Daniele Friolo

About me:
About me: Currently Post-Doc at University of Salerno at the Cryptography Research Group and PhD candidate in Cryptography at Sapienza University of Rome. My Research topics are on Multi-Party Computation, Zero-Knowledge, Distributed Ledgers/ Blockchains, Digital Contact Tracing.

WORK EXPERIENCE

31/05/2015 – 17/02/2016
MOBILE APP DEVELOPER VIVEREINFORMA SRLS

Android App developer, uGym project: an application focused on geolocalize gyms near a certain place
Address Guidonia

31/01/2017 – 30/09/2017
MOBILE APP DEVELOPER PEZZUTO SRL

- Android app developing

Address Lecce, Italy

EDUCATION AND TRAINING

01/11/2017 – CURRENT Rome, Italy
PHD STUDENT University of Rome "La Sapienza"

Cryptography

Address Rome, Italy

15/01/2015 – 24/10/2017 Rome, Italy
MASTER DEGREE IN COMPUTER SCIENCE Università degli studi "La Sapienza" di Roma

Curriculum: Information science and applications.
Thesis on Cryptography.

Address Rome, Italy

30/09/2009 – 12/01/2015 Rome, Italy
BACHELOR DEGREE IN COMPUTER SCIENCE Università Degli Studi "La Sapienza"

Address Rome, Italy

15/09/2004 – 10/06/2009
DIPLOMA DI SCUOLA SUPERIORE Liceo Scientifico "Lazzaro Spallanzani" di Tivoli

LANGUAGE SKILLS

Mother tongue(s): **ITALIAN**

Other language(s):

	UNDERSTANDING		**SPEAKING**		**WRITING**
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	B2	C1	B2	B2	B2

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

ADDITIONAL INFORMATION

COMMUNICATION AND INTERPERSONAL SKILLS

Communication and interpersonal skills - sharing ideas with a precise explanation of possible methods to realize them in a simple way

JOB-RELATED SKILLS

Job-related skills

- Teaching Math and Computer Science using simple logical schemas, so students can easily understand the subject and go on with the timeline without problems
- Problem solving attitude given by active research in my field

PUBLICATIONS

Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement

Proceedings of Theory of Cryptography Conference 2019
https://eprint.iacr.org/2018/473.pdf – 2019
join work with Daniel Masny and Daniele Venturi

Shielded Computations in Smart Contracts Overcoming Forks

Proceedings of Financial Cryptography and Data Security 2021
https://eprint.iacr.org/2019/891.pdf – 2021
joint work with Vincenzo Botta, Daniele Venturi and Ivan Visconti
https://www.youtube.com/watch?v=C_eZS13RXNI&t=230s

Vision: What If They All Die? Crypto Requirements For Key People

2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
https://ieeexplore.ieee.org/document/9229860 – 2020
joint work with Chan Nam Ngo, Fabio Massacci, Daniele Venturi, Ettore Battaiola

Terrorist Attacks for Fake Exposure Notifications in Contact Tracing System

Proceedings of the 19th International Conference on Applied Cryptography and Network Security 2021
https://eprint.iacr.org/2020/1150.pdf – 2021
join work with Gennaro Avitabile and Ivan Visconti

Affordable Security or Big Guy vs Small Guy

Security Protocols Workshops 2019
2019
joint work with Chan Nam Ngo, Fabio Massacci and Daniele Venturi

PROJECTS

Toolkit for Secure Multi-Party Computation on Ledgers https://priviledge-project.eu/news/toolkit-for-secure-multi-party-computation-on-ledgers
Developed a library to enable the Ethereum blockchain as a communication channel between players interacting in a
Multi-Party Computation protocol.

HOBBIES AND INTERESTS

Taekwondo and acrobatics Actually 2nd dan black belt

Piano