Curriculum Vitae Prof. Dario Catalano

Email: catalano@dmi.unict.it
Tel: 095 7383030
Home page: http://www.ippari.unict.it/~catalano/

Formazione

- Laurea con lode in Scienze dell'Informazione (Università di Catania), 1995.
- Dottorato in Informatica (Università di Catania), 2002.

Esperienze di Lavoro e soggiorni di studio all'estero

- Dal 1 Ottobre 2006 : Professore Associato, Dipartimento di Matematica e Informatica, Università di Catania.
- Dal 1 Ottobre 2003 - 30 settembre 2006: *Chargé de Recherche (titulaire) au CNRS*: Ricercatore confermato presso il CNRS francese. Laboratorio di Affiliazione: **Dipartimento di Informatica, Ecole Normale Supérieure - Parigi**.
- 1 Ottobre 2002 - 30 Settembre 2003: *Chargé de Recherche (stagiaire) au CNRS.* Ricercatore non confermato presso il CNRS (Centro Nazionale di Ricerca Scientifica) francese. Laboratorio di Affiliazione: **Dipartimento di Informatica, Ecole Normale Supérieure - Parigi**.
- Novembre 2001 - Settembre 2002: **Ricercatore Post-Doc, Dipartimento di Informatica, Ecole Normale Superieure - Parigi**.
- *Visiting Scholar* (Studioso in visita). **Dipartimento di Informatica, Columbia University (New York, NY, USA)**. Gennaio 1999 - Novembre 2000
- *Visiting student* (Studente in visita). **IBM T.J. Watson Research Center (Hawtorne NY, USA)**. Gennaio 2001 - Aprile 2001.

Attività didattica.

Ho insegnato diversi corsi tra cui: Crittografia, Sicurezza dei Sistemi Informatici, Teoria dell'Informazione, Algebra lineare e Geometria, Complessità Computazionale.
In qualità di relatore invitato ho partecipato alle seguenti scuole di dottorato internazionali

- *Elliptic Curves Essentials and Cryptography*. Smirne, Turchia; 9-11 Settembre 2003. Invited Lecturer (Relatore invitato) (due lezioni).
- *Advanced Course on Contemporary Cryptography.* Barcellona, Spagna, 2-13 Febbraio 2004. Invited Lecturer (Relatore invitato) (cinque lezioni).

Attività scientifica

Negli ultimi 15 anni la mia attività scientifica si è sviluppata nell'ambito della crittografia.
I miei interessi di ricerca si concentrano principalmente su tematiche di carattere teorico ispirate da esigenze di tipo pratico e su questioni legate alla realizzazione di soluzioni crittografiche efficienti e sicure per soddisfare tali esigenze. Tali tematiche includono, ad esempio, la crittografia basata su password, il voto elettronico e primitive crittografiche con proprietà particolari (quali firme omomorfiche e searchable encryption).
Agli inizi della carriera mi sono interessato a problemi di machine learning.

Attività professionali

- Membro di: International Association for Cryptologic Research (IACR).

- Organizzazione di Conferenze Internazionali
  - Ecrypt Workshop on Provable Security 2004 - Co-organizer.
  - IACR Public Key Cryptography Conference 2011 - Local Arrangements Chair.
  - IACR Theory of Cryptography Conference 2012 - Local Arrangements Chair.

- Comitati di Programma in Conferenze Internazionali (selezione)
  - Security, Privacy and Ethics track of the 15th World Wide Web Conference 2006 (WWW2006)
  - Information Security Conference 2006 (ISC'06)
  - Conference on Security and Cryptography for Networks (SCN) 2006, 2008, 2012.
  - IACR Eurocrypt 2007, 2012, 2014
  - Cryptographers Track RSA Conference (CT RSA) 2008.
  - Applied Cryptography and Network Security (ACNS) 2008, 2009, 2011.
  - Africacrypt 2009, 2011, 2014.
  - IACR Theory of Cryptography Conference (TCC) 2010.
  - IACR Public Key Cryptography Conference (PKC) 2010, 2012.
  - International Conference on Provable Security (ProvSec) 2010, 2011.

Studenti di dottorato supervisionati

1. Dr. Dario Fiore (2007-2010). Attualmente Assistant Research Professor (tenure-track) presso l'IMDEA Software Institute, Madrid, Spagna.
2. Orazio Puglisi (2010-in corso).

Lista di 10 Pubblicazioni Selezionate (in ordine cronologico):

La lista completa dei miei articoli è disponibile alla pagina
http://scholar.google.com/citations?user=Gg7nd14AAAAJ&hl=it&oi=ao

D. Catalano, R. Gennaro and S. Halevi.
Computing inverses over a shared secret modulus.
In Proc. of EUROCRYPT 2000, LNCS vol. 1807 pages 190-206, 2000

D. Catalano, R. Gennaro and N. Howgrave-Graham.
The Bit Security of Paillier's Encryption Scheme and its Applications
In Proc. of EUROCRYPT 2001, LNCS vol. 2045 pages 229-243, 2001

D. Catalano, R. Gennaro, N. Howgrave-Graham and P. Nguyen.
Paillier's Cryptosystem Revisited
In Proc. 8th ACM Conference on Computer and Communication Security (ACM CCS) pages 206-214, 2001

E. Bresson, D. Catalano and D. Pointcheval.
A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and its Applications.
In Proc. of ASIACRYPT 2003, LNCS vol. 2894 pages 37-54, 2003.

A. Juels, D. Catalano and M. Jakobsson.
Coercion-Resistant Electronic Elections.
In Proc. of ACM Workshop on Privacy in the Electronic Society (WPES), pages 61-70, 2005.

M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi.
Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions.
In Proc. of CRYPTO 2005, LNCS 3621, pages 205–222, 2005.

D. Catalano, D. Pointcheval and T. Pornin.
Trapdoor Hard-to-Invert Isomorphisms and their Application to Password-Based Authentication
Journal of Cryptology Vol. 20 (1), pages 115-149, 2007.

D. Catalano, D. Fiore and M. Messina.
Zero Knowledge Sets with short proofs.
In Proc. of EUROCRYPT 2008, LNCS 4965, pages 433-450, 2008.

D. Catalano, D. Fiore and B. Warinschi.
Adaptive Pseudofree Groups and Applications
In Proc. of EUROCRYPT 2011, LNCS 6632, pages 207-223, 2011.

D. Catalano and D. Fiore.
Practical Homomorphic MACs for Arithmetic Circuits
In Proc. of EUROCRYPT 2013, LNCS 7881, pages 336-352, 2013.