



Carozza Eliana

Nationality: Italian Date of birth: 18/06/1998  Phone: (+33) 695728390  Email: carozza@irif.fr

 Website: <https://elianacarozza.github.io/>

ABOUT MYSELF

PhD Researcher in advanced post-quantum cryptography

WORK EXPERIENCE

Research Fellow - PhD

Université de Paris [30/09/2021 – Current]

City: Paris | Country: France

PhD in Computer Science, specializing in code-based post-quantum cryptography.
Expert in signatures, zero-knowledge protocols, and MPC-in-the-head.

Internship

Cryptoexpert [11/2023 – 03/2024]

City: Paris | Country: France

PUBLICATIONS

[2024]

On Threshold Signatures from MPC-in-the-Head

Eliana Carozza, Geoffroy Couteau

[2024]

Short Signatures from Regular Syndrome Decoding. Revisited

IACR publication presented in ASIACRYPT 2024

Dung Bui, Eliana Carozza, Geoffroy Couteau, Dahmun Goudarzi, Antoine Joux

[2023]

Short Signatures from Regular Syndrome Decoding in the Head

IACR publication presented in EUROCRYPT 2023

Eliana Carozza, Geoffroy Couteau, Antoine Joux

TEACHING

[09/2024 – Current]

Teaching Assistant in Computer science

Teaching Assistant for the "Informatique" course at the Department of Computer Science, Paris Diderot University.

[09/2024 – Current]

Teaching Assistant in Introduction à la programmation Python

Teaching Assistant for the "Introduction à la programmation Python" course at the Department of Computer Science, Paris Diderot University.

[09/2023 – 01/2024]

Teaching Assistant in Introduction aux systèmes d'exploitation

Teaching Assistant for the "Introduction aux systèmes d'exploitation" course at the Department of Computer Science, Paris Diderot University.

[09/2023 – 01/2024]

Teaching Assistant in Introduction à la programmation Python

Teaching Assistant for the "Introduction à la programmation Python" course at the Department of Computer Science, Paris Diderot University.

[09/2020 – 02/2021]

Teaching Assistant in Algebra

Teaching Assistant for the Algebra course in the first year of the Master's program at the Department of Mathematics, University of Rome.

EDUCATION AND TRAINING

Phd in Computer Science

Institut de Recherche en Informatique Fondamentale - Université Paris Cité [30/09/2021 – Current]

Address: 8 Pl. Aurélie Nemours, 75013 Paris (France) | Website: <https://www.irif.fr> | Field(s) of study: Post quantum cryptography

Financial Controller Master

Melius Form [13/11/2020 – 28/05/2021]

Address: Via Duilio, 12, 00192 Rome (RM) (Italy) | Website: <https://www.meliusform.it/> | Field(s) of study: Business, administration and law: • Finance, banking and insurance | Level in EQF: EQF level 7

Master of Mathematics

Univserità degli studi Roma Tre [09/2019 – 17/03/2021]

Address: Via Ostiense, 159, 00154 Rome (RM) (Italy) | Website: <https://www.uniroma3.it/> | Field(s) of study: Natural sciences, mathematics and statistics: • Mathematics | Final grade: Cum Laude | Level in EQF: EQF level 7 | National classification: Master's Degree | Thesis: Isogeny- based post-quantum cryptography

Bachelor of Mathematics

Università degli Sudi di Salerno [09/2016 – 07/2019]

Address: Via Giovanni Paolo II, 132, 84084 Fisciano (SA) (Italy) | Website: <https://www.unisa.it/> | Field(s) of study: Natural sciences, mathematics and statistics: • Mathematics | Final grade: Cum Laude | Level in EQF: EQF level 6 | National classification: Bachelor's Degree | Thesis: Finite field and cryptography

Scientific high school diploma

Liceo scientifico "A. Diaz" [08/2011 – 07/2016]

Address: 81020 Caserta (CE) (Italy) | Website: <https://www.liceodiazce.edu.it/> | Final grade: Cum Laude | Level in EQF: EQF level 4 | National classification: Scientific diploma

COURSES

[29/08/2021 – 02/09/2021]

CISPA SUMMER SCHOOL 2021: Coding Techniques & Advanced Post-Quantum Cryptography

[23/05/2021 – 27/05/2021]

UNCG Summer School 2021: Applications of Expander Graphs to Number Theory and Computer Science

[06/2019 – 08/2019]

Corso di formazione in Trasferimento delle Tecnologie Matematiche per l'Innovazione

LANGUAGE SKILLS

Mother tongue(s): Italian

Other language(s):

English

LISTENING C1 READING C1 WRITING C1

SPOKEN PRODUCTION B2 SPOKEN INTERACTION B2

French

LISTENING C1 READING C1 WRITING C1

SPOKEN PRODUCTION B2 SPOKEN INTERACTION B2

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user

DIGITAL SKILLS

Software Skills

C / C++ / Python / Java / Linux / SQL