procedura selettiva di chiamata per n. 1 posto di **Ricercatore a tempo determinato - Tipologia A** presso il Dipartimento di Informatica, Facoltà di Ingegneria dell'Informazione, Informatica e Statistica Settore Scientifico-disciplinare INF/01, Settore concorsuale 01/B1 di cui al bando emanato con D.D. n. 3138/2021, 3277/2021, 341/2022, 931/2022, 3264/2021 con avviso pubblicato sulla G.U. – IV serie speciale n. 5 in data 20/01/23, codice concorso 2023RTDAPNRR074

Daniele Friolo
Curriculum Vitae

Part I – General Information

Full Name	Daniele Friolo
Spoken Languages	Italian, English

Part II – Education

Type	Year	Institution	Notes (Degree, Experience,…)
University graduation	2015	Università di Roma "La Sapienza"	Bachelor Degree
Post-graduate studies	2017	Università di Roma "La Sapienza"	Master Degree
PhD	2021	Università di Roma "La Sapienza"	PhD

Part III – Appointments

IIIA – Academic Appointments

Start	End	Institution	Position
01/07/20	31/06/21	Università di Salerno	Assegnista di ricerca / Research fellow
01/08/21	now	Università di Roma "La Sapienza"	Assegnista di ricerca / Research fellow

IIIB – Other Appointments

Start	End	Institution	Position

Part IV – Teaching experience

Year	Institution	Lecture/Course

2021	Università di Trento	Complexity, Cryptography and Financial Technologies
2022	Università di Roma “La Sapienza”	Security in Software Applications

Part V - Society memberberships, Awards and Honors

Year	Title

Part VI - Funding Information [grants as PI-principal investigator or I-investigator]

Year	Title	Program	Grant value

Part VII – Research Activities

Keywords	Brief Description
Multi-party Computation	Secure evaluation of functions in a distributed setting with the aid of DLT (Distributed Ledger Technologies). New constructions and new primitives for Secure MPC and Predicate Encryption. Improved constructions of zero-knowledge proofs.
Zero-knowledge.	
Blockchain applications	
predicate encryption	

Part VIII – Summary of Scientific Achievements

Product type	Number	Data Base	Start	End
Papers [international]	8	Google scholar / dblp	2018	2023
Papers [national]				
Books [scientific]				
Books [teaching]				

Total Impact factor	8.278
Total Citations	45
Average Citations per Product	5
Hirsch (H) index	4

Part IX– Selected Publications

List of the publications selected for the evaluation. For each publication report title, authors, reference data, journal IF (if applicable), citations, press/media release (if any).

[1] Friolo, D., Masny, D., & Venturi, D. (2019, December). A black-box construction of fully-simulatable, round-optimal oblivious transfer from strongly uniform key agreement. In *Theory of Cryptography Conference* (pp. 111-130). Springer, Cham. Citations: 4
[2] Botta, V., Friolo, D., Venturi, D., & Visconti, I. (2021, March). Shielded computations in smart contracts overcoming forks. In *International Conference on Financial Cryptography and Data Security* (pp. 73-92). Springer, Berlin, Heidelberg. Citations: 1
[3] 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* (pp. 220-247). Springer, Cham. Citations: 2
[4] 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.
[5] Friolo, D., Massacci, F., Ngo, C. N., & Venturi, D. (2022). Cryptographic and financial fairness. *IEEE Transactions on Information Forensics and Security*, *17*, 3391-3406. Journal

[6] Avitabile, G., Botta, V., Friolo, D., & Visconti, I. (2022, September). Efficient proofs of knowledge for threshold relations. In *Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III* (pp. 42-62). Cham: Springer Nature Switzerland.

[7] Friolo, D., Massacci, F., Ngo, C. N., & Venturi, D. (2019, April). Affordable Security or Big Guy vs Small Guy. In *Cambridge International Workshop on Security Protocols* (pp. 135-147). Springer, Cham.
[8] Friolo, D., Salvino M., Venturi V., (2023). On the Complete Non-Malleability of the Fujisaki-Okamoto Transform. The 21st International Conference on Applied Cryptography and Network Security (ACNS 2023). Kyoto, Japan 19,22 Juner 2023. To appear

Roma, 26/01/23