curricul um vitae	

PERSONAL INFORMATION

Surname	**Cimorelli Belfiore**
Name	**Roberta**
Address	**Piazza Carducci, 21, 86170, Isernia, Italy**
Telephone	**3899563929**
Fax	
E-mail	r.cimorellibelfio@studenti.unimol.it
Skype	

Nationality	Italian

Date of birth	4 June 1997

Education and training

• Date (from – to)	2023
• Name and type of organisation providing education and training	University of Molise, Department of Biosciences and Territory
Duration of the program of study	3 years
• Principal subjects/occupational skills covered	Design and analysis of cryptographic primitives for access control on encrypted data
• Title of qualification awarded	PhD in Biology and Applied Sciences
Final mark obtained	Ongoing

• Date (from – to)	2021-2023
• Name and type of organisation providing education and training	University of Molise, Department of Biosciences and Territory
Duration of the program of study	2 years
• Principal subjects/occupational skills covered	Software Systems Security
• Title of qualification awarded	Laurea Magistrale in Sicurezza informatica (LM-66)
Final mark obtained	110/110 cum laude

• Date (from – to)		2019-2021
• Name and type of organisation providing education and training		University of Molise, Department of Biosciences and Territory
Duration of the program of study		3 years
• Principal subjects/occupational skills covered		Computer Science
• Title of qualification awarded		Laurea in Scienze e Tecnologie Informatiche (L-31)
Final mark obtained		109/110

• Date (from – to)		2011-2016
• Name and type of organisation providing education and training		Liceo Scientifico Ettore Majorana (ISERNIA)
Duration of the program of study		5 years
• Title of qualification awarded		High school diploma
Final mark obtained		95/100

graduation thesis

Title	Identity-Based Matchmaking Encryption: A Generic Construction and Instantiations from Standard Lattice Assumptions
Thesis	Master's degree thesis in Software Systems Security
Language	English
Supervisor	Prof. Anna Lisa Ferrara
Thesis Summary	Identity-Based Matchmaking Encryptyion (IB-ME) is an extension of identity-based encryption that emphasizes privacy and authenticity. The content of a message is revealed only when the identity of the receiver matches the identity specified by the sender, and when the identity of the destination sender, chosen by the receiver during decryption, matches the actual identity of the sender. In this thesis we first show a generic construction of an IB-ME that achieves not only a new concept of advanced privacy as defined in the literature, but also authenticity, using an anonymous Identity Based Encryption (IBE) and context-hiding homomorphic signatures as the starting block. In addition, some specific instances are defined based on lattice assumptions. The framework allows secure IB-ME schemes to be instantiated in the standard model using lattice-based assumptions and providing post-quantum security.

Title	Security Analysis of Access Control Policies for Smart Home
Thesis	Bachelor's Thesis in Computer Science
Language	Italian
Supervisor	Prof. Anna Lisa Ferrara
Thesis Summary	

| | The objective of this thesis is to define an expressive administrative model for smart homes and explore the possibility of designing automatic tools for security analysis of such administrative policies. |
| | Accordingly, an extension (Extended-AEGRBAC) was created to a preexisting model that makes it possible to express the application of administrative rules in dependence of preconditions. With the knowledge gained, it was possible to perform a reduction that makes it possible to transform an access control policy for smart home into an administrative policy for RBAC. Thus, a realistic example policy was created that represents a possible scenario for smart homes and on which the results of this thesis were tested. |

publications and articles submitted	

Author(s) and title	Roberta Cimorelli Belfiore, Anna Lisa Ferrara - "Security Analysis of Access Control Policies for Smart Homes"
Language	English
Publication place	Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT '23), Association for Computing Machinery, New York, NY, USA
Date of publication	24/05/23

Author(s) and title	Roberta Cimorelli Belfiore, Andrea De Cosmo and Anna Lisa Ferrara - "Identity-Based Matchmaking Encryption from Standard Lattice Assumptions"
Language	English
Publication place	ACNS 2024: 22nd International Conference on Applied Cryptography and Network Security
Date of publication	Accepted

participation and presentation	28th ACM Symposium on Access Control Models and Technologies (SACMAT '23), Trento 7-9 June 2023

certifications

Certifications of language knowledge	English Speaking Board International Ltd (ESB), level B2, score 79,5/100 on 03/10/2022

Work experience, stages, studies abroad	

• Date (from – to)	08/02/2023 – 23/05/2023
• Name and address of firm/university	University of Molise
• Type of business or sector	Orientation and Tutoring Sector
• Type of employment	Tutor
• Main activities and responsibilities	I have carried out in-progress tutoring activities directed at orienting and assisting students, and for students with D.S.A. I have also carried out support activities for students enrolled in bachelor's and master's degree programs in dealing with administrative paperwork, as well as teaching support.

Personal skills and competences *Acquired in the course of life and career but not necessarily evidenced by formal certificates and diplomas.*	

Mother tongue	**Italian**

Other language(s)	

	Inglese
• reading	excellent
• writing	good
• speaking	good

Social skills and competences *Living and working with other people, in multicultural environments, in positions where communication is important and situations where teamwork is essential (e.g. Culture and sports), etc.*	During my college career, I participated in numerous group projects, which allowed me to develop strong teamwork skills. These experiences taught me the importance of collaboration, effective communication and the ability to achieve common goals together with other team members. In addition, I have performed tutoring activities at the university that allowed me to practice my communication skills and help other students in developing their skills and knowledge. Through these group projects and tutoring, I learned how to manage group dynamics, coordinate activities, listen to and respect the opinions of others, and work effectively and harmoniously toward a common goal. These experiences have also taught me to adapt to different personalities and work styles, fostering a culture of collaboration and success.

Organizational skills and competences *E.g. coordination and management of people, projects and budgets; at work, in voluntary work (e.g. culture and sports) and at home, etc.*	During the "Software Project Manager" course at my university, I had the opportunity to take on the role of manager for a group of Bachelor's degree students. In this context, I was responsible for leading the team in the development and implementation of a software project, ensuring that the established timelines were met. I worked with the team to fully understand the project objectives and clearly and concisely define what was to be achieved. I broke the project down into specific tasks and assigned tasks to the team, taking into account the skills and preferences of each member. I set clear deadlines and monitored the progress of the work to ensure that the project was progressing on schedule.

Technical skills and competences *With computers, specific kinds of equipment, machinery, etc.*	Office Automation: I possess advanced knowledge of the Microsoft Office suite, including Word, Excel, PowerPoint and Outlook. I am able to effectively use these applications to create documents, spreadsheets, presentations, and manage e-mail. Geographic Information System (GIS): I have intermediate-level proficiency in using QGIS software, which allows me to work with geographic data, create thematic maps, and analyze spatial data. Programming: I am familiar with several integrated development environments (IDEs), including Android Studio, Eclipse, NetBeans, and Visual Studio Code. I have a basic knowledge of Apache Maven for build automation, Javascript libraries such as Angular, markup languages such as CSS and HTML, and programming languages such as C and Java. I have basic expertise in configuring and managing the Apache Tomcat web server for web application development. Systems and network management: I have intermediate-level proficiency in the Linux operating system, which allows me to perform systems management and configuration tasks. Data Management: I have intermediate-level knowledge of database management systems (DBMS), including MongoDB and MySQL. I am able to create and manage databases, perform queries, and ensure data security. Security: I possess intermediate-level skills in using Kali Linux, a distribution of Linux that specializes in computer security. Vulnerability Assessment: I have learned the methodologies and techniques

	for identifying and assessing vulnerabilities in computer systems and networks. Cryptography: I have a solid understanding of cryptographic principles and techniques used to protect sensitive data and ensure the confidentiality, integrity and authenticity of information. I understand the concepts of symmetric and asymmetric cryptography, digital signatures, digital certificates and security protocols. Network Security and Software: I have gained knowledge of network and software systems security techniques, e.g., access management, threat identification, and common attacks.

Artistic skills and competences *Music, writing, drawing etc.*	I am a creative person and find pleasure in exploring new ideas and innovative solutions. My creativity is expressed through approaching problems, generating new perspectives, and thinking outside the box. I possess a good ability to communicate clearly and effectively through writing. I am able to express my ideas in an organized and coherent manner, adapting style and tone to the target audience.

Other skills and competences *Competences not mentioned above.*	Adaptability: I am flexible and able to adapt to changes and new situations. I am open to new ideas and perspectives, and can effectively handle the challenges and pressures of work.