DANIELE FRIOLO
Curriculum Vitae

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 project SmartDeFi.
I work in *cryptography*. My research topics vary from **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. For the entire 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 and multiple seminars at the weekly meetings and the COBRA meeting at the Computer Science Department of Aarhus University in Denmark.
In 2023, I had the chance to work for 6 months as a visiting scholar hosted by Prof. Giuseppe Ateniese at George Mason University in Virginia, USA.
I have been part of the Organizational Committee of the national cryptographic conference CIFRIS23.
I had the honor to serve as a Program Committee Member of the international cryptographic conferences CIFRIS23 and CIFRIS24. I am part of the Program Committee of the AiSec Workshop co-located with ACM CCS conference 2024.

Part I – General Information

Full Name	Daniele Friolo
Date of Birth	24/10/1990
Place of Birth	Roma
Citizenship	Italian
Spoken Languages	Italian, English

Part II – Education

Type	Year	Institution	Notes (Degree, Experience,…)
PhD	2021	Sapienza University of Rome	Area: *Cryptography*
			Thesis: *New perspectives in multi-party computation: low round complexity from new assumptions, financial fairness and public verifiability.*
			Supervisor: Prof. Daniele Venturi
Post-graduate studies	2017	Sapienza University of Rome	Master Degree
			Thesis: *Predictable Arguments*
			Advisor: Prof. Daniele Venturi
University graduation	2015	Sapienza University of Rome	Bachelor Degree

Part III – Appointments

IIIA – Academic Appointments

Start	End	Institution	Position
04/2023	Ongoing	DI, Sapienza University of Rome	RTD-A
07/2021	03/2023	DI, Sapienza University of Rome	Postdoc
06/2020	05/2021	DIEM, University of Salerno	Research Fellow

IIIB – Other Appointments

Start	End	Institution	Position
04/2023	10/2023	George Mason University, VA, USA	**Visiting Scholar**
			*Host***:** Prof. Giuseppe Ateniese
01/2019	05/2020	Aarhus University, Denmark	**Visiting PhD Student**
			Host: Prof. Ivan Damgaard

Part IV – Teaching experience

Part IV.1 -Teaching

Year	Institution	Experience
2025	DI, Sapienza University of Rome	**3CFU - Course:** Post-Quantum Cryptography – Cybersecurity PhD Course
2025	DI, Sapienza University of Rome	**6CFU - Course:** Ethical Hacking — Master in Cybersecurity
2024	DI, Sapienza University of Rome	**6CFU - Course:** Security in Software Applications — Master in Computer Science/Cybersecurity
2024	DI, Sapienza University of Rome	**3CFU - Course:** Fondamenti di Programmazione
2023	DI, Sapienza University of Rome	**6CFU - Course:** Ethical Hacking — Master in Cybersecurity
2023	DI, Sapienza University of Rome	**3CFU - Course:** Security in Software Applications — Master in Computer Science/Cybersecurity
2022	DI, Sapienza University of Rome	**6CFU - Course**: Security in Software Applications –- Master in Computer Science/Cybersecurity
2021	DISI, University of Trento	**6CFU - Course:** Complexity, Cryptography and Financial Technologies — Master in Computer Science

Part IV.2 –Thesis Advising

2025 ongoing	Dipartimento di Matematica, Università di Trento – Master in Mathematics	Filippo Trotter *Thesis title*: Selective Disclosure Post Quantum credentials
2024	DI, Sapienza – Master in Cybersecurity	Giuseppe Di Naso *Thesis title*: Embedding Post-quantum Cryptography inside SmartCards
2024	DI, Sapienza – Master in Cybersecurity	Greco Cosmo *Thesis title*: Enhancing security by design processes: analysis of best practices, frameworks, technologies and improvement with digital forensics
2024	DI, Sapienza – Master in Cybersecurity	Francesco Alessandrini *Thesis title*: A Comparative Analysis of Modern Smart Contract Vulnerabilities Detection Mechanisms
2021	DISI, University of Trento – Master in Computer Science	Matteo Castagna *Thesis title*: SmartDECO: Fully Decentralized Markets Based On Ethereum Smart Contracts And Decentralized Tls Oracles
2021	DISI, University of Trento – Master in Computer Science	Helidona Shabani. *Thesis title*: Blockchain Securitization: An Innovative And Decentralized Technology To Tokenize And Implement Digital Assets

Part V – Research Activities

Keywords	Brief Description
Decentralized Finance	As a Work-Package Leader of the Project SmartDeFi, funded by PNRR, in coordination with the partner university of UNIGE and UMIMI, he 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, he developed new cryptographic primitives for Advanced Encryption Schemes [1,2,5], Enhanced Zero-knowledge proofs [4,6], and protocols for efficient blockchain-based Central Bank Digital Currencies [12].
Privacy in Blockchains	As a member of the PRIViLEDGE project, funded by European Union's Horizon 2020 research and innovation programme under grant agreement, he conducted research on blockchain-based attacks against digital contract tracing systems [8] and developed a Toolkit allowing MPC protocol execution with a blockchain as a communication channel with reduced communication time [15].
Multi-Party Computation	During his PhD, he conducted research on fully simulatable oblivious transfer protocols [3], financially and cryptographically fair MPC protocols [10], and fork-resilient blockchain-based protocols [7].
Advanced Encryption Schemes	During his post-doc, he developed Advanced Encryption Scheme such as Multi-Input Predicate Encryption [1,5] and Registered Functional Encryption [2] allowing for decryption against multiple ciphertexts and removal of trusted public key infrastructure in Functional Encryption schemes.

Part VI – Program Committees and Peer Review

Workshop General Chair of the IACR top-notch international conference EUROCRYPT 2026, that will be held in Rome at May 2025

Conference Chair of the international conference CIFRIS23, held in Rome at October 2023

Program Committee Member of the following conferences:

- 2024: AiSec workshop, collocated with The ACM Conference on Computer and Communications Security (CCS) international conference
- 2024: CIFRIS24, Rome
- 2023: CIFRIS23, Rome

Served as a *peer reviewer* for the following conferences/journals:

- 2025: IEEE Symposium on Security and Privacy 2024 (IEEE S&P), Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Transactions on Dependable and Secure Computing
- 2024: IEEE Symposium on Security and Privacy 2024 (IEEE S&P), 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 (ACM CCS), International Conference on Practice and Theory in Public Key Cryptography (PKC)
- 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).
- 2021: 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)
- 2020: International Cryptology Conference (CRYPTO), IEEE Transactions on Information Forensics and Security (TIFS), International Conference on Applied Cryptopraphy and Network Security (ACNS)
- 2019: IEEE Transactions on Information Forensics and Security (TIFS), International Conference on Practice and Theory in Public Key Cryptography (PKC)

Session chair at

- ASIACRYPT 2023, Guangzhou, China
- ACNS 2022, Rome, Italy

Part VII – Selected Talks

Part VII.1 – Conference Paper Presentations

Year	Where	Seminar Title
2025	Financial Cryptography and Data Security 2025 Workshops	Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance
2024	DLT24 Workshop – Turin, Italy	Data Redaction in Smart-Contract-Enabled Blockchains
2023	The International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2023 in Guangzhou, China.	Registered (Inner-Product) Functional Encryption
2021	Financial Cryptography and Data Security 2021, Virtual	Shielded Computations in Smart Contracts Overcoming Forks
2021	9th International Conference on Applied Cryptography and Network Security (ACNS) 2021, Virtual.	Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems
2019	Theory of Cryptography Conference in Nuremberg, Germany	A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement

Part VII.2 – Invited Talks

2022	Workshop on Privacy preserving systems, software and tools, Rome	Multi-Key and Multi-Input Predicate Encryption from Learning with Errors
2019	COBRA Seminars - Computer Science dept, University of Aarhus	The Rush Dilemma: Attacking and Repairing Smart Contracts on Forking Blockchains
	University of Lund, SWE – Security Seminars	
	Chalmers University, SWE – Security and Privacy Lab	
2019	De Cifris Schola Latina seminars – DI, Sapienza University of Rome	On Financial Fairness
2019	Crypto Weekly Seminar - Computer Science dept, University of Aarhus	A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement

Part VII – Summary of Scientific Achievements

Product type	Number	Data Base	Start	End
Papers [international]	14	DBLP	2018	2025

Total Impact factor	11,396 (Scimago)
Total Citations	141 (Google Scholar), 44 (Scopus)
Average Citations per Product	9,5 (Google Scholar), 2,92 (Scopus)
Hirsch (H) index	7 (Google Scholar), 5 (Scopus)

Part VIII – Other Experiences

Year	Where	Experience
2024	Ministero Degli Esteri, Rome	Invited to join the conference "Ecosistema Nazionale di Cyber Capacity Building" as a rapresentative of Dipartimento di Informatica
2024	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.

Part VIII–Publications

Part VIII.1– Selected Publications

[1] Francati, D., **Friolo, D**., Malavolta, G., & Venturi, D. (2023, April). Multi-key and multi-input predicate encryption from learning with errors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)* (pp. 573-604). Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-30620-4_19

Conference Rating of EUROCRYPT:
GII-GRIN-SCIE (GGS): **A++**

[2] Francati, D., **Friolo, D.,** Maitra, M., Malavolta, G., Rahimi, A., & Venturi, D. (2023, December). Registered (inner-product) functional encryption. In *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)* (pp. 98-133). Singapore: Springer Nature Singapore. DOI: https://doi.org/10.1007/978-981-99-8733-7_4

Conference Rating of ASIACRYPT:
GII-GRIN-SCIE (GGS): **A+**

[3] **Friolo, D.,** Masny, D., & Venturi, D. (2019). A black-box construction of fully-simulatable, round-optimal oblivious transfer from strongly uniform key agreement. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I 17* (pp. 111-130). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-36030-6_5

Conference Rating of TCC:
GII-GRIN-SCIE (GGS): **A+**

[4] Avitabile, G., Botta, V., **Friolo, D.,** & Visconti, I. (2022, September). Efficient proofs of knowledge for threshold relations. In *European Symposium on Research in Computer Security (ESORICS)* (pp. 42-62). Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-17143-7_3

Conference Rating of TCC:
GII-GRIN-SCIE (GGS): **A+**

[5] Francati, D., **Friolo, D.,** Malavolta, G., & Venturi, D. (2024). Multi-key and Multi-input Predicate Encryption (for Conjunctions) from Learning with Errors. *Journal of Cryptology*, *37*(3), 24. DOI: https://doi.org/10.1007/978-3-031-30620-4_19

Journal of Cryptology
Ranking: **Q1** (Scimago)
Impact Factor: **3.125** (Scimago)

[6] Avitabile, G., Botta, V., Friolo, D., Venturi, D., & Visconti, I. (2025). Compact proofs of partial knowledge for overlapping CNF formulae. *Journal of Cryptology*, *38*(1), 7.

Ranking: **Q1** (Scimago)
Impact Factor: **3.125** (Scimago)

[7] Botta, V., **Friolo, D.,** Venturi, D., & Visconti, I. (2021). Shielded computations in smart contracts overcoming forks. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25* (pp. 73-92). Springer Berlin Heidelberg. DOI: https://doi.org/10.1007/978-3-662-64322-8_4

Conference Rating of FC:
GII-GRIN-SCIE (GGS): **A**

[8] Avitabile, G., **Friolo, D.,** & Visconti, I. (2021, June). Terrorist attacks for fake exposure notifications in contact tracing systems. In *International Conference on Applied Cryptography and Network Security (ACNS)* (pp. 220-247). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-78372-3_9

Conference Rating of ACNS:
GII-GRIN-SCIE (GGS): **A-**

[9] **Friolo, D.,** Salvino, M., & Venturi, D. (2023, May). On the complete non-malleability of the Fujisaki-Okamoto transform. In *International Conference on Applied Cryptography and Network Security* (pp. 307-335). Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-33491-7_12

Conference Rating of ACNS:
GII-GRIN-SCIE (GGS): **A-**

[10] **Friolo, D.,** Massacci, F., Ngo, C. N., & Venturi, D. (2022). Cryptographic and financial fairness. *IEEE Transactions on Information Forensics and Security*, *17*, 3391-3406. DOI**:** 10.1109/TIFS.2022.3198852

Ranking: **Q1** (Scimago)
Impact Factor: **8.271** (Scimago)

[11] Marangone, E., Di Ciccio, C., Friolo, D., Nemmi, E. N., Venturi, D., & Weber, I. (2023, October). MARTSIA: enabling data confidentiality for blockchain-based process execution. In *International Conference on Enterprise Design, Operations, and Computing (EDOC)* (pp. 58-76). Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-46587-1_4

Conference Rating of EDOC:
GII-GRIN-SCIE (GGS): **B**

[12] **Friolo, D.,** Goodell G., Toliver D. and Al Nakib H. D. *Financial Cryptography and Data Security Workshops FC 2025* (volume to appear).

Part VIII.2 – Other Publications

[13] Friolo, D., Massacci, F., Ngo, C. N., & Venturi, D. (2020). Affordable Security or Big Guy vs Small Guy: Does the Depth of Your Pockets Impact Your Protocols?. In *Security Protocols XXVII: 27th International Workshop, Cambridge, UK, April 10–12, 2019, Revised Selected Papers 27* (pp. 135-147). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-57043-9_13

[14] Ngo, C. N., Friolo, D., Massacci, F., Venturi, D., & Battaiola, E. (2020, September). Vision: What If They All Die? Crypto Requirements For Key People. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 178-183). IEEE. DOI**:** 10.1109/EuroSPW51379.2020.00032

[15] MPC Toolkit. https://github.com/danielefriolo/ledgerMPC