of Computing, Newcastle University.

INDAM - GNCS
Member of the research group of the Istituto Nazionale di Alta Matematica "Francesco Severi" (INDAM), part of the UNIMOL research unit. UNIMOL collaborates with INDAM to promote scientific research and advanced training in mathematical disciplines, hosting a Research Unit administratively based at the Department of Biosciences and Territory.

Publications

[1]: Cimorelli Belfiore, R., Ferrara, A. L., & Ghadafi, E. (2025). *ACE+: Access Control Encryption with Verifiable Sender Provenance*. Preprint.

[2]: Cimorelli Belfiore, R., Ferrara, A. L., & Ghadafi, E. (2025). *Sender-Authenticated ACE: Bridging Practicality and Efficiency*. Preprint.

[3]: Cimorelli Belfiore, R., De Santis, A., Ferrara, A. L., & Masucci, B. (2025). *Hierarchical Key Assignment Schemes with Key Rotation and Bidirectional Secret Derivation*. Submitted to International Journal.

[4]: Cimorelli Belfiore, R., De Santis, A., Ferrara, A. L., & Masucci, B. (2024). *Hierarchical Key Assignment Schemes with Key Rotation*. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT 2024), ACM.

[5]: Cimorelli Belfiore, R., De Cosmo, A., & Ferrara, A. L. (2024). *Identity-Based Matchmaking Encryption from Standard Lattice Assumptions*. In Pöpper, C., & Batina, L. (Eds.), *Applied Cryptography and Network Security (ACNS 2024)*, Lecture Notes in Computer Science, vol. 14584, Springer.

[6]: Cimorelli Belfiore, R., & Ferrara, A. L. (2023). *Security Analysis of Access Control Policies for Smart Homes*. In Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT 2023), ACM.