europass Curriculum vitae

INFORMAZIONI PERSONALI

Daniele Friolo

APPLICAZIONE PER Bando DOC 03/2022

INTERESSI LAVORATIVI

Il mio interesse primario è nel campo della **Crittografia**. Il mio lavoro si incentra su ricerca nell'ambito della **Secure Multi-Party Computation** e applicazioni nelle **Blockchain**. Dato l'avvento della pandemia, ho approfondito attacchi e soluzioni crittografiche per **Digital Contact Tracing**. Ho fatto parte come assegnista in "privacy e crittografia nelle blockchain" nel gruppo di ricerca del prof. Ivan Visconti al DIEM dell'Università di Salerno e come assegnista in "progetto di protocolli distribuiti per il tracciamento dei contatti in pandemia" con il gruppo di ricerca del Prof. Daniele Venturi al dipartimento di Informatica dell'Università di Roma "La Sapienza". Durante il mio percorso di dottorato ho avuto la fortuna di visitare e lavorare con il gruppo di ricerca di Secure Multi-Party Computation del Prof. Ivan Damgård alla Aarhus University in Danimarca.
Ho insegnato in lingua inglese il corso di "Complexity, Cryptography and Financial Technologies" al DISI dell'Università di Trento per l'annualità 2021/2022.

ESPERIENZE LAVORATIVE

Ottobre 2021 – Settembre 2022

Professore a contratto

Corso di Complexity, Cryptography and Financial Technologies
DISI, Università di Trento

Agosto 2021 – Adesso

Assegnista di Ricerca

Protocolli distribuiti per il tracciamento dei contatti in pandemia
Dipartimento di Informatica, Università di Roma "La Sapienza"

Luglio 2020 – Maggio 2021

Assegnista di Ricerca

Privacy e Crittografia nelle Blockchain
DIEM, Università di Salerno

ISTRUZIONE

Novembre 2017–Luglio 2021

PhD - Titolo Tesi: "New Perspectives in Multi-Party Computation: Low Round Complexity from New Assumptions, Financial Fairness and Public Verifiability [1]

Università di Roma "La Sapienza"
Supervisore: Prof. Daniele Venturi

2009–2015

Laurea Magistrale in Informatica

Università di Roma "La Sapienza"
Tesi: Predictable Arguments
Relatore: Prof. Daniele Venturi

2015–2017

Laurea Triennale in Informatica

Università di Roma "La Sapienza"
Tesi: Android Client and Soa Server Mobile App for Car Pooling
Relatore: Prof. Andrea Sterbini

ESPERIENZE ACCADEMICHE

Gennaio 2019 – Giugno 2020

Ricercatore in visita

Aarhus University (DK)
Ospitato da Ivan Damgård, ho lavorato con l'Aarhus Crypto Group su progetti di ricerca in Multi-Party Computation

2018 **Tutor di insegnamento**

Dipartimento di Informatica, Università di Roma "La Sapienza"
Corsi: Architetture degli elaboratori, Metodologie di programmazione (Java)

PEER REVIEW

2022 International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), ESORICS 2022, International Conference on Applied Cryptopraphy and Network Security (ACNS)

2021 IEEE Transaction on Information Forensics and Security (TIFS)

2020 Advances in Cryptology (CRYPTO)

2019 Advances in Cryptology (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)

PROGETTI

2021–Adesso **SPECTRA (Sapienza Università di Roma) [4, 3, 2]**

2020–2021 **PRIViLEDGE Project HORIZON 2020 (EU) [6, 8, 5, 7, 9]**

2020–2021 **Toolkit for Secure Multi-Party Computation on Ledgers (PRIViLEDGE Project HORIZON 2020) [5]**

Sviluppo di una libraria che consente l'interazione degli utenti all'interno di un protocollo Multi-Party attraverso la blockchain di Ethereum in modo efficiente.

SEMINARI TENUTI

2022 **Multi-Key and Multi-Input Predicate Encryption from Learning With Errors [4]**

Presentato al Crypto Summer Day organizzato ad Aarhus University (DK)

2021 **Shielded Computations in Smart Contracts Overcoming Forks [10]**

Presentato alla Financial Cryptography and Data Security 2021 Conference (Virtuale) e al Crypto Summer Day organizzato ad Aarhus University (DK)

Terrorist Attacks for Fake Exposure Notifications in Contact Tracing [9]

Presentato alla 19th International Conference on Applied Cryptography and Network Security 2021 (Virtuale)

2019 **On Financial Fairness [2]**

Talk settimanale nel dipartimento di Informatica alla Aarhus University (DK), Invited talk al dipartimento di Informatica all'Università di Roma La Sapienza (Seminari De Cifris Schola Latina)

A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement [11]

Talk settimanale nel dipartimento di Informatica alla Aarhus University (DK). Presentato alla Theory of Cryptography Conference in Norimberga (Dec 2019)

The Rush Dilemma: Attacking and Repairing Smart Contracts on Forking Blockchains [10]

Invited talk alla Chalmers University (SWE), Lund University (SWE) e Seminario COBRA al dipartimento di Informatica della Aarhus Unviersity (DK)

TECHNICAL REPORTS E PUBBLICAZIONI

[1] **Daniele Friolo**. «New Perspectives in Multi-Party Computation: Low Round Complexity from New Assumptions, Financial Fairness and Public Verifiability.» Tesi di dott. Rome, 2021. URL: https://iris.uniroma1.it/retrieve/handle/11573/1566920/1893360/Tesi_dottorato_Friolo.pdf.

[2] **Daniele Friolo**, Fabio Massacci, Chan Nam Ngo e Daniele Venturi. «Cryptographic and Financial Fairness». In: *IEEE Transaction on Information Forensics and Security (to appear)* (2022).

[3] Gennaro Avitabile, Vincenzo Botta, **Daniele Friolo** e Ivan Visconti. «Efficient Proofs of Knowledge for Threshold Relations». In: *ESORICS Conference 2022 (to appear)* (2022).

[4] Danilo Francati, **Daniele Friolo**, Giulio Malavolta e Daniele Venturi. «Multi-key and Multi-input Predicate Encryption from Learning with Errors». In: *Cryptology ePrint Archive* (2022).

[5] Ahto Truu GT, Maria Iliadi, Foteinos Mergoupis-Anagnou, Sven Heiberg, Berry Schoenmakers TUE, Markulf Kohlweiss, **Daniele Friolo**, Ivan Visconti e Panos Louridas. «Report on Tools for Privacy-Preserving Applications on Ledgers». In: (2021).

[6] Michele Ciampi, Aikaterini-Panagiota Stouka, Thomas Zacharias, **Daniele Friolo**, Vincenzo Iovino, Ivan Visconti, Aggelos Kiayias, Volkhov Misha, Markulf Kohlweiss, Toon Segers TUE et al. «Revision of Extended Core Protocols». In: (2021).

[7] Ahto Truu GT, Markulf Kohlweiss, Toon Segers TUE, Ivan Visconti, Sven Heiberg, Panos Louridas, Nikos Voutsinas, Nikos Karagiannidis e **Daniele Friolo**. «Second Scientific & Research Impact Measurement». In: (2021).

[8] Michele Ciampi, Markulf Kohlweiss, Mikhail Volkhov, **Daniele Friolo**, Ivan Visconti, Berry Schoenmakers, Toon Segers TUE, Janno Siim UT e Sven Heiberg. «Revision of Privacy-Enhancing Cryptographic Primitives for Ledgers». In: (2021).

[9] Gennaro Avitabile, **Daniele Friolo** e Ivan Visconti. «Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems». In: *Applied Cryptography and Network Security - 19th International Conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021, Proceedings, Part I*. A cura di Kazue Sako e Nils Ole Tippenhauer. Vol. 12726. Lecture Notes in Computer Science. Springer, 2021, pp. 220–247. URL: https://doi.org/10.1007/978-3-030-78372-3%5C_9.

[10] Vincenzo Botta, **Daniele Friolo**, Daniele Venturi e Ivan Visconti. «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*. A cura di Nikita Borisov e Claudia Dıaz. Vol. 12674. Lecture Notes in Computer Science. Springer, 2021, pp. 73–92. URL: https://doi.org/10.1007/978-3-662-64322-8%5C_4.

[11] **Daniele Friolo**, Daniel Masny e Daniele Venturi. «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*. A cura di Dennis Hofheinz e Alon Rosen. Vol. 11891. Lecture Notes in Computer Science. Springer, 2019, pp. 111–130. URL: https://doi.org/10.1007/978-3-030-36030-6%5C_5.

[12] **Daniele Friolo**, Fabio Massacci, Chan Nam Ngo e Daniele Venturi. «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*. A cura di Jonathan Anderson, Frank Stajano, Bruce Christianson e Vashek Matyás. Vol. 12287. Lecture Notes in Computer Science. Springer, 2019, pp. 135–147. URL: https://doi.org/10.1007/978-3-030-57043-9%5C_13.

[13] Chan Nam Ngo, **Daniele Friolo**, Fabio Massacci, Daniele Venturi e Ettore Battaiola. «Vision: What If They All Die? Crypto Requirements For Key People». In: *IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2020, Genoa, Italy, September 7-11, 2020*. IEEE, 2020, pp. 178–183. URL: https://doi.org/10.1109/EuroSPW51379.2020.00032.