Dario Fiore

IMDEA Software Institute
Campus Montegancedo s/n,
28223 Pozuelo de Alarcón, Madrid
SPAIN

Phone: (+34) 911012202 (ext. 4160)
Mobile: (+34) 722497624
Email: dario.fiore@imdea.org
Homepage: http://www.dariofiore.it

Personal Data

Date of birth: April 11, 1983 Citizenship: Italian

Current Position

Nov.2013 — Present **Assistant Research Professor** (tenure-track)
IMDEA Software Institute, Madrid, Spain

Research Interests

Cryptography and Security

Education and Training

Nov.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.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

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. 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.

2. 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.

3. 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.

4. 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.

5. 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

6. 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. 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.

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

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

4. 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*.

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

6. 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.

7. 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).

8. 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.

9. 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.

10. 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.
    Also in Cryptology ePrint Archive, Report 2012/434.

11. 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.
    Also in Cryptology ePrint Archive, Report 2011/495.

12. 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.

13. 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.
Also in IACR ePrint Archive – Report 2011/696

14. 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.

15. 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.
Also in IACR ePrint Archive – Report 2010/648

16. 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.

17. 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

18. 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.

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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

25. 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

Invited Talks

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.

Professional Activities

Projects: Vice-Chair and Management Committee member (representing Spain) of COST Action IC1306 "Cryptography for Secure Digital Interaction".

Program Committee member: CRYPTO 2015, PKC 2015, The Third International Workshop on Security in Cloud Computing (SCC 20015), SCN 2014, Africacrypt 2014, Pairing 2012–2013, Workshop on Applied Homomorphic Cryptography (WAHC) 2013–2015, IWSEC 2012–2013, PKC 2011.

External Reviewer for (selection): Eurocrypt 2009, 2011–2015. Crypto 2009, 2011–2014. Asiacrypt 2011–2014. TCC 2009–2013. PKC 2010–2014. FOCS 2008. ACM CCS 2012–2014. Oakland 2013–2014, CT-RSA 2008. ACM SAC (Security Track) 2014–2015, Inscrypt 2013, ACNS 2011–2012. SCN 2008, 2012. ICALP 2011, ITCS 2012.
Journals: Design Codes and Cryptography, Algorithmica, ACM TISSEC, , Journal of Computer Security, IEEE Transactions on Information Forensic and Security, Transactions on Computers, Journal of Computational and Applied Mathematics.

Teaching Experience

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

Supervision of students

- (PhD student) Luca Nizzardo, IMDEA Software Institute (September 2014 –)
- Luca Nizzardo, IMDEA Software Institute
  March–June 2014. Research internship on "Constrained Pseudorandom Functions".
- Raphael M. Reischuk, Saarland University
  Research project on "Verifiable delegation of computation and homomorphic MACs". Results of the project published at ACM CCS 2013.
- Konstantinos Vamvourellis, New York University
  Master's thesis "Algebraic (Trapdoor) One-Way Functions and Applications to Linearly-Homomorphic Signatures" (co-advised with Yevgeniy Dodis), submitted to NYU on May 2013.
  Research project on linearly-homomorphic signatures. Results of the project published at TCC 2013.
- Mariagrazia Messina, University of Catania
  Master thesis: "Efficient constructions of Zero-Knowledge Sets" (co-advised with Dario Catalano), October 2007.
  Research project on "Zero-Knowledge Sets". Work published at Eurocrypt 2008.

Languages

Italian: *native*. English: *fluent*. French: *fluent*. Spanish: *basic*.

Last updated: January 19, 2015