

CURRICULUM VITÆ ET STUDIORUM DI

Anna Lisa Ferrara

24 FEBBRAIO 2008

Indice

| | | |
|----------|---|----------|
| 1 | Dati Personali | 2 |
| 2 | Posizione Attuale | 2 |
| 3 | Formazione | 2 |
| 4 | Partecipazione a Progetti Internazionali e Nazionali | 3 |
| 5 | Presentazioni a Conferenze Nazionali ed Internazionali | 4 |
| 6 | Attività Didattica | 4 |
| 7 | Attività di Revisione | 4 |
| 8 | Attività di Ricerca | 4 |
| 9 | Elenco delle Pubblicazioni | 5 |

1 Dati Personali

Nome: Anna Lisa
Cognome: Ferrara
Data di nascita: 24/02/1977
Luogo di nascita: Napoli
Stato civile: Nubile

Dipartimento di Informatica ed Applicazioni,
Università degli studi di Salerno Via Ponte Don Melillo
84081 Fisciano (SA)

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

Department of Computer Science,
University of Illinois at Urbana-Champaign,
3215 Siebel Center, 201 N.Goodwin Avenue,
Urbana, Illinois, USA 62801-2302.

e-mail: annalisa@uiuc.edu

2 Posizione Attuale

- Da Febbraio 2008 è Visiting Researcher presso il *Department of Computer Science*, University of Illinois at Urbana-Champaign.
- Da Dicembre 2005 è titolare di un assegno per la collaborazione ad attività di ricerca presso il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno, per la realizzazione del progetto dal titolo: "Schemi di Assegnamento di Chiavi Crittografiche e Politiche di Controllo degli Accessi", (Responsabile: Prof. A. De Santis), per il periodo 1 Dicembre 2005 - 30 Novembre 2008.

3 Formazione

- Da Febbraio 2007 a Gennaio 2008 è stata Post-Doc presso l'*Information Security Institute and Department of Computer Science* della Johns Hopkins University, Baltimore, MD, USA.
- Dal 28 Ottobre al 3 Novembre 2006 ha partecipato all' *Autumn International School on Zero Knowledge: Foundations and Applications*, tenutasi a Bertinoro, presso il Centro Residenziale dell'Università di Bologna. Docenti: Jonathan Katz (University of Maryland, USA), Yehuda Lindell (Bar-Ilan University, Israele), Giuseppe Persiano (Università di Salerno, Italia).

- Il giorno *11 Aprile 2006* ha conseguito il *Dottorato di Ricerca in Informatica*, presso il Dipartimento di Informatica ed Applicazioni dell'Università degli Studi di Salerno, discutendo una tesi dal titolo: *On Access Control Policies and Key Assignment Schemes*.
- Da *Settembre 2004* a *Maggio 2005* ha svolto attività di ricerca al *Centre for Applied Cryptographic Research*, presso la scuola di Computer Science dell'Università di Waterloo, Ontario, Canada, sotto la supervisione del Prof. Douglas Stinson.
- Dal *2 Febbraio* al *13 Febbraio 2004* ha partecipato all' *Advanced Course on Contemporary Cryptology*, tenutosi a Barcellona. Docenti: Dario Catalano (École Normale Supérieure, Paris), Ivan Damgard (Aarhus Universitet), Giovanni Di Crescenzo (Telcordia Technologies, Inc. Morristown, New Jersey), David Pointcheval (École Normale Supérieure, Paris), Tsuyoshi Takagi (Technische Universität Darmstadt).
- Il *25 Luglio 2002* ha conseguito la Laurea in Informatica presso l'Università degli Studi di Salerno, con votazione pari a 110/110 e lode, discutendo una tesi dal titolo *Assegnamento di Chiavi in una Gerarchia*. Relatore: Prof. Alfredo De Santis.

4 Partecipazione a Progetti Internazionali e Nazionali

Ha fatto parte regolarmente di unità di ricerca i cui progetti sono stati approvati e finanziati. In particolare:

- *European Network of Excellence in Cryptology - ECRYPT*, progetto n. IST-2003-507932.
- Progetto ex 60% - Università di Salerno, anno 2007: *Protocolli Crittografici ed Algoritmi di Compressione*.
- Progetto ex 40% - MURST, anno 2006: *Gestione e protezione di basi di dati crittografate* (coordinatore scientifico: Prof. S. Paraboschi, Università di Bergamo).
- Progetto ex 60% - Università di Salerno, anno 2006: *Sicurezza delle Reti, Animazione di Protocolli Crittografici, e Algoritmi*.
- Progetto ex 60% - Università di Salerno, anno 2005: *Sicurezza, Reti, e Compressione*.
- Progetto ex 60% - Università di Salerno, anno 2004: *Sicurezza Dati, Computazione Distribuita e Compressione Dati*.
- Progetto ex 60% - Università di Salerno, anno 2003: *Sicurezza Dati e Algoritmica*.
- Progetto ex 60% - Università di Salerno, anno 2002: *Sicurezza e Algoritmi in Protocolli di Comunicazione*.

5 Presentazioni a Conferenze Nazionali ed Internazionali

- *32nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2007)*, 27-31 Agosto 2007, Cesky Krumlov, Repubblica Ceca. *Efficient Provably-Secure Hierarchical Key Assignment Schemes.*
- *12th ACM Symposium on Access Control Models and Technologies (SACMAT 2007)*, 20-22 Giugno 2007, Sophia Antipolis, Francia. *New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes.*
- *International Workshop on Coding and Cryptography (WCC 2005)*, 14-18 Marzo 2005, Bergen, Norvegia. *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 Ottobre 2003, University Center Bertinoro, Italia. *An Information-Theoretic Approach to the Access Control Problem.*

6 Attività Didattica

- Da Giugno 2006 ad Ottobre 2006 e da Giugno 2007 ad Ottobre 2007 ha svolto attività di tutorato per l'insegnamento di *Crittografia* del Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche edizione online dell'Università degli Studi di Milano.
- Negli anni accademici 2003-2004, 2004-2005 e 2005-2006 ha svolto cicli di seminari per gli studenti del corso di *Sicurezza su Reti*, del Corso di Laurea in Informatica presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università di Salerno.
- Negli anni accademici 2003-2004, 2004-2005 e 2005-2006 ha svolto attività di cultrice della materia per l'insegnamento di *Sicurezza su Reti* del Corso di Laurea in Informatica presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università di Salerno.

7 Attività di Revisione

Ha svolto e svolge revisioni di lavori per diverse riviste e conferenze internazionali nell'ambito della crittografia e della sicurezza dei dati (*Design, Codes and Cryptography, Theoretical Computer Science, IEEE Transaction on Computers, Information Processing Letters, IEEE Transaction on Knowledge and Data Engineering, Information Sciences, Theoretical Computer Science, CCS 2007, PKC 2007, ICICS 2007, PET 2007, ICALP 2008.*)

8 Attività di Ricerca

Gli interessi principali riguardano Algoritmi, Crittografia e le problematiche inerenti alla Sicurezza dei Dati.

9 Elenco delle Pubblicazioni

Riviste:

- [1] A. De Santis, A. L. Ferrara, e B. Masucci, New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, *Theoretical Computer Science*, accettato per pubblicazione, *Cryptology ePrint Archive*, Report 2006/483.
- [2] A. De Santis, A. L. Ferrara, e B. Masucci, An Attack on a Payment Scheme, *Information Sciences*, Vol. 178 , No. 5, pp. 1418-1421, March 2008.
- [3] A. De Santis, A. L. Ferrara, e B. Masucci, Enforcing the Security of a Time-Bound Hierarchical Key Assignment Scheme, *Information Sciences*, Vol. 176, No. 12, pp. 1684–1694, June 2006.
- [4] A. De Santis, A. L. Ferrara, e B. Masucci, Unconditionally Secure Key Assignment Schemes, *Discrete Applied Mathematics*, Vol. 154, No. 2, pp. 234–252, February 2006.
- [5] S. Cimato, A. De Santis, A. L. Ferrara e B. Masucci, Ideal Contrast Visual Cryptography Schemes with Reversing, *Information Processing Letters*, Vol. 93, No. 4, pp. 199-206, February 2005.
- [6] A. De Santis, A. L. Ferrara, e B. Masucci, Cryptographic Key Assignment Schemes for Any Access Control Policy, *Information Processing Letters*, Vol. 92, No. 4, pp. 199-205, November 2004.
- [7] F. Y. L. Chin, A. De Santis, A. L. Ferrara, N. L. Ho e S. K. Kim, A Simple Algorithm for the Constrained Sequence Problem, *Information Processing Letters*, Vol. 90, No. 4, , pp. 175-179, May 2004.
- [8] C. Blundo, S. Cimato, R. De Prisco e 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.

Conferenze:

- [9] 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.
- [10] 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.
- [11] 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.

- [12] A. De Santis, A. L. Ferrara, e 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.
- [13] A. De Santis, A. L. Ferrara e 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.
- [14] A. L. Ferrara e 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.

Lavori Sottomessi e Technical Reports:

- [15] A. L. Ferrara, M. Green, S. Hohenberger, M. Ø. Pedersen, On the Practicality of Short Signature Batch Verification, sottomesso a conferenza internazionale, Cryptology ePrint Archive, Report 2008/015.
- [16] P. D’Arco, A. De Santis, A. L. Ferrara, and B. Masucci, Variations on a Theme by Akl and Taylor: Security and Tradeoffs, sottomesso a conferenza internazionale.
- [17] A. De Santis, A. L. Ferrara, and B. Masucci, Efficient Provably-Secure Hierarchical Key Assignment Schemes, Cryptology ePrint Archive, Report 2006/479.
- [18] G. Ateniese, A. De Santis, A. L. Ferrara, e B. Masucci, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, Cryptology ePrint Archive, Report 2006/225.