Last Updated on 21st August 2023

Daniele **Friolo**

Contact

Daniele Friolo
daniele.friolo@gmail.com

Languages

Fluent English and Italian

Programming Languages

C, Java, SQL, Solidity.

Education

2017–2021 **Ph.D.** in Cryptography — Sapienza University of Rome - CS Dept.
Thesis: New Perspectives in Multi-Party Computation: Low Round Complexity from New Assumptions, Financial Fairness and Public Verifiability
Supervisor: Prof. Daniele Venturi

2015–2017 **Master Degree** in Computer Science — Sapienza University of Rome - CS Dept.
Thesis: Predictable Arguments
Advisor: Prof. Daniele Venturi

2009–2015 **Bachelor Degree** in Computer Science — Sapienza University of Rome - CS Dept.
Thesis: Android Client and Soa Server Mobile App for Car Pooling
Advisor: Prof. Andrea Sterbini

Academia

2023–now **Assistant Professor** — Sapienza University of Rome. CS Dept.

2021–2023 **Postdoctoral Researcher** — Sapienza University of Rome. CS Dept.
Supervisor: Prof. Daniele Venturi

2020-2021 **Research Fellow** — DIEM - University of Salerno.
Supervisor: Prof. Ivan Visconti

Research Interests

I am an Assistant Professor at the Computer Science Department of Sapienza University of Rome. I work on cryptography. My research topics vary from **Secure Multi-Party Computation**, **Advanced Encryption Schemes**, and **Blockchain Applications**. As a research fellow, I worked on Privacy and Cryptography on Blockchains with the research group of Prof. Ivan Visconti under the PRIViLEDGE project, Horizon 2020. I have been a Postdoctoral Researcher in Distributed Protocols for Digital Contact Tracing during pandemic under the supervision of Prof. Daniele Venturi.

Publications

- **A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement**, Friolo D., Masny D., Venturi D., in Proceedings of Theory of Cryptography Conference (TCC) 2019, Nuremberg, Germany,
- **Affordable Security or Big Guy vs Small Guy**, Friolo D., Nam Ngo C., Massacci F., Venturi D. , in Security Protocols Workshop 2019
- **Shielded Computations in Smart Contracts Overcoming Forks** , Botta V., Friolo D., Visconti I., Venturi D. , in Proceedings of Financial Cryptography and Data Security 2021, Virtual
- **Vision: What If They All Die? Crypto Requirements For Key People**, Ngo C., Friolo D., Massacci F., Venturi D., Battaiola E., in EuroUSec 2020 Workshop, Virtual.
- **Terrorist Attacks for Fake Exposure Notifications in Contact Tracing System**, Avitabile G., Friolo D., Visconti I., in Proceedings of the 19th International Conference on Applied Cryptography and Network Security 2021, Virtual
- **Efficient Proofs of Knowledge for Threshold Relations**, Avitabile G., Botta V., Friolo D., Visconti I., in Proceedings of the 27th European Symposium on Research in Computer Security (ESORICS) 2022, Copenaghen, Denmark.
- **On the Complete Non-Malleability of the Fujisaki-Okamoto Transform**, Friolo D., Salvino M., Venturi D. in Proceeding of the 21st International Conference on Applied Cryptography and Network Security (ACNS 2023), Kyoto, Japan.

- **Cryptographic and Financial Fairness**, Friolo D., Nam Ngo C., Massacci F., Venturi D. in IEEE Transactions on Information Forensics and Security.
- **Multi-Key and Multi-Input Predicate Encryption from Learning with Errors**, Francati D., Friolo D., Malavolta G., Venturi D. in Advances in Cryptology (EUROCRYPT) 2022
- **MARTSIA: Enabling Data Confidentiality for Blockchain-based Process Execution**, Marangone E., Di Ciccio C., Friolo D., Nemmi E. N., Venturi D., Weber I., in Proceedings of the 27th International EDOC Conference (EDOC 2023) (to appear).

Projects

- **SmartDeFi (SERICS)**. I am a Work-Package leader of the SmartDeFi spoke for the SERICS PNRR-funded project. I work on designing and implementing Smart Contracts in the Decentralized Finance context.
- **Toolkit for Secure Multi-Party Computation on Ledgers** (PRIViLEDGE Project HORIZON 2020). Developed a library to enable the Ethereum blockchain as a communication channel between players interacting in a Multi-Party Computation protocol.

Selected Talks

2022 **Shielded Computations in Smart Contracts Overcoming Forks**
Presented at Financial Cryptography and Data Security 2021, Virtual

2021 **Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems**
Presented at the 19th International Conference on Applied Cryptography and Network Security 2021, Virtual.

2019 **On Financial Fairness**
Weekly crypto group talk at CS Dept. Aarhus University, Invited talk at Sapienza University of Rome - CS Dept. (De Cifris Schola Latina seminars)

A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement
Weekly crypto group talk at CS Dept. Aarhus University (DK). Presented at Theory of Cryptography Conference in Nuremberg (Dec 2019)

The Rush Dilemma: Attacking and Repairing Smart Contracts on Forking Blockchains
Invited talk at Chalmers University (SWE), Lund University (SWE) and Weekly COBRA Seminar at CS Dept. Aarhus Unviersity (DK)

Teaching

2022 **Lecturer - 6 CFU** Sapienza University of Rome - CS Dept.
Security in Software Applications

2021 **Lecturer - 6 CFU** University of Trento - DISI
Cryptography, Complexity and Financial Technologies

2019 **Teaching assistant** Sapienza University of Rome - CS Dept.
Architetture degli Elaboratori, Metodologie di Programmazione

Research Visits

2023 **Visiting Researcher - 6 months** George Mason University (USA)
Hosted by Prof. Giuseppe Ateniese, I worked on blockchain and cryptocurrency-related projects.

2019 **Visiting Researcher - 1 year** Aarhus University (DK)
Hosted by Prof. Ivan Damgård, I worked together with Aarhus Crypto Group on MPC projects

Conferences

2023 **CIFRIS 2023** Rome, Italy
Organizing Committee Member and Program Committee Member

2022 **ACNS 2022** Rome, Italy
Session Chair

Peer Review

2022 **Advances in Cryptology (EUROCRYPT), 13th Conference on Security and Cryptography for Networks (SCN), European Symposium on Research in Computer Security (ESORICS), Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)**

2020 **Advances in Cryptology (EUROCRYPT), International Conference on Applied Cryptopraphy and Network Security (ACNS), 19th International Conference on Cryptology and Network Security (CANS), Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)**

2019 **International Cryptology Conference (CRYPTO), IEEE Transactions on Information Forensics and Security (TIFS), International Conference on Applied Cryptopraphy and Network Security (ACNS)**

2018 **IEEE Transactions on Information Forensics and Security (TIFS), International Conference on Practice and Theory in Public Key Cryptography (PKC)**