

Dario Fiore

Dept. of Computer Science
New York University
251 Mercer Street,
New York, NY – 10012, USA

Phone: (+1) 212-992-7533
Mobile: (+1) 646-538-9417
Email: fiore@cs.nyu.edu
Homepage: <http://www.dariofiore.it>

Personal Informations

Born on April 11, 1983.

Citizenship: Italian.

Research Interests: Cryptography and Security.

Education

January 2007 – March 2010: *Ph.D. in Computer Science*, University of Catania, Italy.

Completed on: March 1, 2010.

Advisor: Prof. Dario Catalano.

Thesis: “Efficient Cryptographic Constructions from Bilinear Maps”.

October 2004 – July 2006: *Master in Computer Science*, University of Catania, Italy.

Completed on: July 27, 2006.

Grade: 110/110 cum laude.

Thesis: “About timestamping and its application to a technical report archive system” (in italian).

Thesis Advisors: Prof. Domenico Cantone, Dr. Mario Di Raimondo.

October 2001 – October 2004: *Bachelor in Computer Science*, University of Catania, Italy.

Completed on: October 8, 2004.

Grade: 110/110.

Thesis: “A tool to visualize shortest path algorithms on grid graphs” (in italian).

Thesis Advisors: Prof. Domenico Cantone, Dr. Simone Faro.

Research

Research Experience

January 2012 – Present: *Postdoctoral Researcher*, Courant Institute of Mathematical Sciences, New York University, New York, NY, USA.

April 2010 – December 2011: *Postdoctoral Researcher*, École Normale Supérieure, Paris, France.

August – December, 2008: *Visiting Student under Prof. Yeogeniy Dodis*. New York University, New York, NY, USA.

September – December, 2008: *Visiting Student under Dr. Rosario Gennaro*. IBM T.J. Watson Research Center, Hawthorne, NY, USA.

Publications

Journal Papers

1. 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.
2. 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
3. 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.

Conference Papers

1. 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, to appear.
Also in IACR ePrint Archive – Report 2011/696
2. 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, to appear.
3. 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, to appear.
Also in IACR ePrint Archive – Report 2010/648
4. 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.
5. 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
6. 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.

7. 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 Fingercodes 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
8. 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 Fingercodes 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
9. 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
10. 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
11. 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
12. 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
13. 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

Other Papers

- Dario Catalano and Dario Fiore
Vector Commitments and their Applications, Cryptology Eprint Archive, Report 2011/495.

Invited Talks

- *Vector Commitments and their Applications*.
ENS, Paris, France. March 2012.

IBM T.J. Watson Research Center, Hawthorne, NY, USA. March 2012.

- *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

Program Committee member: IWSEC 2012, Pairing 2012, PKC 2011.

External Reviewer for (selection): Eurocrypt 2009, 2011, 2012. Crypto 2009, 2011, 2012. Asiacrypt 2011.
TCC 2009, 2010, 2011, 2012. PKC 2010, 2012. FOCS 2008. CT-RSA 2008. ACNS 2011. SCN 2008.

Teaching Experience

Semester Spring 2012: Teaching Assistant.

Course: Introduction to Cryptography (graduate program of Math and Computer Science)
Institute: Department of Computer Science, New York University, New York, NY, USA.
Instructor: Prof. Yevgeniy Dodis.

September 6–9, 2011: Series of 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.

Semester Fall 2008: Teaching Assistant.

Course: Introduction to Cryptography (graduate program in Computer Science)
Institute: Department of Computer Science, New York University, New York, NY, USA.
Instructor: Prof. Yevgeniy Dodis.

Academic Years 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.

Academic Years 2007–2009: Teaching Assistant.

Course: Cryptography (graduate program in Computer Science)
Institute: University of Catania, Catania, Italy.
Instructor: Prof. Dario Catalano.

Thesis Co-Advisor

Master thesis: "Efficient constructions of Zero-Knowledge Sets", Mariagrazia Messina, October 2007.

Awards

PhD fellowship (3 years) sponsored by the Italian ministry of education, December 2006.

Languages

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

Last updated: April 26, 2012