

CURRICULUM VITÆ ET STUDIORUM

Anna Lisa Ferrara

1 OCTOBER, 2010

Contents

1	Personal Data	2
2	Current Position	2
3	Education	2
4	Research Experiences	3
5	Projects	3
6	Teaching Activity	3
7	Refereeing for Conferences and Journals	4
8	Conference Talks Given	4
9	Publications	4

1 Personal Data

First Name: Anna Lisa
Family Name: Ferrara
Birth Date: 02/24/1977
Birth Place: Napoli (Italy)
Citizenship: Italian

Dipartimento di Informatica ed Applicazioni
Università degli Studi di Salerno
84081 Fisciano (SA), Italy

E-mail: ferrara@dia.unisa.it
URL: <http://www.dia.unisa.it/dottorandi/ferrara>

2 Current Position

- I am a post-doc at the the Dipartimento di Informatica ed Applicazioni of the Università degli Studi di Salerno (Italy).

3 Education

- I attended the *Autumn International School on Zero Knowledge: Foundations and Applications*, held at the University of Bologna Residential Center Bertinoro (Forlì), Italy, from October 28 - November 3, 2006. Speakers: Yehuda Lindell (Bar-Ilan University, ISRAEL), Giuseppe Persiano (University of Salerno, ITALY), Jonathan Katz (University of Maryland, USA).
- On April 2006, I received a PhD in Computer Science (*Dottorato di Ricerca in Informatica*) at the *Università degli Studi di Salerno*, discussing a thesis in Cryptography whose title is: *On Access Control Policies and Key Assignment Schemes*. The thesis was supervised by Prof. Alfredo De Santis.
- From September 2004 to May 2005, I was a visiting researcher at the CACR (Centre for Applied Cryptographic Research) in the School of Computer Science of the University of Waterloo, Ontario, Canada.
- I attended the *Advanced Course on Contemporary Cryptology*, held in Barcelona, Spain, from February 2, to February 13, 2004. Speakers: Dario Catalano (École Normale Supérieure, Paris), Ivan Damgård (Aarhus Universitet), Giovanni Di Crescenzo (Telcordia Technologies, Inc. Morristown, New Jersey), David Pointcheval (École Normale Supérieure, Paris), Tsuyoshi Takagi (Technische Universität Darmstadt).

- On July 2002, I received a Master with Honours in Computer Science (*Laurea cum laude in Informatica*) at the Università degli Studi di Salerno, discussing a thesis in Cryptography whose title is: *Assegnamento di Chiavi in una Gerarchia* (Hierarchical Key Assignment Schemes). The thesis was supervised by Prof. Alfredo De Santis.

4 Research Experiences

- From February 2008 to April 2009, I was visiting researcher at the Department of Computer Science, University of Illinois at Urbana-Champaign.
- From February 2007 to January 2008, I held a Post-Doctoral Fellowship at the Department of Computer Science, within the School of Engineering at the Johns Hopkins University.
- From December 2005 to January 2007, I held a Research Fellowship (Assegno di Ricerca) at the Dipartimento di Informatica ed Applicazioni of the Università degli Studi di Salerno (Italy).

5 Projects

- Member of *European Network of Excellence in Cryptology - ECRYPT*, project n. IST-2003-507932.
- Member of the Italian Projects 60%, every year since 2002.
- Member of the Italian Project ex 40% - MURST, 2006: *Confidentiality and Selective Access in a Database as a Service Scenario*. (coordinator: Prof. S. Paraboschi, Università di Bergamo).

6 Teaching Activity

- In May 2009, I offered the class *Advanced Topics in Network Security - Access Control: An Information Theoretic Approach and Provable Secure Solutions* at the ICT International Doctorate School, Trento, Italy.
- From June to October, every year since 2006, I was tutor for the *Cryptography* class of the Master in System Security and Networks (Sicurezza dei Sistemi e delle Reti Informatiche), online edition, Università degli Studi di Milano.
- From 2003 to 2006 I was teaching assistant for the class *Network Security*, of the Master in Computer Science, Università di Salerno.

7 Refereeing for Conferences and Journals

I have been involved in reviewing processes for several international journals and conferences (*Design, Codes and Cryptography, Theoretical Computer Science, IEEE Transaction on Computers, Information Processing Letters, IEEE Transaction on Knowledge and Data Engineering, IEEE Transaction on Information Forensic and Security, Information Sciences, CCS 2007, PKC 2007, ICICS 2007, PET 2007, ICALP 2008, Asiacrypt 2008, PKC 2009, Asiacrypt 2009, TCC 2009, PKC 2010, SAC 2010, ICISC 2010, PKC 2011.*)

8 Conference Talks Given

- *34th International Symposium on Mathematical Foundations of Computer Science (MFCS 2009)*, Novy Smokovec, Slovak Republic, August 24 - 28, 2009. *Security and Tradeoffs of the Akl-Taylor Scheme and its Variants.*
- *32nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2007)*, 27-31 August 2007, Cesky Krumlov, Czech Republic. *Efficient Provably-Secure Hierarchical Key Assignment Schemes.*
- *12th ACM Symposium on Access Control Models and Technologies (SACMAT 2007)*, 20-22 June 2007, Sophia Antipolis, France. *New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes.*
- *International Workshop on Coding and Cryptography (WCC 2005)*, 14-18 Marzo 2005, Bergen, Norway. *A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy.*
- *The Eighth Italian Conference on Theoretical Computer Science (ICTCS 2003)*, 13 - 15 October 2003, University Center Bertinoro, Italy. *An Information-Theoretic Approach to the Access Control Problem.*

9 Publications

International Journals:

- G. Ateniese, A. De Santis, A. L. Ferrara, B. Masucci, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, *Journal of Cryptology*, accepted for publication.
- P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci, Variations on a Theme by Akl and Taylor: Security and Tradeoffs, *Theoretical Computer Science*, Vol. 411, pp. 213-227, 2010.
- A. De Santis, A. L. Ferrara, and B. Masucci, New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, *Theoretical Computer Science*, Vol. 407, No. 1-3, pp. 213-230, November 2008.

- A. De Santis, A. L. Ferrara, and B. Masucci, An Attack on a Payment Scheme, *Information Sciences*, *Information Sciences*, Vol. 178 , No. 5, pp. 1418-1421, March 2008.
- A. De Santis, A. L. Ferrara, and B. Masucci, Enforcing the Security of a Time-Bound Hierarchical Key Assignment Scheme, *Information Sciences*, Vol. 176, No. 12, pp. 1684–1694, June 2006.
- A. De Santis, A. L. Ferrara, and B. Masucci, Unconditionally Secure Key Assignment Schemes, *Discrete Applied Mathematics*, Vol. 154, No. 2, pp. 234–252, February 2006.
- S. Cimato, A. De Santis, A. L. Ferrara and B. Masucci, Ideal Contrast Visual Cryptography Schemes with Reversing, *Information Processing Letters*, Vol. 93, No. 4, pp. 199-206, February 2005.
- A. De Santis, A. L. Ferrara, and B. Masucci, Cryptographic Key Assignment Schemes for Any Access Control Policy, *Information Processing Letters*, Vol. 92, No. 4, pp. 199-205, November 2004.
- F. Y. L. Chin, A. De Santis, A. L. Ferrara, N. L. Ho and S. K. Kim, A Simple Algorithm for the Constrained Sequence Problem, *Information Processing Letters*, Vol. 90, No. 4, , pp. 175-179, May 2004.
- C. Blundo, S. Cimato, R. De Prisco and A. L. Ferrara, Modeling a Certified Email Protocol using I/O Automata, *Electronic Notes in Theoretical Computer Science*, Elsevier, Vol. 99, pp. 339-359, 2004.

International Conferences:

- P. D’Arco, A. De Santis, A. L. Ferrara, and B. Masucci, Security and Tradeoffs of the Akl-Taylor Scheme and its Variants, in *Proc. of the 34th International Symposium on Mathematical Foundations of Computer Science - MFCS 2009*, Novy Smokovec, High Tatras, Slovak Republic, August 24 - 28, 2009, R. Krlovc and D. Niwinski (Eds.), *Lecture Notes in Computer Science*, Vol. 5734, pp. 247-257, Springer Verlag, 2009.
- Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, Michael Østergaard Pedersen, Practical Short Signature Batch Verification. *Topics in Cryptology - CT-RSA 2009*, The Cryptographers’ Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009, Marc Fischlin (Ed.), *Lecture Notes in Computer Science*, vol. 5473, pp. 309–324, Springer Verlag, 2009.
- A. De Santis, A. L. Ferrara, and B. Masucci, Efficient Provably-Secure Hierarchical Key Assignment Schemes, in *Proc. of the 32nd International Symposium on Mathematical Foundations of Computer Science - MFCS 2007*, Cesky Krumlov, Czech Republic, August 27 - 31, 2007, L. Kucera and A. Kucera (Eds.), *Lecture Notes in Computer Science*, Vol. 4708, pp. 371–382, Springer Verlag, 2007.

- A. De Santis, A. L. Ferrara, and B. Masucci, New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, in Proc. of the 12th ACM Symposium on Access Control Models and Technologies - SACMAT 2007, Sophia Antipolis, France, June 20 - 22 2007, pp. 133–138.
- G. Ateniese, A. De Santis, A. L. Ferrara, and B. Masucci, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, in Proc. of the 14th ACM Conference on Computer and Communications Security - CCS 2006, Alexandria, Virginia, USA, November 2006, pp. 288–297.
- A. De Santis, A. L. Ferrara, and B. Masucci, A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy, in Proc. of the International Workshop on Coding and Cryptography - WCC 2005, Bergen, Norway, March 14 - 18 2005, O. Ytrehus (Ed.), Lecture Notes in Computer Science, Vol. 3969, pp. 202–217, Springer Verlag, 2006.
- A. De Santis, A. L. Ferrara and B. Masucci, Unconditionally Secure Hierarchical Key Assignment Schemes, in Proc. of the International Workshop on Coding and Cryptography - WCC 2003, Veirsalles, France, March 24 - 28, 2003.

National Conferences:

- A. L. Ferrara and B. Masucci, An Information-Theoretic Approach to the Access Control Problem, in Proc. of The Eighth Italian Conference on Theoretical Computer Science - ICTCS 2003, University Center Bertinoro, Italy, October 13 - 15, 2003, Lecture Notes in Computer Science, Vol. 2841, pp. 342–354, Springer Verlag, 2003.