

Luigi Russo

Curriculum Vitae

Work Experience

2021 **Research Engineer**, *EURECOM*, Sophia Antipolis, France.
Description 7 months research activity on Rerandomizable RCCA-secure public-key encryption schemes and Identity-Based encryption
Supervisor prof. Antonio Faonio

Education

2021 **Summer School - Foundations and Frontiers of Probabilistic Proofs**, *ETH*, Zurich, Switzerland.
Description Graduate school co-organized by UC Berkeley and the University of Warwick, on proof protocols for delegating computations

2018-2020 **M. Sc. Computer Engineering**, *Sapienza University*, Rome, Italy.
GPA 29.71/30
Final Grade 110/110 cum laude
Thesis *Matchmaking Encryption against Chosen-Ciphertext Attacks*
Advisors prof. Daniele Venturi and prof. Riccardo Lazzeretti

2018-2019 **Mentee at LeadTheFuture**.
Description Series of talks on DevOps, Site Reliability and Release Engineering
Mentor Nicola Timoncini - Google, Zurich (Switzerland)

2017 **CyberChallenge 2017**, *Sapienza University*, Rome, Italy.
Description Member of the first edition of Italian Cyberchallenge, a training program in cybersecurity

2015-2018 **B. Sc. Computer and Systems Engineering**, *Sapienza University*, Rome, Italy.
GPA 29.4/30
Thesis *Minerva*, RoR Platform for Open-Access papers management
Final Grade 110/110 cum laude

Advisor	prof. Leonardo Querzoni
2014	Skysef , <i>Shizuoka Kita Youth Science Engineering</i> , Shizuoka, Japan.
Description	Annual International Forum on Energy
Project	Energy for life
2010-2015	High School , <i>Classical Lyceum "A. Gatto"</i> , Agropoli, Italy.
Final mark	100/100

Publications

2021 Oliva *et al.* - Risks and Protective Factors Associated With Mental Health Symptoms During COVID-19 Home Confinement in Italian Children and Adolescents. doi:10.3389/fped.2021.664702

Under Review

Francati, Guidi, Russo and Venturi - Identity-Based Matchmaking Encryption without Random Oracles. Submitted to CANS 2021

Faonio, Hofheinz, Russo - Almost Tightly-Secure Re-Randomizable and Replayable CCA-secure Public Key Encryption. Submitted to Asiacrypt 2021

Projects

Supervised Projects

During my time at EURECOM, I had the possibility to supervise, together with prof. Faonio, the following semester's spring projects.

Title	Implementing Rerandomizable Public Key Encryption Schemes
Student	Canitano G.

Title	Implementing SNARKs: Verifiable Computation on Encrypted Data
Student	Richard D.

Other Projects

- 2020 **Ped-Pan.** The advent of pan-enteric capsule endoscopy in pediatric Crohn's disease, *Sapienza University*, Rome, Italy.
Role Data manager
- 2020 **Understanding Kids.** Effects of Home Confinement on Children during the Covid-19 Outbreak in Italy, *Sapienza University*, Rome, Italy.
Role Data curation and formal analysis
- 2020 **Milites**, *Visual Analytics tool for Roman battles and wars.*
Description Born as a university project, milites is an innovative d3.js tool for Visual Analytics on ancient Roman history.
- 2020 **Simple Biblio**, *Android epub reader.*
Description An Android ebook reader written in Kotlin that allows downloading ebooks from open libraries and catalogs.

A more detailed list is available at github.com/lrusso96

Computer Skills

Coding C, C++, JAVA, PYTHON, RUBY, CONTEX T, LATEX

Languages

Italian Native

English Self-assessment (CEFR)
Reading C1
Listening B2
Speaking B2
Writing B2

More

Blog I manage a personal blog with cryptography-related notes, exercises, and theoretical definitions, collected as a set of Jekyll posts

Wikimedia	I am an autopatrolled user on Wikipedia and Wikidata, with more than 7k global contributions. I have also developed a set of scripts to make the patrolling easier
Interests	Russian literature