Dario Fiore

IMDEA Software Institute	Phone:	(+34) 911012202 (ext. 4160)
Campus Montegancedo s/n,	Mobile:	(+34) 722497624
28223 Pozuelo de Alarcón, Madrid	Email:	`dario.fiore@imdea.org`
SPAIN	Homepage:	`http://www.dariofiore.it`

Current Position

May 2019 — Present	**Associate Research Professor** IMDEA Software Institute, Madrid, Spain

Research Interests

Cryptography and Security

Education and Training

Jan.2007 – Mar.2010	**Ph.D. in Computer Science**, University of Catania, Italy Advisor: Dario Catalano Thesis: “Efficient Cryptographic Constructions from Bilinear Maps” Date of defense: March 1, 2010.
Aug – Dec, 2008	**Visiting student**, New York University, New York, USA Host: Prof. Yevgeniy Dodis.
Sep – Dec, 2008	**Visiting student**, IBM T.J. Watson Research Center, Hawthorne, NY, USA Host: Dr. Rosario Gennaro.
Oct.2004 – Jul.2006	**Master’s in Computer Science**, University of Catania, Italy Thesis: “Timestamping and its application to a technical report archive system” Supervisors: Prof. Domenico Cantone, Dr. Mario Di Raimondo Date of defense: July 27, 2006. Grade: 110/110 cum laude.
Oct.2001 – Oct.2004	**Bacherlor’s in Computer Science**, University of Catania, Italy Thesis: “A tool to visualize shortest path algorithms on grid graphs” Supervisors: Prof. Domenico Cantone, Dr. Simone Faro Date of defense: October 8, 2004. Grade: 110/110.

Professional Experience

Nov.2013 – May 2019	**Assistant Research Professor** (tenure-track) IMDEA Software Institute, Madrid, Spain
Nov.2012 – Oct.2013	**Postdoctoral Researcher**, Max Planck Institute for Software Systems (MPI-SWS) Saarbruecken, Germany. Host: Prof. Michael Backes
Jan.2012 – Oct.2012	**Postdoctoral Researcher**, Courant Institute of Mathematical Sciences New York University, USA. Host: Prof. Yevgeniy Dodis
Apr.2010 – Dec.2011	**Postdoctoral Researcher**, École Normale Supérieure, Paris, France. Hosts: Dr. David Pointcheval, Dr. Michel Abdalla

Awards

ERC Consolidator Grant, 2020.

CNIL-INRIA Award for Privacy Protection, 2016.

Juan de la Cierva 'Incorporacíon', individual fellowship of the Spanish Ministry of Science and Innovation, 2016–2017.

Amarout-II fellowship, Marie-Curie Cofund Action, 2014.

PhD fellowship (3 years) sponsored by the Italian ministry of education, 2007–2009.

Student Travel Awards: PKC 2008, Eurocrypt 2008, Eurocrypt 2009, ACM CCS 2009.

Publications

Journal Papers

1. Somayeh Dolatnezhad Samarin, Dario Fiore, Daniele Venturi, and Morteza Amini
   A compiler for multi-key homomorphic signatures for Turing machines
   Theoretical Computer Science. October 2021.

2. Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, and Elena Pagnin
   Multi-Key Homomorphic Authenticators
   IET Information Security. Published online on April 2019.

3. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, John Mitchell, and Benedikt Schmidt
   Automated Analysis of Cryptographic Assumptions in Generic Group Models
   Journal of Cryptology. Published online on December 2018.

4. Dario Catalano, Dario Fiore and Luca Nizzardo.
   Homomorphic Signatures with Sublinear Public Keys via Asymmetric Programmable Hash Functions.
   Design, Codes and Cryptography. Accepted on November 2017.

5. Dario Fiore, Maria Isabel Gonzalez Vasco, and Claudio Soriente.
   Partitioned Group Password-Based Authenticated Key Exchange.
   The Computer Journal. Accepted on August 2017.

6. Dario Catalano, Dario Fiore and Rosario Gennaro.
   A Certificateless Aprooach to Onion Routing.
   International Journal of Information Security. Accepted on June 2016.

7. Dario Catalano and Dario Fiore.
   Practical Homomorphic Message Authenticators for Arithmetic Circuits.
   Journal of Cryptology. Accepted on April 2016.

8. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi.
   Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds.
   IET Information Security. Accepted on April 2016.

9. Dario Catalano, Dario Fiore, Rosario Gennaro, and Konstantinos Vamvourellis
   Algebraic (Trapdoor) One-Way Functions: Constructions and Applications
   Theoretical Computer Science. Published online on June 2015.

10. Michel Abdalla, Dario Catalano and Dario Fiore
Verifiable Random Functions: Relations to Identity-Based Key-Encapsulation and New Constructions
Journal of Cryptology. Published online on May 2013. DOI: 10.1007/s00145-013-9153-x.

11. Emmanuel Bresson, Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro
Off-line/on-line signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results
International Journal of Information Security. Springer, May 2013. DOI: 10.1007/s10207-013-0200-2. ISSN: 1615-5262.

12. Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro and Orazio Puglisi
Fully non-interactive Onion Routing with Forward Secrecy
International Journal of Information Security, Vol. 12(1), pp. 33–47. Springer 2013.
DOI: 10.1007/s10207-012-0185-2. ISSN: 1615-5262.

13. Dario Fiore, Rosario Gennaro and Nigel P. Smart.
Relations between the security models for Certificateless Encryption and ID-Based Key Agreement
International Journal of Information Security, Vol. 11(1), pp. 1–22, Springer 2012.

14. Dario Fiore and Rosario Gennaro.
Identity-Based Key-Exchange Protocols without Pairings
Transactions on Computational Sciences X. Special Issue on Security in Computing, Part I.
Volume 6340 of Lecture Notes in Computer Science, pp.42–77, Springer-Verlag 2010.
ISBN: 978-3-642-17498-8

15. Dario Catalano, Mario Di Raimondo, Dario Fiore and Mariagrazia Messina.
Zero-Knowledge Sets with Short Proofs
IEEE Transactions on Information Theory. Vol. 57(4), pp. 2488–2502, April 2011.
ISSN: 0018-9448.

Conference Proceedings

1. Dario Catalano, Dario Fiore, and Emanuele Giunta
Adaptively Secure Single Secret Leader Election from DDH
In the proceedings of the 41st ACM Symposium on Principles of Distributed Computing (PODC 2022).

2. Cecilia Boschini, Dario Fiore, and Elena Pagnin
Progressive And Efficient Verification For Digital Signatures
In the proceedings of the 20th International Conference on Applied Cryptography and Network Security (ACNS 2022).

3. Antonio Faonio, Dario Fiore, Luca Nizzardo, and Claudio Soriente
Subversion-Resilient Enhanced Privacy ID
In the proceedings of CT-RSA 2022.

4. Matteo Campanelli, Antonio Faonio, Dario Fiore, Anais Querol, and Hadrian Rodriguez
Lunar: a Toolbox for More Efficient Universal and Updatable zkSNARKs and Commit-and-Prove Extensions
In the proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2021).

5. Alexandre Bois, Ignacio Cascudo, Dario Fiore, and Dongwoo Kim
Flexible and Efficient Verifiable Computation on Encrypted Data
In the proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC 2021).

6. Daniel Benarroch, Matteo Campanelli, Dario Fiore, Dimitris Kolonelos
   Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
   Financial Cryptography and Data Security (FC 2021).

7. Miguel Ambrona, Dario Fiore, and Claudio Soriente
   Controlled Functional Encryption Revisited: Multi-Authority Extensions and Efficient Schemes for Quadratic Functions
   Proceedings on Privacy Enhancing Technologies, 21st Privacy Enhancing Technologies Symposium (PETS 2021).

8. Matteo Campanelli, Dario Fiore, Nicola Greco, Dimitris Kolonelos, and Luca Nizzardo
   Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage
   In the proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2020).

9. Antonio Faonio, and Dario Fiore
   Improving the Efficiency of Re-Randomizable and Replayable CCA Secure Public Key Encryption
   In the proceedings of the 18th International Conference on Applied Cryptography and Network Security (ACNS 2020).

10. Dario Fiore, Anca Nitulescu, and David Pointcheval
    Boosting Verifiable Computation on Encrypted Data
    In the proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC 2020).

11. Dario Catalano, Mario Di Raimondo, Dario Fiore, and Irene Giacomelli
    MonZa: Fast Maliciously Secure Two Party Computation on Z_{2^k}
    In the proceedings of the International Conference on Practice and Theory in Public-Key Cryptography (PKC 2020).

12. Antonio Faonio, Dario Fiore, Javier Herranz, and Carla Ràfols
    Structure-Preserving and Re-randomizable RCCA-secure Public Key Encryption and its Applications
    In the proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2019).

13. Matteo Campanelli, Dario Fiore, and Anais Querol
    LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs
    In the proceedings of the 26th ACM Conference on Computer and Communications Security (ACM CCS 2019).

14. Dario Fiore, and Elena Pagnin
    Matrioska: A Compiler for Multi-Key Homomorphic Signatures
    In *SCN 2018*.

15. Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu
    Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings
    In *Advances in Cryptology – CRYPTO 2018*.

16. Dario Catalano, Dario Fiore, and Luca Nizzardo
    On the Security Notions for Homomorphic Signatures
    In *ACNS 2018*.

17. Manuel Barbosa, Dario Catalano, and Dario Fiore
    Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data

In the proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017).

18. Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay
Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption
In *Advances in Cryptology – CRYPTO 2017*.

19. Yegveniy Dodis and Dario Fiore
Unilaterally-Authenticated Key Exchange
In *Financial Cryptography and Data Security 2017*.

20. Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, and Elena Pagnin
Multi-Key Homomorphic Authenticators
In the proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2016).

21. Dario Fiore and Anca Nitulescu
On the (In)security of SNARKs in the presence of Oracles
In the proceedings of the 14th IACR Theory of Cryptography Conference – TCC 2016-B.

22. Dario Fiore, Cedric Fournet, Esha Gosh, Markulf Kohlweis, Olya Ohrimenko
Hash First, Argue Later: Adaptive Verifiable Computations on Encrypted Data
In the proceedings of the 23rd ACM Conference on Computer and Communications Security, (ACM CCS 2016).

23. Johannes Krupp, Dominique Schroeder, Mark Simkin, Dario Fiore, Giuseppe Ateniese, and Stefan Nuernberger
Nearly Optimal Verifiable Data Streaming
In the proceedings of the 19th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2016.

24. Dario Catalano and Dario Fiore
Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data
In the proceedings of the 22nd ACM Conference on Computer and Communications Security, Denver, Colorado, USA, October 12–16, 2015 (ACM CCS 2015).

25. Dario Catalano, Dario Fiore, and Luca Nizzardo
Programmable Hash Functions go Private: Constructions and Applications to (Homomorphic) Signatures with Short Public Keys
In *Advances in Cryptology – CRYPTO 2015*.
Selected for presentation at JNIC 2015 (Jornadas Nacionales de Investigacion en Ciberseguridad) where it was the recipient of a best paper award for the category of short papers (which includes already published works).

26. Manuel Barbosa, Michael Backes, Dario Fiore, and Raphael M. Reischuk
ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data
IEEE Security and Privacy (Oakland) 2015.

27. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi
Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds
In the proceedings of the 18th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2015.

28. Dario Fiore, Rosario Gennaro, and Valerio Pastro
Efficiently Verifiable Computation on Encrypted Data
In the proceedings of the 21st ACM Conference on Computer and Communications Security, Scottsdale, Arizona, USA, November 3–7, 2014 (ACM CCS 2014).

29. Yegveniy Dodis and Dario Fiore
Interactive Encryption and Message Authentication
In *Security and Cryptography for Networks – SCN 2014*.

30. Gilles Barthe, Edvard Fagerholm, Dario Fiore, Andre Scedrov, John Mitchell, and Benedikt Schmidt
Automated Analysis of Cryptographic Assumptions in Generic Group Models
In *Advances in Cryptology – CRYPTO 2014*.

31. Dario Catalano, Dario Fiore, and Bogdan Warinschi
Homomorphic Signatures with Efficient Verification for Polynomial Functions
In *Advances in Cryptology – CRYPTO 2014*.

32. Dario Catalano, Dario Fiore, Rosario Gennaro, and Luca Nizzardo
Generalizing Homomorphic MACs for Arithmetic Circuits
In the proceedings of the 17th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2014, Buenos Aires, Argentina, March 26–28, 2014. Volume 8383 of Lecture Notes in Computer Science, pp. 538–555, Springer-Verlag 2014.

33. Michael Backes, Dario Fiore, and Raphael M. Reischuk
Verifiable Delegation of Computation on Outsorced Data
In the proceedings of the 20th ACM Conference on Computer and Communications Security, Berlin, Germany, November 5–7, 2013 (ACM CCS 2013).

34. Michael Backes, Dario Fiore, and Esfandiar Mohammadi
Privacy-Preserving Accountable Computation
In the proceedings of the 18th European Symposium on Research in Computer Security, Egham, UK, September 9–13, 2013 (ESORICS 2013), pp. 38–56.

35. Dario Catalano and Dario Fiore
Practical Homomorphic MACs for Arithmetic Circuits
In *Advances in Cryptology – EUROCRYPT 2013*, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26–30, 2013. Volume 7881 of Lecture Notes in Computer Science, pp. 336–352. Springer-Verlag 2013.

36. Dario Catalano, Dario Fiore, Rosario Gennaro and Konstantinos Vamvourellis
Algebraic (Trapdoor) One-Way Functions and their Applications
In the proceedings of the 10th Theory of Cryptography Conference – TCC 2013, Tokyo, Japan, March 3–6, 2013. Volume 7785 of Lecture Notes in Computer Science, pp. 680–699, Springer-Verlag 2013.

37. Dario Catalano and Dario Fiore
Vector Commitments and their Applications
In the proceedings of the 16th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2013, Nara, Japan, February 26 – March 1, 2013. Volume 7778 of Lecture Notes in Computer Science, pp. 55–72, Springer-Verlag 2013.

38. Dario Fiore and Rosario Gennaro
Publicly Verifiable Delegation of Large Polynomials and Matrix Computations, with Applications
In the proceedings of the 19th ACM Conference on Computer and Communications Security, Raleigh, NC (USA), October 16–18, 2012 (ACM CCS 2012), pp. 501–512.

39. Dario Catalano, Dario Fiore and Bogdan Warinschi
Efficient Network Coding Signatures in the Standard Model In the proceedings of the 15th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2012, Darmstadt, Germany, May 21-23, 2012. Volume 7293 of Lecture Notes in Computer Science, pp. 680–696, Springer-Verlag 2012.

40. Michel Abdalla, Dario Fiore and Vadim Lyubashevsky
From Selective to Full Security: Semi-Generic Transformations in the Standard Model
In the proceedings of the 15th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2012, Darmstadt, Germany, May 21-23, 2012. Volume 7293 of Lecture Notes in Computer Science, pp. 316–333, Springer-Verlag 2012.

41. Dario Fiore and Dominique Schroeder
Uniqueness is a Different Story: Impossibility of Verifiable Random Functions from Trapdoor Permutations
In the proceedings of the 9th Theory of Cryptography Conference – TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Volume 7194 of Lecture Notes in Computer Science, pp. 636–653, Springer-Verlag 2012.

42. Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro and Orazio Puglisi
Fully non-interactive Onion Routing with Forward Secrecy
In the proceedings of the 9th International Conference on Applied Cryptography and Network Security – ACNS 2011, Nerja, Spain, June 7–10, 2011. Volume 6715 of Lecture Notes in Computer Science, pp. 255–273, Springer-Verlag 2011.

43. Dario Catalano, Dario Fiore and Bogdan Warinschi
Adaptive Pseudo-Free Groups and Applications
In Advances in Cryptology – EUROCRYPT 2011, 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallin, Estonia, May 15–19, 2011. Proceedings. Volume 6632 of Lecture Notes in Computer Science, pp. 207–223, Springer-Verlag 2011

44. Dario Fiore, Rosario Gennaro and Nigel P. Smart
Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key- Agreement
In the proceedings of Pairing-Based Cryptography – Pairing 2010, 4th International Conference, Yamanaka Hot Spring, Japan, December 13-15, 2010, Proceedings. Volume 6487 of Lecture Notes in Computer Science, pp.167–186, Springer-Verlag 2010.

45. M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Dionida Labati, P. Faill, D. Fiore, R. Lazzeretti, V. Piuri and F. Scotti
A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates
IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2010), September 27–29, 2010, Washington, D.C., USA. IEEE. IEEE Catalog Number: CFP10BTA-USB; ISBN: 978-1-4244-7580-3

46. M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Dionida Labati, P. Faill, D. Fiore, R. Lazzeretti, V. Piuri and F. Scotti
Privacy-Preserving Fingercode Authentication
In the proceedings of the 12th ACM Workshop on Multimedia and Security (ACM MM & Sec 2010) – ACM, ISBN 978-1-4503-0286-9, Order n. 433102, pp. 231–241

47. Dario Fiore and Rosario Gennaro
Making the Diffie-Hellman Protocol Identity-Based
In Topics in Cryptology – CT-RSA 2010 The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1–5, 2010. Proceedings. Volume 5985 of Lecture Notes in Computer Science, pp.165–178, Springer-Verlag 2010

48. Dario Catalano, Dario Fiore and Rosario Gennaro
Certificateless Onion Routing
In the proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL (USA), November 10–13, 2009 (ACM CCS 2009) – ACM, ISBN 978-1-60558-894-0, Order no. 537091, pp. 151–160

49. Michel Abdalla, Dario Catalano and Dario Fiore
Verifiable Random Functions from Identity-Based Key-Encapsulation
In Advances in Cryptology – EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26–30, 2009. Proceedings. Volume 5479 of Lecture Notes in Computer Science, pp.554–571, Springer-Verlag 2009

50. Dario Catalano, Dario Fiore and Mariagrazia Messina
Zero-Knowledge Sets with short proofs
In Advances in Cryptology – EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings Volume 4965 of Lecture Notes in Computer Science, pp.433–450, Springer-Verlag 2008

51. Dario Catalano, Mario Di Raimondo, Dario Fiore and Rosario Gennaro
Off-Line/On-Line Signatures: Theoretical aspects and Experimental Results
In Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography, Barcelona, Spain, March 2008 (PKC 2008). Volume 4939 of Lecture Notes in Computer Science, pp.101–120, Springer-Verlag 2008

Patents

1. Claudio Soriente, Antonio Faonio, Dario Fiore, Luca Nizzardo. *Subversion Resilient Attestation for Trusted Execution Environments*. Granted by the United States Patent & Trademark Office (US 11,361,069), and by the European Patent office (EP 3 627 367), 2022.

2. Claudio Soriente, Miguel Ambrona, Dario Fiore. *Multi-authority Controlled Functional Encryption*. US provisional Patent application no. US 62/834,458. Submitted on April 2019.

Projects (as PI or co-PI)

1. European Research Council (ERC) Consolidator grant "PICOCRYPT" (June 2021–May 2026). PI.

2. Protocol Labs Research Grant on "Foundations of Functional Commitments" (2022), in collaboration with Dominique Schroeder (FAU, Germany).

3. NEC Labs Europe Research Contract on "Secure, Private and Verifiable Computation for Machine Learning" (2022). PI.

4. NEC Labs Europe Research Contract on "Securing Computation for Big Data" (2021). PI.

5. Research Grant from Tezos Foundation & Nomadic Labs on "Cryptographic primitives for privacy and randomness generation" (November 2020–October 2022). Co-PI with Ignacio Cascudo.

6. BBVA research contract (January–August 2020). Co-PI with Antonio Faonio.

7. NEC Labs Europe Research Contract on "Securing Computation in Platforms" (2020). PI.

8. Spanish MICINN Red de Investigación "SECURITAS" (Jan 2020–Dec 2022). Local PI.

9. Spanish MICINN Retos de la Investigación grant "SCUM" (Jan 2019–Dec 2022). Co-PI with Juan Caballero.
10. Protocol Labs Research Grant on "Novel Constructions of Proof-of-Spacetime" (Aug 2018–May 2020). Co-PI with Matteo Campanelli.
11. NEC Labs Europe Research Contract on "Securing Data and Computation in Distributed Systems" (2019). PI.
12. NEC Labs Europe Research Contract on "Secure Cloud Storage with Controlled Computation" (2018). PI.
13. Spanish MICINN Europa Excelencia grants "CRYPTOEPIC" (Dec 2018–Dec 2021). PI.
14. Spanish MINECO RETOS grant "DataMantium" (July 2016–June 2019). Co-PI with Carmela Troncoso.
15. EU H2020 project "NEXTLEAP" (2016–2018). Co-PI with Carmela Troncoso.
16. EIT Digital activity "HC@WORKS" (2016). PI.
17. Spanish MINECO "Juan de la Cierva Incorporación" fellowship (2016–2017).
18. EU COST Action IC1306 "Cryptography for Secure Digital Interaction" (2014–2018). Vice-chair.

Invited Talks and Seminars

A journey in vector commitments.
– Invited talk at Vector commitment research day, hosted by Protocol Labs, virtual. April 2022. – IWSEC 2021, virtual. September 2021.

Succinct Zero-Knowledge Batch Proofs for Set Accumulators.
– Nomadic Labs research seminars. February 2022.

Cryptography for Privacy and Integrity of Computation on Untrusted Machines.
– Summer seminars on cybersecurity", Department of Computer, Control and Management Engineering of Sapienza University of Rome, June 2021.

Boosting Verifiable Computation on Encrypted Data.
– Kookmin University, South Korea, August 2020.

LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs.
– Invited talk at 2nd ZKP Workshop, Berkeley, United States. April 2019. – ICIAM 2019, Valencia, Spain. July 2019.

Homomorphic Authentication for Computing Securely on Untrusted Machines.
– Invited Keynote at NordSec 2017, Tartu, Estonia. November 2017.
– Invited talk at Paris Crypto Day, Paris, France, March 2019.
– Invited talk at University of Verona, Italy, May 2019.

Zero-Knowledge Proofs and Applications to IoT and Blockchains.
– Invited talk at B4Things, Madrid, Spain. April 2018.

Computing Quadratics Functions on Encrypted Data.
– Invited talk at MathCrypt 2017, Daejeon, South Korea. June 2017.

On the (In)Security of SNARKs in the Presence of Oracles.
– II CryptoAction Symposium, Amsterdam, The Netherlands. March 2017.
– IV Congreso de Jóvenes Investigadores de la Real Sociedad Matemática Española, Valencia, Spain. September 2017.

Secure Outsourcing of Data and Computation to the Cloud.
– Invited talk at the EIT Digital Symposium: security of digital systems and protocols, Rennes, France. November 2016.

Labeled Homomorphic Encryption: Practical Delegation of Computation on Encrypted Data.
– 3rd Microsoft Research—IMDEA Software Institute Collaboration Workshop (MICW 2016), Cambridge, UK. May 2016.

ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data.
— CryptoAction Symposium, Budapest, Hungary. April 2016.
— Hanyang University, Seoul, South Korea. July 2017.

Ensuring integrity in Cloud computing via homomorphic digital signatures: new tools and results.
— CyberCamp 2015, Madrid, Spain. November 2015.

Programmable Hash Functions go Private: Constructions and Applications to (Homomorphic) Signatures with Short Public Keys.
— Cryptography Seminars Day @ UPC, Universitat Politècnica de Catalunya, Barcelona, Spain. September 2015.
— Cryptography Workshop, Bochum, Germany. April 2015.

Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data.
— Congreso Jovenes Investigadores RSME, Murcia, Spain. September 2015.
— ENS, Paris, France. March 2015.

Advanced Cryptographic Techniques for Secure Outsourcing to the Cloud.
— Universisad Carlos III, Madrid, Spain. February 2015.

Efficiently Verifiable Computation on Encrypted Data.
— CryptoAction WG1 Meeting, Warsaw, Poland. March 2015.

Verifiable Delegation of Computation on Outsourced Data.
— Universidad Rey Juan Carlos, Madrid, Spain. May 2014.
— Instituto de Computacion, Facultad de Ingenieria, Universidad de la Republica, Montevideo, Uruguay. March 2014.
—2nd PROMETIDOS Winter School, Madrid, Dec 2013.

Practical Homomorphic MACs for Arithmetic Circuits.
— ENS Lyon, France. June 2013.

Publicly Verifiable Delegation of Large Polynomials and Matrix Computations.
— IBM T.J. Watson Research Center, Yorktown Heights, NY, USA. October 2012.
— Université de Versailles Saint-Quentin-en-Yvelines, Versailles, France. April 2013.

Verifiable Outsourcing of Computation.
— New York University, New York, NY, USA. September 2012.

Vector Commitments and their Applications.
— ENS, Paris, France. March 2012.
— IBM T.J. Watson Research Center, Hawthorne, NY, USA. March 2012.
— UPC Barcelona, Spain. June 2013.

Adaptive Pseudo-Free Groups and Applications.
— New York University, New York, NY, USA. February 2012.
— European Postdoctoral Day of Excellence in Cryptography, Darmstadt, Germany. November 2011
— Université de Caen, Caen, France. June 2011
— LACS Seminar, University of Luxembourg, Luxembourg, May 2011
— ENS, Paris, France. May 2010.
— First CryptoForma Workshop, Institut Henri Poincaré, Paris, France. May 2010.

Certificateless Onion Routing.
— University of Bristol, Bristol, UK. November 2009.
— IBM T.J. Watson Research Center, Hawthorne, NY, USA. November 2009.

Zero-Knowledge Sets with Short Proofs.
— IBM T.J. Watson Research Center, Hawthorne, NY, USA. November 2008.
— NYU, New York, USA. October 2008.

Students

Graduated PhD Students:

1. Luca Nizzardo, IMDEA Software Institute (September 2014 – May 2018);
   Thesis title: *Cryptographic Techniques for the Security of Cloud and Blockchain Systems.*
   → Research scientist at Protocol Labs.

2. Elena Pagnin, Chalmers University (October 2016 – September 2018). Jointly supervised with Andrei Sabelfeld.
   Thesis title: *Be More and Be Merry: Enhancing Data and User Authentication in Collaborative Settings.*
   → Postdoc at Aarhus University. → Assistant Professor at Lund University.

3. Anca Nitulescu, ENS Paris (October 2015 – *Defense scheduled on April 1, 2019*). Jointly supervised with David Pointcheval and Michel Abdalla.
   Thesis title: *A tale of SNARKs: quantum resilience, knowledge extractability and data privacy.*
   → Postdoc at Aarhus University. → Cryptographer at Cosmian.

Current PhD Students:

1. Anaïs Querol Cruz, IMDEA Software Institute (October 2018 – present).

2. Dimitris Kolonelos, IMDEA Software Institute (March 2019 – present).

3. David Balbás, IMDEA Software Institute (October 2021 – present).

Postdocs

1. Hamza Abusalah, IMDEA Software Institute (May 2022 – present).

2. Peter Chvojka, IMDEA Software Institute (October 2021 – present).

3. Lydia Garms, IMDEA Software Institute (April 2021 – April 2022).

4. Ida Tucker, IMDEA Software Institute (October 2020 – January 2022).

5. Antonio Faonio, IMDEA Software Institute (January 2017 – June 2020).

6. Matteo Campanelli, IMDEA Software Institute (March 2018 – July 2020).
7. Miguel Ambrona, IMDEA Software Institute (January 2019 – May 2019).

Professional Activities

Program Committee member: ACM CCS (2015, 2016, 2018, 2019, 2022); CRYPTO (2015, 2018, 2022); PKC (2011, 2015–2017, 2019–2020, 2022); Eurocrypt (2016, 2021); Asiacrypt (2017); EuroS&P (2016–2017); Financial Crypto (2017, 2018, 2020–2021); ACM Cloud Computing Security Workshop (2017); Africacrypt (2014, 2016); SEC@ACM SAC (2016); SCN (2014); Pairing (2012, 2013); The Third International Workshop on Security in Cloud Computing (SCC 20015); Workshop on Applied Homomorphic Cryptography (WAHC) (2013–2015); IWSEC (2012–2013); I Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2015).

Editorial Board of International Journals: IET Information Security, International Journal of Applied Cryptography.

External Reviewer for:

Conferences: Crypto (2009, 2011–2014, 2016, 2017); Eurocrypt (2009, 2011–2015, 2017–2019); Asiacrypt (2011–2014, 2016); TCC (2009–2016); PKC (2010–2014, 2018); FOCS (2008); ACM CCS (2012–2014); IEEE S&P Oakland (2013–2014); NDSS (2016); CC (2016); ISSAC (2016); CT-RSA (2008); ESORICS (2015); ACNS (2011–2012); SCN (2008, 2012); ACM SAC (Security Track) (2014–2015); Inscrypt (2013); ICALP (2011); ITCS (2012).

Journals: Nature, ACM TISSEC, IEEE Transactions on Information Forensic and Security, Design Codes and Cryptography, Algorithmica, Journal of Computer Security, Transactions on Computers, Journal of Computational and Applied Mathematics, IET Information Security.

Teaching

Fall 2014–2020 **Co-Instructor** for the course "Computer Security" (graduate program in Computer Science)
Institute: Universidad Politecnica de Madrid (UPM)

Spring 2018 **Instructor** for the course "Foundations of Cryptography" (graduate program in Computer Science)
Institute: Universidad Politecnica de Madrid (UPM)

Fall 2014 **Instructor** for the course "Introduction to Cryptography" (graduate program in Computer Science)
Institute: Universidad Politecnica de Madrid (UPM)

Jan 2013 **Guest lectures** on "Functional Encryption"
Course: Public Key Encryption
Institute: Saarland University, Germany
Instructor: Prof. Dominique Schroeder.

Spring 2012 **Teaching Assistant**, Dept. of Computer Science, New York University
Course: Introduction to Cryptography (graduate program of Math and Computer Science)
Instructor: Prof. Yevgeniy Dodis.

Sep 6–9, 2011 **Invited lectures** on "Impossibility results and Black-Box Separations"
Course: Foundations of Cryptography
Institute: Scuola Superiore di Catania (Mediterranean University Center), Catania, Italy
Instructor: Prof. Dario Catalano.

Fall 2008 **Teaching Assistant**, Dept. of Computer Science, New York University
Course: Introduction to Cryptography (graduate program in Computer Science)
Instructor: Prof. Yevgeniy Dodis.

2007–2009 **Invited lectures** on "Real time security protocols" and "RFID protocols"
Course: Computer Security (undergraduate program in Computer Science)
Institute: University of Catania, Catania, Italy.
Instructor: Prof. Dario Catalano.

Languages

Italian: *mother tongue*. English: *fluent*. French: *fluent*. Spanish: *fluent*.

Last updated: June 18, 2022