Daniele Venturi

Curriculum Vitae

RESEARCH INTERESTS

My main area of interest is theoretical and applied *cryptography*. Current topics include: cryptographic currencies and distributed ledgers technologies, public-key cryptography, non-malleability, leakage and tamper resilience, cloud security, zero knowledge, multiparty computation.

CURRENT POSITION

Apr 22–now **Full Professor**, Department of Computer Science, Sapienza University of Rome, Italy.

PREVIOUS APPOINTMENTS

Dec 19–March 22 **Associate Professor**, Department of Computer Science, Sapienza University of Rome, Italy.

Dec 16–Nov 19 **Assistant Professor**, *Tenure Track (Italian Law n. 240/2010, art. 24, comma 5, letter b)*, Department of Computer Science, Sapienza University of Rome, Italy.

Apr 16–Nov 16 **Assistant Professor**, *Tenure Track (Italian Law n. 240/2010, art. 24, comma 5, letter b)*, Department of Information Engineering and Computer Science, University of Trento, Italy.

Sep 13–Apr 16 **Postdoc**, *Department of Computer Science*, Sapienza University of Rome, Italy.

Promoters Prof. Giuseppe Ateniese.

Feb 12–Sep 13 **Postdoc**, *Department of Computer Science*, Aarhus University, Denmark.

Promoters Prof. Ivan Damgård and Prof. Jesper Buus Nielsen.

Oct 09–Sep 10 **Visiting Researcher**, *Centrum Wiskunde & Informatica (CWI)*, Amsterdam, The Netherlands.

Promoters Prof. Krzysztof Pietrzak and Prof. Eike Kiltz

EDUCATION

Nov 08–Apr 12 **PhD in Information and Communication Engineering**, *Department of Engineering, Electronics and Telecommunications (DIET)*, Sapienza University of Rome, Italy.

Advisor Prof. Andrea Baiocchi.

Sep 05–Dec 07 **M. Sc. Communication Engineering**, *Sapienza University of Rome*, Italy.

Final grade Full marks (110/110) and *summa cum laude*.

CGPA $30/30$.

Advisor Prof. Andrea Baiocchi and Dott. Alfredo Todini.

Sep 02–Sep 05 **B. Sc. Electrical Engineering**, *University of Rome ROMA TRE*, Italy.

Final grade Full marks (110/110) and *summa cum laude*.

GPA $28.4/30$.

Advisor Prof. Franco Gori.

Sep 97–Jul 02 **High school**, *Scientific Lyceum "Stanislao Cannizzaro"*, Rome, Italy.

Final grade Full marks (100/100).

PUBLICATIONS

Conference Proceedings

[C62] **Non-malleable Fuzzy Extractors** (with Danilo Francati), Proceedings of the 22nd International Conference on Applied Cryptography and Network Security (ACNS 2024), 135-155, Lecture Notes in Computer Science 14583, ISBN 978-3-031-33490-0.

[C61] **On the Complete Non-malleability of the Fujisaki-Okamoto Transform** (with Daniele Friolo and Matteo Salvino), Proceedings of the 21st International Conference on Applied Cryptography and Network Security (ACNS 2023), 307-335, Lecture Notes in Computer Science 13906, ISBN 978-3-031-33490-0.

[C60] **Continuously Non-malleable Codes Against Bounded-Depth Tampering** (with Danilo Francati, Daniele Friolo, Monosij Maitra, Giulio Malavolta and Ahmadreza Rahimi), Proceedings of the 29th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2023), 98-133, Lecture Notes in Computer Science 14442, ISBN 978-981-99-8732-0.

[C59] **MARTSIA: Enabling Data Confidentiality for Blockchain-Based Process Execution** (with Edoardo Marangone, Claudio Di Ciccio, Daniele Friolo, Eugenio Nerio Nemmi and Ingo Weber), Proceedings of the 27th International Conference on Enterprise Design, Operations, and Computing (EDOC 2023), 58-76, Lecture Notes in Computer Science 14367, ISBN 978-3-031-46586-4.

[C58] **Multi-key and Multi-input Predicate Encryption from Learning with Errors** (with Danilo Francati, Daniele Friolo and Giulio Malavolta), Proceedings of the 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2023), 573-604, Lecture Notes in Computer Science 14006, ISBN 978-3-031-30619-8.

[C57] **Continuously Non-malleable Codes Against Bounded-Depth Tampering** (with Gianluca Brian, Sebastian Faust and Elena Micheli), Proceedings of the 28th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2022), 384-413, Lecture Notes in Computer Science 13794, ISBN 978-3-031-22971-8.

[C56] **From Privacy-Only to Simulatable OT: Black-Box, Round-Optimal, Information-Theoretic** (with Varun Madathil, Chris Orsini and Alessandra Scafuro), Proceedings of the 3rd Conference on Information-Theoretic Cryptography (ITC 2022), 272-302, Lecture Notes in Computer Science 13275.

[C55] **Universally Composable Subversion-Resilient Cryptography** (with Suvradip Chakraborty, Bernardo Magri and Jesper Buus Nielsen), Proceedings of the 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2022), 5-20, Lecture Notes in Computer Science 13275, ISBN 978-3-031-06943-7.

[C54] **Identity-Based Matchmaking Encryption Without Random Oracles** (with Danilo Francati, Alessio Guidi, and Luigi Russo), Proceedings of the 22nd International Conference on Cryptology in India (INDOCRYPT 2021), 333-364, Lecture Notes in Computer Science 13143, ISBN 978-3-030-92518-5.

[C53] **Continuously Non-malleable Secret Sharing: Joint Tampering, Plain Model and Capacity** (with Gianluca Brian and Antonio Faonio), Proceedings of the 19th International Theory of Cryptography Conference (TCC 2021), 415-435, Lecture Notes in Computer Science 13043, ISBN 978-3-030-90452-4.

[C52] **Shielded Computations in Smart Contracts Overcoming Forks** (with Vincenzo Botta, Daniele Friolo, and Ivan Visconti), Proceedings of the 25th International Conference on Financial Cryptography and Data Security (FC 2021), 73-92, Lecture Notes in Computer Science 12674, ISBN 978-3-662-64321-1.

[C51] **The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free** (with Gianluca Brian, Antonio Faonio, Maciej Obremski, Joao L. Ribeiro, Mark Simkin and Maciej Skórski), Proceedings of the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2021), 408-437, Lecture Notes in Computer Science 12697, ISBN 978-3-030-77885-9.

[C50] **On Adaptive Security of Delayed-Input Sigma Protocols and Fiat-Shamir NIZKs** (with Michele Ciampi and Roberto Parisella), Proceedings of the 12th International Conference on Security and Cryptography for Networks (SCN 2020), 670-690, Lecture Notes in Computer Science 12238, ISBN 978-3-030-57989-0.

[C49] **Vision: What If They All Die? Crypto Requirements For Key People** (with Chan Nam Ngo, Daniele Friolo, Fabio Massacci and Ettore Battaiola), Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&P Workshops 2020), 178-183, ISBN 978-1-7281-8597-2.

[C48] **Non-malleable Secret Sharing Against Bounded Joint-Tampering Attacks in the Plain Model** (with Gianluca Brian, Antonio Faonio, Maciej Obremski and Mark Simkin), Proceedings of the 40th Annual International Cryptology Conference (CRYPTO 2020), 127-155, Lecture Notes in Computer Science 12172, ISBN 978-3-030-56876-4.

[C47] **Cryptographic Reverse Firewalls for Interactive Proof Systems** (with Chaya Ganesh and Bernardo Magri), Proceedings of the 47th International Colloquium on Automata, Languages and Programming (ICALP 2020), 55:1-55:16, LIPIcs 168, ISBN 978-3-95977-138-2.

[C46] **A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement** (with Daniele Friolo and Daniel Masny), Proceedings of the 17th Theory of Cryptography Conference (TCC 2019), 111-130, Lecture Notes in Computer Science 11891, ISBN 978-3-030-36029-0.

[C45] **Continuously Non-malleable Secret Sharing for General Access Structures** (with Gianluca Brian and Antonio Faonio), Proceedings of the 17th Theory of Cryptography Conference (TCC 2019), 211-232, Lecture Notes in Computer Science 11892, ISBN 978-3-030-36032-0.

[C44] **Non-Malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate** (with Antonio Faonio), Proceedings of the 39th Annual International Cryptology Conference (CRYPTO 2019), 448-479, Lecture Notes in Computer Science 11693, ISBN 978-3-030-26950-0.

[C43] **Match Me if You Can: Matchmaking Encryption and its Applications** (with Giuseppe Ateniese, Danilo Francati, and David Nunez), Proceedings of the 39th Annual International Cryptology Conference (CRYPTO 2019), 701-731, Lecture Notes in Computer Science 11693, ISBN 978-3-030-26950-0.

[C42] **Rate-Optimizing Compilers for Continuously Non-Malleable Codes** (with Sandro Coretti, and Antonio Faonio), Proceedings of the 17th International Conference on Applied Cryptography and Network Security (ACNS 2019), 3-23, Lecture Notes in Computer Science 11464, ISBN 978-3-030-21567-5.

[C41] **Public Immunization against Complete Subversion without Random Oracles** (with Giuseppe Ateniese, Danilo Francati, and Bernardo Magri), Proceedings of the 17th International Conference on Applied Cryptography and Network Security (ACNS 2019), 465-485, Lecture Notes in Computer Science 11464, ISBN 978-3-030-21567-5.

[C40] **Multi-Covert Channel Attack in the Cloud** (with Giuseppe Ateniese, Danilo Francati, and Bernardo Magri), Proceedings of the 6th International Conference on Software Defined Systems (SDS 2019), 160-165, ISBN 978-1-7281-0722-6.

[C39] **Affordable Security or Big Guy vs Small Guy: Does the depth of your pockets impact your protocols?** (with Daniele Friolo, Fabio Massacci, and Chan Nam Ngo), to appear at the Security Protocols Workshop (SPW) 2019.

[C38] **Secure Outsourcing of Circuit Manufacturing** (with Giuseppe Ateniese, Aggelos Kiayias, Bernardo Magri, and Yiannis Tselekounis), Proceedings of 12th International Conference on Provable Security (ProvSec 2018), 75-93, Lecture Notes in Computer Science 11192, ISBN 978-3-030-01445-2.

[C37] **Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions** (with Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti), Proceedings of the 38th Annual International Cryptology Conference (CRYPTO 2018), 608-639, Lecture Notes in Computer Science 10993, ISBN 978-3-319-96877-3.

[C36] **Continuously Non-Malleable Codes with Split-State Refresh** (with Antonio Faonio, Jesper Buus Nielsen, and Mark Simkin), Proceedings of the 16th International Conference on Applied Cryptography and Network Security (ACNS 2018), 121-139, Lecture Notes in Computer Science 10892, ISBN 978-3-319-93386-3.

[C35] **Non-Monotonic Security Protocols and Failures in Financial Intermediation** (with Fabio Massacci, Cham Nam Ngo, and Julian Williams), Proceedings of the Security Protocols Workshop (SPW) 2018, 45-54, Lecture Notes in Computer Science 11286, ISBN 978-3-030-03250-0.

[C34] **FuturesMEX: Secure Distributed Futures Market Exchange** (with Fabio Massacci, Cham Nam Ngo, Jing Nie, and Julian Williams), Proceedings of IEEE S&P 2018, 453-471, ISBN 978-1-5386-4353-2.

[C33] **Non-Malleable Codes for Space-Bounded Tampering** (with Sebastian Faust, Kristina Hostáková and Pratyay Mukherjee), Proceedings of the 37th Annual International Cryptology Conference (CRYPTO 2017), 95-126, Lecture Notes in Computer Science 10402, ISBN 978-3-319-63714-3.

[C32] **Redactable Blockchain - or - Rewriting History in Bitcoin and Friends** (with Ewerton R. Andrade Nielsen, Giuseppe Ateniese and Bernardo Magri), Proceedings of the 2nd IEEE European Symposium on Security and Privacy (Euro S&P 2017), 111-126, IEEE, ISBN 978-1-5090-5762-7.

[C31] **Predictable Arguments of Knowledge** (with Antonio Faonio and Jesper Buus Nielsen), Proceedings of the 20th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2017), 121-150, Lecture Notes in Computer Science 10174, ISBN 978-3-662-54364-1.

[C30] **The Seconomics (Security-Economics): Vulnerabilities of Decentralized Autonomous Organizations** (with Fabio Massacci, Chan Nam Ngo, Jing Nie and Julian Williams), Proceedings of the 25th International Workshop on Security Protocols, 171-179, Lecture Notes in Computer Science 10476, ISBN 978-3-319-71074-7.

[C29] **Securing Underwater Communications: Key Agreement based on Fully Hashed MQV** (with Angelo Capossele, Chiara Petrioli, Gabriele Saturni and Daniele Spaccini), Proceedings of the International Conference on Underwater Networks & Systems (WUWNet 2017), 12:1-12:5, ACM, ISBN 978-1-4503-5561-2.

[C28] **Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience** (with Antonio Faonio), Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016), 877-907, Lecture Notes in Computer Science 10031, ISBN 978-3-662-53886-9.

[C27] **Naor-Yung Paradigm with Shared Randomness and Applications** (with Silvio Biagioni and Daniel Masny), Proceedings of the 10th International Conference on Security and Cryptography for Networks (SCN 2016), 62-80, Lecture Notes in Computer Science 9841, ISBN 978-3-319-44617-2.

[C26] **Fiat-Shamir for Highly Sound Protocols Is Instantiable** (with Arno Mittlebach), Proceedings of the 10th International Conference on Security and Cryptography for Networks (SCN 2016), 198-215, Lecture Notes in Computer Science 9841, ISBN 978-3-319-44617-2.

[C25] **Chosen-Ciphertext Security from Subset Sum** (with Sebastian Faust and Daniel Masny), Proceedings of the 19th International Conference on on Practice and Theory in Public-Key Cryptography (PKC 2016), 35-46, ISBN 978-3-662-49383-0.

[C24] **Non-Malleable Encryption: Simpler, Shorter, Stronger** (with Sandro Coretti, Yevgeniy Dodis, and Björn Tackmann), Proceedings of the 13th Theory of Cryptography Conference (TCC 2016-A), 306-335, ISBN 978-3-662-49095-2.

[C23] **Secure Data Sharing and Processing in Heterogeneous Clouds** (with Bojan Suzic, Andreas Reiter, Florian Reimair and Baldur Kubo), Proceedings of the 1st International Conference on Cloud Forward: From Distributed to Complete Computing (Cloud Forward 2015), 116-126, Elsevier, DOI: 10.1016/J.PROCS.2015.09.228.

[C22] **(De)-Constructing TLS 1.3** (with Markulf Kohlweiss, Ueli Maurer, Cristina Onete and Björn Tackmann), Proceedings of the 16th International Conference on Cryptology in India (INDOCRYPT 2015), 85-102, ISBN 978-3-319-26616-9.

[C21] **Subversion-Resilient Signature Schemes** (with Giuseppe Ateniese and Bernardo Magri), Proceedings of the 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015), 364-375, ISBN 978-1-4503-3832-5.

[C20] **Entangled Encodings and Data Entanglement** (with Giuseppe Ateniese, Özgür Dagdelen, and Ivan Damgård), Proceedings of the 3rd International Workshop on Security in Cloud Computing (SCC@ASIACCS 2015), 3-12, ISBN 978-1-4503-3447-1.

[C19] **Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation** (with Antonio Faonio and Jesper Buus Nielsen), Proceedings of the 42nd International Colloquium on Automata, Languages and Programming (ICALP 2015), 456-468, Lecture Notes in Computer Science 9134, ISBN 978-3-662-47671-0.

[C18] **The Chaining Lemma and Its Application** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), Proceedings of the 8th International Conference on Information Theoretic Security (ICITS 2015), 181-196, Lecture Notes in Computer Science 9063, ISBN 978-3-319-17469-3.

[C17] **A Tamper and Leakage Resilient von Neumann Architecture** (with Sebastian Faust, Pratyay Mukherjee, and Jesper Buus Nielsen), Proceedings of the 18th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2015), 579-603, Lecture Notes in Computer Science 9020, ISBN 978-3-662-46446-5.

[C16] **From Single-Bit to Multi-Bit Public-Key Encryption via Non-Malleable Codes** (with Sandro Coretti, Ueli Maurer, and Björn Tackmann), Proceedings of the 12th Theory of Cryptography Conference (TCC 2015), 532-560, Lecture Notes in Computer Science 9014, ISBN 978-3-662-46493-9.

[C15] **A Multi-Party Protocol for Privacy-Preserving Cooperative Linear Systems of Equations** (with Özgür Dagdelen), Proceedings of the 1st International Conference in Cryptography and Information Security in the Balkans (BalkancryptSec 2014), 161-172, Lecture Notes in Computer Science 9024, ISBN 978-3-319-21355-2.

[C14] **A Second Look at Fischlin's Transformation** (with Özgür Dagdelen), Proceedings of the 7th International Conference on Cryptology (AFRICACRYPT 2014), 356-376, Lecture Notes in Computer Science 8469, ISBN 978-3-319-06733-9.

[C13] **Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits** (with Sebastian Faust, Pratyay Mukherjee, and Daniel Wichs). Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2014), 111-128, Lecture Notes in Computer Science 8441, ISBN 978-3-642-55219-9.

[C12] **Leakage-Resilient Signatures with Graceful Degradation** (with Jesper Buus Nielsen and Angela Zottarel), Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2014), 362-379, Lecture Notes in Computer Science 8383, ISBN 978-3-642-54630-3.

[C11] **Continuous Non-Malleable Codes** (with Sebastian Faust, Pratyay Mukherjee, and Jesper Buus Nielsen), Proceedings of the 11th Theory of Cryptography Conference (TCC 2014), 465-488, Lecture Notes in Computer Science 8349, ISBN 978-3-642-54241-1.

[C10] **Bounded Tamper Resilience: How to go beyond the Algebraic Barrier** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2013), 140-160, Lecture Notes in Computer Science 8270, ISBN 978-3-642-42044-3.

[C09] **Outsourced Pattern Matching** (with Sebastian Faust and Carmit Hazay), Proceedings of the 40th International Colloquium on Automata, Languages, and Programming (ICALP 2013), 545-556, Lecture Notes in Computer Science 7966, ISBN 978-3-642-39211-5.

[C08] **Anonymity-Preserving Public Key Encryption: A Constructive Approach** (with Markulf Kohlweiss, Ueli Maurer, Cristina Onete and Björn Tackmann), Proceedings of the 13th International Symposium on Privacy Enhancing Technologies (PETS 2013), 19-39, Lecture Notes in Computer Science 7981, ISBN 978-3-642-39076-0.

[C07] **On the Connection between Leakage Tolerance and Adaptive Security** (with Jesper Buus Nielsen and Angela Zottarel), Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013), 497-515, Lecture Notes in Computer Science 7778, ISBN 978-3-642-36361-0.

[C06] **Rate-Limited Secure Function Evaluation** (with with Özgür Dagdelen and Payman Mohassel), Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013), 461-478, Lecture Notes in Computer Science 7778, ISBN 978-3-642-36361-0.

[C05] **On the Non-malleability of the Fiat-Shamir Transform** (with Sebastian Faust, Markulf Kohweiss and Giorgia Azzurra Marson), Proceedings of the 13th International Conference on Cryptology in India (INDOCRYPT 2012), 60-79, Lecture Notes in Computer Science 7668, ISBN 978-3-642-34930-0.

[C04] **Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience** (with Sebastian Faust and Krzysztof Pietrzak), Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP 2011), 391-402, Lecture Notes in Computer Science 6755, ISBN 978-3-642-22005-0.

[C03] **Efficient Authentication from Hard Learning Problems** (with Eike Kiltz, Krzysztof Pietrzak, David Cash and Abishek Jain), Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011), 7-26, Lecture Notes in Computer Science 6632, ISBN 978-3-642-20464-7.

[C02] **Leakage-Resilient Storage** (with Francesco Davì and Stefan Dziembowski), Proceedings of the 7th International Conference on Security and Cryptography for Networks (SCN 2010), 121-137, Lecture Notes in Computer Science 6280, ISBN 978-3-642-15316-7.

[C01] **Inadequacy of the Queue-Based Max-Weight Optimal Scheduler on Wireless Links with TCP Sources** (with Alfredo Todini and Andrea Baiocchi), Proceedings of IEEE International Conference on Communications (ICC 2009), 1-6.

Journals

[J21] **Multi-key and Multi-input Predicate Encryption (for Conjunctions) from Learning with Errors** (with Danilo Francati, Daniele Friolo and Giulio Malavolta), full version of [C57], Journal of Cryptology 37(3), 2024. DOI: 10.1007/S00145-024-09504-7.

[J20] **Cryptographic and Financial Fairness** (with Daniele Friolo, Fabio Massacci and Chan Nam Ngo), IEEE Transaction on Information Forensics and Security, 17(2022), 3391-3406, 2022. DOI: 10.1109/TIFS.2022.3198852.

[J19] **The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free** (with Gianluca Brian, Antonio Faonio, Maciej Obremski, Joao Ribeiro, Mark Simkin and Maciej Skorski), full version of [C50], IEEE Transaction on Information Theory, 68(12), 8197-8227, 2022. DOI: 10.1109/TIT.2022.3193848.

[J18] **Short Non-Malleable Codes from Related-Key Secure Block Ciphers, Revisited** (with Gianluca Brian, Antonio Faonio and Joao Ribeiro), IEEE Transaction on Symmetric Cryptology, 2022(3), 1-19, 2022. DOI: 10.46586/TOSC.V2022.I3.1-19.

[J17] **A Compiler for Multi-Key Homomorphic Signatures for Turing Machines** (with Somayeh Dolatnezhad Samarin, Dario Fiore and Morteza Amini), Theoretical Computer Science 889. DOI: 10.1016/j.tcs.2021.08.002.

[J16] **Match Me if You Can: Matchmaking Encryption and Its Applications** (with Giuseppe Ateniese, Danilo Francati, and David Nunez), full version of [C42], Journal of Cryptology 34(3), 2021. DOI: 10.1007/s00145-021-09381-4.

[J15] **Cryptographic Reverse Firewalls for Interactive Proof Systems** (with Chaya Ganesh and Bernardo Magri), full version of [C46], Theoretical Computer Science 855., 104-132, 2021. DOI: 10.1016/j.tcs.2020.11.043.

[J14] **Immunization against Complete Subversion without Random Oracles** (with Giuseppe Ateniese, Danilo Francati and Bernardo Magri), full version of [C40], Theoretical Computer Science 859, 1-36, 2021. DOI: 10.1016/j.tcs.2021.01.002.

[J13] **Non-malleable Encryption: Simpler, Shorter, Stronger** (with Sandro Coretti, Yevgeniy Dodis, Björn Tackmann), full version of [C16] and [C23], Journal of Cryptology 33(4), 2020. DOI: 10.1007/s00145-020-09361-0.

[J12] **Continuously Non-Malleable Codes in the Split-State Model** (with Sebastian Faust, Pratyay Mukherjee and Jesper Buus Nielsen), full version of [C11], Journal of Cryptology 33(4), 2020. DOI: 10.1007/s00145-020-09362-z.

[J11] **Subversion-Resilient Signatures: Definitions, Constructions and Applications** (with Giuseppe Ateniese and Bernardo Magri), full version of [C21], Theoretical Computer Science 820, 91-122, 2020. DOI: 10.1016/j.tcs.2020.03.021.

[J10] **Continuously Non-Malleable Codes with Split-State Refresh** (with Antonio Faonio, Jesper Buus Nielsen, and Mark Simkin), full version of [C35], Theoretical Computer Science 759, 98-132, 2019. DOI: 10.1016/j.tcs.2018.05.001.

[J09] **Fiat-Shamir for Highly Sound Protocols is Instantiable** (with Arno Mittelbach), full version of [C25], Theoretical Computer Science 740, 28-72, 2018. DOI: 10.1016/j.tcs.2018.05.001.

[J08] **Outsourced Pattern Matching** (with Sebastian Faust and Carmit Hazay), full version of [C09], International Journal of Information Security, 17(3), 327-346, 2018. DOI: 10.1007/s10207-017-0374-0.

[J07] **Efficient Authentication from Hard Learning Problems** (with Eike Kiltz, Krzysztof Pietrzak, David Cash and Abishek Jain), full version of [C03], Journal of Cryptology, 30(4), 2017. DOI: 10.1007/s00145-016-9247-3.

[J06] **Bounded Tamper Resilience: How to go beyond the Algebraic Barrier** (with Ivan Damgård, Sebastian Faust and Pratyay Mukherjee), full version of [C10], Journal of Cryptology, 30(1), 2017. DOI: 10.1007/s00145-015-9218-0.

[J05] **Fully Leakage-Resilient Signatures Revisited: Graceful Degradation, Noisy Leakage, and Construction in the Bounded-Retrieval Model** (with Antonio Faonio and Jesper Buus Nielsen), full version of [C19], Theoretical Computer Science 660, 23-56, 2017. DOI: 10.1016/j.tcs.2016.11.016.

[J04] **Naor-Yung Paradigm with Shared Randomness and Applications** (with Silvio Biagioni and Daniel Masny), full version of [C26], Theoretical Computer Science 692, 90-113, 2017. DOI: 10.1016/j.tcs.2017.06.019.

[J03] **Entangled Cloud Storage** (with with Giuseppe Ateniese, Özgür Dagdelen, and Ivan Damgård), full version of [C20], Future Generation Computer Systems (Special Issue on Cloud Cryptography), 62, 104-118, 2016. DOI: 10.1016/j.future.2016.01.008.

[J02] **Rate-Limited Secure Function Evaluation: Definitions and Constructions** (with with Özgür Dagdelen and Payman Mohassel), full version of [C06], Theoretical Computer Science 653, 53-78, 2016. DOI: 10.1016/j.tcs.2016.09.020.

[J01] **Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits** (with Sebastian Faust, Pratyay Mukherjee, and Daniel Wichs), full version of [C13], IEEE Transaction on Information Theory, 62(12), 7179-7194, 2016. DOI: 10.1109/TIT.2016.2613919.

Books & Surveys

[B04] **Proceedings of the 20th International Conference on Applied Cryptography and Network Security (ACNS 2022** (with Giuseppe Ateniese), Rome, Italy, June 20-23, 2022, Lecture Notes in Computer Science 13269, Springer 2022, ISBN 978-3-031-09233-6.

[B03] **Tampering in Wonderland**, Sapienza Università Editrice, 2013.

[B02] **Crittografia nel Paese delle Meraviglie**, Collana UNITEXT, Springer 2012, ISBN 978-88-470-2480-9.

[B01] **Lecture Notes on Algorithmic Number Theory**, Technical Report ECCC—TR09-06, Electronic Colloquium on Computational Complexity, 28 July 2009.

BIBLIOMETRICS

H-Index **28**, *Google Scholar*, July 2024.

Citations **2978**, *Google Scholar*, July 2024.

GRANTS

2023–2025 **Smart Decentralized Finance (SmartDeFi)**, *Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU*, Principal Investigator.

2021–2023 **Secure and Privacy-Preserving Contact Tracing**, *Progetto di Ateneo, Sapienza University of Rome, Italy*, Principal Investigator.

2019–2021 **SmartDefense: Models, Algorithms and Mechanisms for Reducing Cyber Risks in Smart Industry**, *Progetto di Ateneo, Sapienza University of Rome, Italy*, Co-applicant and Researcher.

2017–2019 **Protect Yourself and Your Data when using Social Networks**, *Progetto di Ateneo, Sapienza University of Rome, Italy*, Co-applicant and Researcher.

2014–2018 **Cryptography for Secure Digital Interaction**, *ICT COST Action IC1306*, Official Substitute Management Committee member.

2015–2018 **Secure Information Sharing in Federated Heterogeneous Private Clouds (SUNFISH)**, *European Union's Horizon 2020 research and innovation programme under grant agreement No 644666*, Work Package Leader.

2014–2017 **Geopolitics-Aware Internet Strategies (GAINS)**, *European Commission (Directorate-General Home Affairs) project HOME/2013/CIPS/AG/4000005057*, Co-applicant and Researcher.

COMMISSIONS OF TRUST

Responsibilities **Head of the Master's Degree Program in Cybersecurity**, Sapienza University of Rome, Italy.

Head of the Scientific Committee, Cybersecurity Competence Center, Cyber 4.0.

Editorial Activities **Editorial Board Member**, IEEE Transactions on Information Forensics and Security.

Program Co-Chair (with Giuseppe Ateniese), 20th International Conference on Applied Cryptography and Network Security (ACNS 2022).

Reviewing

Program Committee Member, EUROCRYPT 2025 (42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques), PKC 2025 (28th International Conference on Practice and Theory in Public-Key Cryptography), CRYPTO 2024 (43rd International Cryptology Conference. University of California), PKC 2024 (27th International Conference on Practice and Theory in Public-Key Cryptography), CANS 2023 (22nd International Conference on Cryptology and Network Security), ESORICS 2023 (28th European Symposium on Research in Computer Security), ACNS 2023 (21st International Conference on Applied Cryptography and Network Security), ITASEC 2022 (2022 Italian Conference on Cybersecurity), EUROCRYPT 2022 (40th Annual International Conference on the Theory and Applications of Cryptographic Techniques), CANS 2021 (20th International Conference on Cryptology and Network Security), CRYPTO 2021 (41st International Cryptology Conference), EUROCRYPT 2021 (40th Annual International Conference on the Theory and Applications of Cryptographic Techniques), SCN 2020 (12th Conference on Security and Cryptography for Networks), CSCML 2020 (4th International Symposium on Cyber Security Cryptology and Machine Learning) ACNS 2020 (18th International Conference on Applied Cryptography and Network Security), PKC 2020 (23rd International Conference on the Theory and Practice of Public-Key Cryptography), CRYPTO 2019 (39th International Cryptology Conference), SCN 2018 (12th International Conference on Security and Cryptography for Networks), PKC 2017 (20th International Conference on the Theory and Practice of Public-Key Cryptography), PKC 2016 (19th International Conference on the Theory and Practice of Public-Key Cryptography), EUROCRYPT 2016 (35th Annual International Conference on the Theory and Applications of Cryptographic Techniques).

External Reviewer, for the most prestigious conferences and journals in cryptography and computer security, among which ACM CCS, IEEE S&P, ACM STOC, IEEE FOCS, CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, Journal of Cryptology, Design Codes and Cryptography, IEEE Transactions on Information Theory, and for EU projects (H2020).

TEACHING (SELECTION)

2023-now *Lecturer* for the class “Automi, Calcolabilità e Complessità”, Bachelor’s Degree in Computer Science, Sapienza University of Rome

2018-2022 *Lecturer* for the class “Secure Computation”, Master’s Degree in Cybersecurity, Sapienza University of Rome

2017-now *Lecturer* for the class “Data Privacy and Security”, Master’s Degree in Data Science, Sapienza University of Rome

2016-now *Lecturer* for the class “Cryptography”, Master’s Degree in Computer Science, Master’s Degree in Cybersecurity, and Master’s Degree in Mathematics, Sapienza University of Rome

MENTORING AND SUPERVISION OF STUDENTS (SELECTION)

PhD Advisor

Andrea Reale, Department of Computer Science, Sapienza University of Rome, Italy. .
2023-2026

Lorenzo Magliocco, Department of Computer Science, Sapienza University of Rome, Italy..
2022-2025

Gianluca Brian, Department of Computer Science, Sapienza University of Rome, Italy..
2019-2022

Daniele Friolo, Department of Computer Science, Sapienza University of Rome, Italy..
2017-2020

PhD Mentor

Cham Nam Ngo, Department of Information Engineering and Computer Science, University of Trento, Italy. 2016.

Bernardo Magri, Department of Computer Science, Sapienza University of Rome, Italy. 2016.

Antonio Faonio, Department of Computer Science, Sapienza University of Rome, Italy. 2013-2016.

Pratyay Mukherjee, Department of Computer Science, Aarhus University, Denmark. 2012-2013.

MSc Advisor I have supervised over 50 master thesis.

HONORS & AWARDS

2013 **Premio Tesi di Dottorato**, *Sapienza Università editrice*, PhD Thesis [S03] awarded amongst the best six thesis defended at Sapienza University between 2010 and 2012.

2011 **Best paper award at Eurocrypt 2011 for [C03]**, *invited to Journal of Cryptology*.

2008 **Degree Prize**, *2000€ for deserving curriculum studiorum*, Sapienza University of Rome, Engineering Faculty.

SELECTED TALKS

2018 **Continuously Non-Malleable Codes: A Tutorial**, *Keynote talk at University of Montenegro*, April 2018.

Bitcoin and Beyond: A Tutorial, *Keynote talk at the Mini-Workshop on Consistency Problems in Distributed and Concurrent Systems, Sapienza University of Rome*, February 2018.

Non-Malleable Codes and Applications, *Keynote talk at "La De Componendis Cifris incontra Roma", University of ROMA TRE*, October 2018.

2017 **Redactable Blockchain**, *Invited talk at TU Graz*, October 2017.

2016 **Fiat-Shamir for Highly Sound Protocols is Instantiable**, *Plenary talk at the 10th Conference on Security and Cryptography for Networks (SCN 2016)*, September 2016.

2015 **Tamper-Resilient Cryptography**:

-*Invited talk at University of Trento*, December 2015

-*Invited talk at University of Cassino and Southern Lazio*, November 2015

-*Invited talk at Kyushu University*, April 2015

Security of Signature Schemes under Tampering and Subversion Attacks, *Invited talk at Ruhr University of Bochum*, July 2015.

Entangled Cloud Storage, *Plenary talk at the Third International Workshop on Security in Cloud Computing (SCC@ASIACCS)*, April 2015.

2014 **Non-Malleable Codes and Applications**, *Keynote talk at the 2014 RISC/Intercity Number Theory Seminar, CWI Amsterdam*, May 2014.

2013 **New Results on Non-Malleable Codes**, *Invited talk at ETH Zurich*, November 2013.

Outsourced Pattern Matching, *Plenary talk at the 40th International Colloquium on Automata, Languages and Programming (ICALP*, July 2013.

On the Connection between Leakage Tolerance and Adaptive Security:

-*Keynote talk at the Workshop on Leakage, Tampering, and Viruses*, Warsaw, June 2013

-*Plenary talk at the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC)*, Nara, February 2013.

2012 **Cryptography and Security**, *Invited Talk at the 2012 Computer Science Day, Aarhus University*, June 2012.

2011 **Tamper-Proof Circuits: How to Trade Leakage for Tamper Resilience**, *Plenary talk at the 38th International Colloquium on Automata, Languages and Programming (ICALP)*, July 2011.

Efficient Authentication from Hard Learning Problems:

-*Invited talk at TU Darmstadt*, February 2011.

-*Invited talk at Aarhus University*, August 2011.

2010 **Leakage-Resilient Storage**, *Universitè catholique de Louvain*, September 2010.

Tamper-Proof Circuits: How to Trade Leakage for Tamper Resilience, *Invited talk at the Summer School on Applied Cryptographic Protocols, Mykonos*, September 2010.

PATENTS

2021 **A Method and Apparatus for Distributed, Privacy-preserving and Integrity-preserving Exchange, Inventory and Order Book**, *Patent n. 19154744.7*, July 2021.

2018 **Hybrid Blockchain**, *Patent n. 9959065*, May 2018.

2017 **Multiple-Link Blockchain**, *Patent n. 9785369*, October 2017.

Distributed Key Secret for Rewritable Blockchain, *Patent n. 9774578*, September 2017.

INDUSTRY EXPERIENCE

Apr 08–Sep 08 **Trainee**, *Telecom Italia LAB (TILAB)*, Via di Val Cannuta 250, Rome, ITALY.

Description Engineering activities on new generation (NGN2) wired networks (Fiber To The Home (FTTH) and Fiber To The Building (FTTB) architectures).

Jan 08–Apr 08 **Trainee**, *Ericsson Telecomunicazioni s.p.a*, Via Anagnina 203, Rome, ITALY.

Description Development, integration and testing of new Intelligent Network (IN) services on INS platform.

CERTIFICATIONS

Mar 07–Jul 07 **EC-ASP: ELSAGDATAMAT Certification for AMTEC Security Professional**, *Elsag Datamat s.p.a.*, Finmeccanica Group.

Skills Covered Basic routing network configuration, planning and design of security infrastructures, use of a management and deployment configuration system, installation and integration of SVPN infrastructures, troubleshooting activities.

COMPUTER SKILLS

Operating systems	Microsoft Windows 3.11/9X/NT/2000/XP, GNU/Linux and others UNIX-like.
Programming	JAVA, bash, LaTeX.
Scientific software	MATHEMATICA, MATLAB, MathCad, ns2.
Others	Inkscape, GIMP, Office and OpenOffice suite.

LANGUAGES

Italian	Mother tongue.
English	Self-assessment (Common European Framework of Reference for Languages, CEFR).
Reading	C2 (Proficient user).
Listening	C2 (Proficient user).
Speaking	C2 (Proficient user).
Writing	C2 (Proficient user).

SPARE TIME ACTIVITIES

Sports Judo: since the age of nine, black belt $2^{\text{-th}}$ DAN, Kime-no-Kata regional champion (years 2006 and 2007).

Hobbies Music: Electric guitar, Acoustic guitar (finger/flat-picking).

Interests Reading and mathematics.

REFERENCES

These persons are familiar with my professional qualifications and my character:

Ivan Damgård
Department of Computer Science, Aarhus University
Åbogade 24, 8200 Aarhus
e-mail: ivan@cs.au.dk

Giuseppe Persiano
Management of Innovation Systems, University of Salerno
Via Ponte Don Melillo, 84081 Fisciano (SA)
e-mail: giuper@gmail.com

Ueli Maurer
Department of Computer Science, ETH Zurich
CH, 8092 Zurich
e-mail: maurer@inf.ethz.ch

“Treatement of personal informations is authorised according to the local privacy laws (D. Lgs 196/2003)”.

Signature: