Danilo Francati

Curriculum Vitae

✉ *dfrancati@cs.au.dk*
✉ *danilofrancati@gmail.com*
in *danilo-francati*
G *Scholar*
dblp
iD *0000-0002-4639-0636*

Positions

Sep. '21-Present **Postdoc in Cryptography**, *Aarhus University (Aarhus Crypto Group, Webpage)*, Denmark.

Dec. '15-Nov. '16 **Graduate Student Researcher**, *Sapienza University of Rome*, Italy.
Supervisor: Prof. Chiara Petrioli.

Education

Aug. '17-Sep. '21 **Ph.D. in Computer Science**, *Stevens Institute of Technology*, NJ, US.
Major: Cryptography.
Advisor: Prof. Giuseppe Ateniese.
Dissertation: *Kolmogorov Complexity and Cryptography: New Connections and Applications to Space-demanding Functions.*

Oct. '14-July '16 **M. Sc. Computer Science**, *Sapienza University of Rome*, Italy.
Final Grade: 110/110 Summa Cum Laude (GPA: 29.77/30).
Thesis: *Practical Backdoors for PRNGs Enabling Mass Surveillance*.
Advisor: Prof. Giuseppe Ateniese.

Oct. '11-July '14 **B. Sc. Computer Science**, *Sapienza University of Rome*, Italy.
Final Grade: 110/110 Summa Cum Laude (GPA: 28.81/30).
Thesis: *Link Prediction in Large Crowds: Gli Smartphone Probes Raccontano chi Frequenti e Dove*.
Advisor: Prof. Alessandro Mei.

Grants

Sep. '21 **RFP-009 on Proofs of Space and Useful Space**, *Protocol Labs*, PI/co-PI and researcher ($50.000, 00).
Topic: New constructions of verifiable capacity-bound functions.

Publications

Preprints

Under Submission **Registered (Inner-Product) Functional Encryption**, *Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta, Ahmadreza Rahimi, and Daniele Venturi*

Conference Proceedings

EUROCRYPT 23 (To appear) **Multi-key and Multi-input Predicate encryption from Learning with Errors**, *Danilo Francati, Daniele Friolo, Giulio Malavolta, and Daniele Venturi*, Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, URL `https://eprint.iacr.org/2022/806`

PKC 23 (To appear) **Structure-Preserving Compilers from New Notions of Obfuscations**, *Matteo Campanelli, Danilo Francati, and Claudio Orlandi*, 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, URL `https://eprint.iacr.org/2022/732`

PKC 23 (To appear) **Verifiable Capacity-bound Functions: A New Primitive from Kolmogorov Complexity (Revisiting space-based security in the adaptive setting)**, *Giuseppe Ateniese, Long Chen, Danilo Francati, Dimitrios Papadopoulos, and Qiang Tang*, 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, URL https://eprint.iacr.org/2021/162

CCS 22 **Eluding Secure Aggregation in Federated Learning via Model Inconsistency**, *Dario Pasquini, Danilo Francati, and Giuseppe Ateniese*, Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022, pp. 2429-2443, ISBN 978-1-4503-9450-5, URL https://dl.acm.org/doi/10.1145/3548606.3560557

INDOCRYPT 21 **Identity-Based Matchmaking Encryption without Random Oracles**, *Danilo Francati, Alessio Guidi, Luigi Russo, and Daniele Venturi*, International Conference on Cryptology in India. Springer, Cham. 2021, pp. 415-435, Lecture Notes in Computer Science 13143, ISBN 978-3-030-92518-8, URL https://link.springer.com/chapter/10.1007/978-3-030-92518-5_19

SBC 21 **Audita: A Blockchain-based Auditing Framework for Off-chain Storage**, *Danilo Francati, Giuseppe Ateniese, Abdoulaye Faye, Andrea Maria Milazzo, Angelo Massimo Perillo, Luca Schiatti, and Giuseppe Giordano*, Proceedings of the 9th International Workshop on Security in Blockchain and Cloud Computing. 2021. ISBN 978-1-4503-8405-6, URL https://dl.acm.org/doi/abs/10.1145/3457977.3460293

CANS 20 **Arcula: A secure hierarchical deterministic wallet for multi-asset blockchains**, *Adriano Di Luzio, Danilo Francati, and Giuseppe Ateniese*, International Conference on Cryptology and Network Security. Springer, Cham, 2020. pp. 323-343, Lecture Notes in Computer Science 12579, ISBN 978-3-030-65410-8, URL https://link.springer.com/chapter/10.1007/978-3-030-65411-5_16

ACNS 19 **Public immunization against complete subversion without random oracles**, *Giuseppe Ateniese, Danilo Francati, Bernardo Magri, and Daniele Venturi*, International Conference on Applied Cryptography and Network Security. Springer. 2019, pp. 465–485, Lecture Notes in Computer Science 11464, ISBN 978-3-030-21567-5, URL https://link.springer.com/chapter/10.1007/978-3-030-21568-2_23

CRYPTO 19 **Match me if you can: Matchmaking encryption and its applications**, *Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi*, Annual International Cryptology Conference. Springer, Cham. 2019, pp. 701–731, Lecture Notes in Computer Science 11693, ISBN 978-3-030-26950-0, URL https://link.springer.com/chapter/10.1007/978-3-030-26951-7_24

Journals

Journal of Cryptology **Match me if you can: Matchmaking encryption and its applications**, *Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi*, Journal of Cryptology, 34.16, (2021). DOI: 10.1007/s00145-021-09381-4, URL https://link.springer.com/article/10.1007/s00145-021-09381-4

Theoretical Computer Science **Immunization against complete subversion without random oracles**, *Giuseppe Ateniese, Danilo Francati, Bernardo Magri, and Daniele Venturi*, Theoretical Computer Science. 2021. DOI: 10.1016/j.tcs.2021.01.002, URL https://www.sciencedirect.com/science/article/abs/pii/S0304397521000190

Talks

November ’22 **Invited talk @ Seminars in Cybersecurity [link]**, *Sapienza University of Rome, Rome, Italy.*
Title: *Eluding Secure Aggregation in Federated Learning via Model Inconsistency.*

July ’22 **Talk @ Crypto Day**, *Aarhus University, Aarhus, Denmark.*
Title: *Structure-Preserving Compilers from New Notions of Obfuscations.*

January ’22 **Invited talk @ SPRING Lab (EPFL)**, *Online due to COVID-19.*
Title: *Anonymous Communication: Matchmaking Encryption.*

June '21 **Author & Speaker @ SBC workshop (held in conjunction with ASIACCS21)**, *Online due to COVID-19.*

Title: *Audita: A Blockchain-based Auditing Framework for Off-chain Storage.*

February '21 **Talk @ Aarhus Crypto Group (Aarhus University) [link]**, *Online due to COVID-19.*

Title: *Kolmogorov complexity and cryptography: New connections and applications to space-demanding functions.*

February '21 **Talk @ IMDEA Software [link]**, *Online due to COVID-19.*

Title: *Kolmogorov complexity and cryptography: New connections and applications to space-demanding functions.*

December '20 **Author & Speaker @ CANS20 [▶ Video]**, *Online due to COVID-19.*

Title: *Arcula: A Secure Hierarchical Deterministic Wallet for Multi-asset Blockchains.*

August '19 **Author & Speaker @ CRYPTO19 [▶ Video]**, *Santa Barbara, California, US.*

Title: *Match me if you can: matchmaking encryption and its applications.*

June '19 **Author & Speaker @ ACNS19**, *Bogotà, Colombia.*

Title: *Public immunization against complete subversion without random oracles.*

Organization and Participation in Conferences/Journals

Program Committee *5th Distributed Ledger Technology Workshop (DLT 2023) May 25-26 2023*, Bologna, Italy.

Subreviewer (Conferences) *CANS 18, CRYPTO 19, PKC 20, CANS 21, CT-RSA 22, CRYPTO 22, CCS 22, TCC 22, Usenix Security 23, EUROCRYPT 23, ACNS 23, ISIT 23.*

Reviewer (Journals) *IEEE Transactions on Information Forensics and Security, IEEE Transaction on Dependable and Secure Computing, The Computer Journal, Journal of Systems Architecture, IET Information Security.*

Session Chair *Track: Advanced Public Key Primitives @ CCS 22, Los Angeles, CA.*

Other Experiences

Students Supervision

Feb. '23-Present **Co-supervising Bachelor project (Supervisor: Prof. Claudio Orlandi)**, *Aarhus University*, Topic: Consensus algorithms in blockchains.

Feb. '23-Present **Co-supervising Bachelor project (Supervisor: Prof. Claudio Orlandi)**, *Aarhus University*, Topic: Cloud security.

Jan. '20-July '20 **Co-supervising M. Sc. Thesis (Supervisor: Prof. Daniele Venturi and Prof. Riccardo Lazzeretti)**, *Sapienza University of Rome.*

Student: Luigi Russo. Thesis Title: Matchmaking Encryption against Chosen-Ciphertext Attacks [link].

Awards and Scholarships

Aug. '18-Jun. '19 **I&E Fellowship**, *offered by Stevens Institute of Technology*, NJ, US.

Aug. '17-Jun. '18 **Provost's Doctoral Fellowship**, *offered by Stevens Institute of Technology*, NJ, US.

Dec. '15-Nov. '16 **Graduate Student Research Scholarship offered by Prof. Chiara Petrioli**, *Sapienza University of Rome*, Italy.

Sep. '12-July '16 **LazioDisu Scholarship**, *Rome*, Italy.

July '16 **LazioDisu M. Sc. degree award**, *Rome*, Italy.

July '14 **LazioDisu B. Sc. degree award**, *Rome*, Italy.

Nov. '13 **Travel grant to ACM Sensys '13**, *Sapienza University of Rome*, Italy.

June '15 **Top three final projects Twitter4Uni contest [link article Italian only]**, *Milan*, Italy.

Languages

Italian (Mother tongue), English.

“Treatement of personal informations is authorised according to the privacy laws (D. Lgs 679/2016)”.