Last Updated on 24th June 2025

# Daniele **Friolo**

## Contact

Daniele Friolo
daniele.friolo@gmail.com
danielefriolo.github.io

## Languages

Fluent English and Italian

## Programming Languages

C, Python, Java, SQL, Solidity.

## Education

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

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

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 (RTD-A)** — 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 (RTD-A) at the Computer Science Department of Sapienza University of Rome under the PNRR SERICS Grant, where I am a Work-Package Leader for the Spoke-9 project SmartDeFi. I work on cryptography. My research topics vary from **Post-Quantum Cryptography**, **Secure Multi-Party Computation**, **Advanced Encryption Schemes**, **Zero-Knowledge**, **Subversion-Resilient Cryptography**, 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. In 2021, I was a Postdoctoral Researcher in Distributed Protocols for Digital Contact Tracing during the pandemic under the supervision of Prof. Daniele Venturi. During the third year of my Ph.D. I had the chance to visit and work with the Aarhus Crypto Group in Denmark, hosted by Prof. Ivan Damgård, and given an invited talk at the University of Lund and Chalmers University in Sweden. In 2023, I had the chance to work for 6 months as a visiting scholar with Prof. Giuseppe Ateniese at George Mason University in Virginia, USA.

I've published 16 papers in various venues, including top-notch cryptography conferences such as Asiacrypt, Eurocrypt, and TCC.

## 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

## Research Activities

**Decentralized Finance:** As a Work-Package Leader of the Project SmartDeFi, funded by PNRR, in coordination with the partners of the University of Genova (UNIGE) and the University of Milan

(UNIMI), I produced the project deliverables for the Work Package 1 for Resilient Smart Contract Development, Cryptographic Tools, and Design of Large Scale Market Exchange. As a member of the SmartDeFi project, I developed new cryptographic primitives for Advanced Encryption Schemes [7,8,11], Enhanced Zero- knowledge proofs [4,9], and protocols for efficient blockchain-based Central Bank Digital Currencies [16].

**Privacy in Blockchains** As a member of the PRIViLEDGE project, funded by European Union's Horizon 2020 research and innovation programme under grant agreement, I conducted research on blockchain-based attacks against digital contact tracing systems and developed a Toolkit allowing MPC protocol execution with a blockchain as a communication channel with reduced communication time.

**Multi-Party Computation** During my PhD, I conducted research on fully simulatable oblivious transfer protocols [1], financially and cryptographically fair MPC protocols [6], and fork-resilient blockchain-based protocols [2].

**Advanced Encryption Schemes:** During my post-doc, I developed Advanced Encryption schemes such as Multi-Input Predicate Encryption [7,8] and Registered Functional Encryption [11] allowing for decryption against multiple ciphertexts and removal of trusted public key infrastructure in Functional Encryption schemes.

**Post-Quantum Cryptography:** In most of the conducted research, constructing post-quantum secure primitives is one of my main research objectives. Indeed, many of the developed works can be instantiated from standardized post-quantum cryptographic assumptions such as LWE and SIS.

## Selected Publications

1. **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.
   **Short description:** We propose a Simulatable Maliciously Secure Oblivious Transfer from a variety of assumptions, including LWE, known to be Post-Quantum secure.

2. **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.
   **Short description:** We propose a fork-resilient Parallel Coin Tossing protocol from unique signatures, which can be implemented from post-quantum assumptions such as SIS and LWE.

3. **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
   **Short description:** We show a bribing attack against the GAEN contact tracing system that exploits a smart-contract-based blockchain system.

4. **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.
   **Short description:** We show how to instantiate an efficient Proofs for Threshold Relation from a large class of $\Sigma$-protocols.

5. **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.
   **Short description:** We show that the Fujisaki-Okamoto transform, used by the post-quantum NIST standard CRYSTALS-Kyber, enjoys strong security properties.

6. **Cryptographic and Financial Fairness**, Friolo D., Nam Ngo C., Massacci F., Venturi D. in IEEE Transactions on Information Forensics and Security.
   **Short description:** We show that many cryptographically fair protocols are not fair in the financial sense, and propose a new protocol enjoying both of the desired properties (cryptographic and financial fairness).

7. **Multi-Key and Multi-Input Predicate Encryption from Learning with Errors**, Francati D., Friolo D., Malavolta G., Venturi D. in Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2022

**Short description:** We construct Multi-Input and Multi-Key Predicate Encryption for a large class of predicates from the standard post-quantum assumption LWE.

8. **Multi-Key and Multi-Input Predicate Encryption (for Conjunctions) from Learning with Errors**, Francati D., Friolo D., Malavolta G., Venturi D. in Journal of Cryptology.
**Short description:** We construct Multi-Input and Multi-Key Predicate Encryption for a large class of predicates (conjunctions) from the standard post-quantum assumption LWE.

9. **Compact proofs of partial knowledge for overlapping CNF formulae** Avitabile, G., Botta, V., Friolo, D., Venturi, D., Visconti, I. (2025). In Journal of Cryptology.
**Short description:** We construct Proofs or Partial Knowledge for CNF formulae sharing literals in an efficient manner.

10. **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).
**Short description:** We construct a blockchain-based process management system with strong privacy guarantees from Attribute-Based Encryption, which can be constructed from post-quantum assumptions.

11. **Registered (Inner-Product) Functional Encryption**, Francati, D., Friolo, D., Maitra, M., Malavolta, G., Rahimi, A., Venturi, D. in International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2023, Guangzhou, China
**Short description:** We construct an efficient Registered Functional Encryption scheme (RFE) for Inner-Product, and a generic RFE scheme from indistinguishability obfuscation.

## Other Publications

12. **Affordable Security or Big Guy vs Small Guy**, Friolo D., Nam Ngo C., Massacci F., Venturi D. , in Security Protocols Workshop 2019

13. **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.

14. **Data Redaction in Smart-Contract-Enabled Blockchains**, Avitabile, A., Botta V., Friolo, D., Visconti, I. in 6th Distributed Ledger Technologies Workshop (DLT) 2024, Turin, Italy

15. **Data Redaction in Smart-Contract-Enabled Blockchains**, Avitabile, A., Botta V., Friolo, D., Visconti, I. in Blockchain: Research And Applications Journal.

16. **Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance**, Friolo, D., Goodell G., Toliver D. and Al Nakib H. D. in Financial Cryptography Workshops.

# Selected Talks

2025 **Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance**
Presented at Financial Cryptography and Data Security Conference Workshops (CoDecFin), 2025 at Miyakojima, Japan, and, as an invited talk, at the CrypTO Local Conference in Turin, Italy.

2024 **Data Redaction in Smart-Contract-Enabled Blockchains**
Presented at the 6th Distributed Ledger Technologies Workshop (DLT) 2024 in Turin, Italy.

2023 **Registered (Inner-Product) Functional Encryption**
Presented at the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2023 in Guangzhou, China.

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

2024/25 **Lecturer - 20 hours** Sapienza University of Rome - CS Dept - PhD course in Cybersecurity
Post-Quantum Cryptography
Topics: Lattices, Post-Quantum NIST Standards, Basic and Advanced Cryptographic primitives from Lattice-Based assumptions.

2024/25 **Lecturer - 6 CFU** Sapienza University of Rome - MSc in Cybersecurity
Ethical Hacking

2024/25 **Lecturer - 3 CFU** Sapienza University of Rome - BSc in Computer Science
Fondamenti di Programmazione (Programming I)

2024/25 **Lecturer - 6 CFU** Sapienza University of Rome - MSc in CS/Cybersecurity
Security in Software Applications

2023/24 **Lecturer - 6 CFU** Sapienza University of Rome - MSc in Cybersecurity
Ethical Hacking

2023/24 **Lecturer - 3 CFU** Sapienza University of Rome - MSc in CS/Cybersecurity
Security in Software Applications

2022/23 **Lecturer - 6 CFU** Sapienza University of Rome - MSc in CS/Cybersecurity
Security in Software Applications

2021/22 **Lecturer - 6 CFU** University of Trento - MSc in Computer Science
Cryptography, Complexity and Financial Technologies

2019/20 **Teaching assistant** Sapienza University of Rome - BSc in Computer Science
Architetture degli Elaboratori, Metodologie di Programmazione

# Thesis Advising

2025 **Filippo Trotter** University of Trento - Math Dept - MSc in Math.
Thesis Title: Quantum Vulnerabilities in Verifiable Credentials: SD-JWT vs. BBS+ and the Path Forward.

2024 **Giuseppe Di Naso** Sapienza University of Rome - CS Dept - MSc in Cybersecurity.
Thesis Title: Embedding Post-quantum Cryptography inside SmartCards.

2024 **Cosmo Greco** Sapienza University of Rome - CS Dept - MSc in Cybersecurity.
Thesis Title: Enhancing security by design processes: analysis of best practices, frameworks, technologies and improvement with digital forensics.

2024 **Francesco Alessandrini** Sapienza University of Rome - CS Dept - MSc in Cybersecurity.
Thesis Title: A Comparative Analysis of Modern Smart Contract Vulnerabilities Detection Mechanisms.

2021 **Matteo Castagna** University of Trento - DISI - MSc in Computer Science.
Thesis Title: SmartDECO: Fully Decentralized Markets Based On Ethereum Smart Contracts And Decentralized Tls Oracles.

2021 **Helidona Shabani** University of Trento - DISI - MSc in Computer Science.
Thesis Title: Blockchain Securitization: An Innovative And Decentralized Technology To Tokenize And Implement Digital Assets.

# Conferences Committees

2026 **Eurocrypt 2026** Rome, Italy
Workshop Chair

2024 **AISec2024 Workshop (co-located w. CCS)** Salt Lake City, USA
Program Committee Member

**CIFRIS 2024** Rome, Italy
Program Committee Member

2023 **CIFRIS 2023** Rome, Italy
Conference co-Chair and Program Committee Member

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

# Other Experiences

2024 **Where: Ministero Degli Esteri, Rome**
Invited to join the conference “Ecosistema Nazionale di Cyber Capacity Building” as a rapresentative of Dipartimento di Informatica, Sapienza University of Rome, Rome, Italy.

2024 **Where: Sala del Refettorio, Camera dei deputati, Rome**
Invited to join the conference “Crittografia e imprese per il Paese” as a researcher and member of DeCifris association.

## Peer Review

2025 **IEEE Symposium on Security and Privacy (IEEE S&P), the 44th Annual International Cryptology Conference (CRYPTO), Transactions on Information Forensics and Security (TIFS), IEEE Transactions on Dependable and Secure Computing (TDSC).**

2024 **14th Conference on Security and Cryptography for Networks (SCN), International Colloquium on Automata, Languages, and Programming (ICALP), IEEE International Conference on Web Services (ICWS) , Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), ACM Conference on Computer and Communications Security (CCS), International Conference on Practice and Theory in Public Key Cryptography (PKC), Transactions on Information Forensics and Security (TIFS)**

2023 **International Conference on Applied Cryptopraphy and Network Security (ACNS), European Symposium on Research in Computer Security (ESORICS), Elsevier Theoretical Computer Science (TCS), Elsevier Vehicular Communications**

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 **Annual International Conference on the Theory and Applications of Cryptographic Techniques (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)**