Luigi Russo

Curriculum Vitae

The minutest speck of the living
Is worth more than all that I'll ever do on this earth.

~V. Majakovskij

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- **PhD in Cryptography**, *Sorbonne University and EURECOM*, Sophia Antipolis, France.
Supervisor prof. Antonio Faonio

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**, *Shizuoka Kita Youth Science Engineering*, Shizuoka, Japan.
Description	Annual International Forum on Energy
Project	Energy for life
2010-2015	**High School**, *Classical Lyceum "A. Gatto"*, Agropoli, Italy.
Final mark	100/100

Publications

[FFKRZ23] From Polynomial IOP and Commitments to Non-malleable zkSNARKs. *TCC 2023.*

[FHR23] Almost Tightly-Secure Re-Randomizable and Replayable CCA-secure Public Key Encryption. *PKC 2023.*

[FaoRus22] Mix-Nets from Re-randomizable and Replayable CCA-Secure Public-Key Encryption. *SCN 2022*, doi:10.1007/978-3-031-14791-3_8.

[FGRV21] Identity-Based Matchmaking Encryption Without Random Oracles, *INDOCRYPT 2021*, doi:10.1007/978-3-030-92518-5_19.

[ORGR+21] 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.

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 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 to download ebooks from open libraries and catalogs.

More at **github.com/lrusso96**

Computer Skills

Coding C, C++, Java, Python, Ruby, ConTeXt, LaTeX

Languages

Italian Native

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

French B1

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 Wikimedia projects, with more than 10k global contributions. I have also developed a set of scripts to make the patrolling easier

Interests Russian literature

Contacts

Email russol AT eurecom.fr
Office 372, EURECOM, Digital Security Department

This document was **last updated** on September 30, 2023 at 09:44.