

CURRICULUM VITÆ ET STUDIORUM

Paolo D'Arco

SEPTEMBER 7, 2011

1 Short Biography

Paolo D'Arco was born in Salerno (Italy) on July 7th, 1972. He received a Master degree (with honours) in Computer Science, from the University of Salerno, in May 1997. From the same university, in February 2002, he received a PhD in Computer Science, defending a thesis in cryptography. During the PhD program, he attended a few schools for phd students on algorithms and cryptography. In the last year of the program he spent a semester studying abroad at the University of Waterloo, in Ontario, (Canada). He also spent two short-term visits at the University of Catalunya in Barcelona, and at Telcordia Technologies (DIMACS), in New Jersey (United States). From November 2001 to October 2002, he was back at the University of Waterloo, as a post-doctoral fellow at the Centre for Applied Cryptographic Research (CACR), in the Department of Combinatorics and Optimization, under the supervision of professor Douglas Stinson. In 2003 he won a competition for a permanent position at the University of Salerno, where, currently he is assistant professor at the Faculty of Science.

His main research interests are cryptography, algorithms and data security. He has worked on the design and the analysis of unconditionally secure cryptographic primitives and protocols, (e.g., secret sharing schemes, key distribution, distributed oblivious transfer, private information retrieval from a database) and on some computationally secure scheme (e.g., robust and distributed broadcast schemes, anonymous communication schemes). In some papers he has also done some crypto-analysis of new protocols. Regarding to data security, he has mainly worked on techniques for proactive password checking. Currently, he is interested in security and privacy problems in rfid communication systems.

Since 2005 he has joined 20 program committees of international conferences, and he has been three times invited speaker, i.e., at the Smart University (2007), at the Third Pythagorean Conference on Geometry, Combinatorial Design and Cryptology (2003), and at the Summer Meeting of the Canadian Mathematical Society (CMS) (2002). Since December 2008 he is member of the PhD Faculty Board for the Phd program in Computer Science, at the University of Salerno. From 2004 to 2009 he has taught courses in algorithms and data structures, operating systems and network security, for undergraduate programs in Computer Science. He has been tutoring more than 30 students for their end-of-degree exams, and co-tutoring a phd student. Since 2005 he is tutor for the department for the Erasmus student-exchange program. He has led two projects for young researchers (years 2001 and 2002) which received two-year funds, and he has actively participated in national and international research projects (e.g. joint actions Italy-Spain). He has also been involved in two Italian PRIN projects on encrypted databases and user privacy, funded for the periods 2006-2008 and 2008-2010, he has been a member of the network of excellence in cryptography ECRYPT, IST-2002-507932, and he currently is member of the network ECRYPT II, ICT-2007-216646, funded for the period 2008-2012. He has also been member of the local organising committees for the conferences Security in Communication Networks, years 1999, 2002, and 2004, and of the 17th International Symposium on Distributed Computing, in 2003. He has published 40 papers in major international journals and conferences in theoretical computer science, cryptography and data security.

Contents

1	Short Biography	1
2	Personal Data	3
3	Current Position	3
4	Research Interests	3
5	Post-Doctoral Positions	3
6	Education and Short-term Visits	4
7	Languages	4
8	Program Committees	4
9	Invited Lectures	6
10	Teaching Activity	6
11	Projects	7
12	Organizing Activity	8
13	Membership	8
14	Referee for Conferences and Journals	9
15	Publications	9

2 Personal Data

First Name: Paolo
Family Name: D'Arco
Birth Date: July 7, 1972
Birth Place: Salerno (Italy)
Citizenship: Italian

Address

Dipartimento di Informatica ed Applicazioni
Università degli Studi di Salerno
Via Ponte Don Melillo, 1 84084 Fisciano (SA), Italy

Phone: +39 089 969718
Fax: +39 089 969600
E-mail: paodar@dia.unisa.it
URL: <http://www.dia.unisa.it/~paodar>

3 Current Position

Assistant Professor at *Facoltà di Scienze MM. FF. NN.*, Università degli Studi di Salerno, Italy.

4 Research Interests

Cryptography, Algorithms, and Data Security.

5 Post-Doctoral Positions

- Post-Doctoral Fellowship received by the Italian *Centro di Competenza RCOST*, at the Università del Sannio, Italy, for a project in the Information and Communication Technology area. Period: July 2004 - December 2004.
- Post-Doctoral Fellowship received by *Facoltà di Scienze MM. FF. NN.*, at the Dipartimento di Informatica ed Applicazioni of the Università degli Studi di Salerno. Period: October 2002 - June 2004.
- Post-Doctoral Fellowship received by the *Centre for Applied Cryptographic Research* (CACR), at the Department of Combinatorics and Optimization of the University of Waterloo, Ontario, Canada. Advisor: Prof. Douglas R. Stinson. Period: November 2001 - October 2002.

6 Education and Short-term Visits

- On February 2002, PhD in Computer Science (*Dottorato di Ricerca in Informatica*) at the *Università degli Studi di Salerno*, with a Thesis in Cryptography. Title: *Distribution and Obliviousness. The Key Establishment Problem*. Advisor: Prof. Carlo Blundo.
- On May 1997, Master (with Honours) in Computer Science (*Laurea cum laude in Scienze dell'Informazione*) at the *Università degli Studi di Salerno*, with a Thesis (in Italian) in Cryptography. Title: *Crittografia Visuale. Il Contrasto negli Schemi a Soglia* (Visual Cryptography. The Contrast in Threshold Schemes). Advisor: Prof. Alfredo De Santis.
- In November 2000, visiting researcher at the *Departament de Matemàtica i Telemàtica* at the *Universitat Politècnica de Catalunya* (Spain).
- From January 2001 to May 2001, visiting researcher at the *Centre for Applied Cryptographic Research*, in the Department of Combinatorics and Optimization of the University of Waterloo, Ontario, Canada.
- In June 2001, visiting researcher at *DIMACS (Telcordia Technologies)*, New Jersey, USA.
- In May 2011, visiting researcher at the *Mathematical Cryptology Group* at the *Universidad Rey Juan Carlos*, Madrid, (Spain).

7 Languages

Italian (mother tongue) and English (fluent).

8 Program Committees

- Program Committee member of the *International Conference on Information Security and Cryptology (ICISC 2011)*, November 30 - December 2, 2011, Seoul, Korea.
- Program Committee member of the *International Conference on Computer Convergence Technology (ICCCT 2011)*, October 20 – 22, 2011, Seoul, Korea.
- Program Committee member of the *2nd International Conference on Security-enriched Urban Computing and Smart Grids (SUCOMS 2011)*, September 21 – 23, 2011, Hualien, Taiwan.
- Program Committee member of the *8th European Workshop on PKI, Services and Applications (EUROPKI 2011)*, September 15 – 16, 2011, Leuven, Belgium.

- Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2011), July 16 – 18, 2011, Seville, Spain.
- Program Committee member of the *5-th International Conference on Information Theoretic Security* (ICITS 2011), May 21 – 24, 2011, Amsterdam, Holland.
- Program Committee member of the *14th International Conference on Practice and Theory in Public Key Cryptography* (PKC 2011), March 6 – 9, 2011, Taormina, Italy.
- Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2010), December 1 – 3, 2010, Seoul, Korea.
- Program Committee member of the *International Conference on Security Technology* (SecTech 2010), November 11 – 13, 2010, Bali, Indonesia.
- Program Committee member of the *First International Conference on Security-enriched Urban Computing and Smart Grid* (SUCOMS 2010), September 15 – 17, 2010, Daejeon, Korea.
- Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2010), July 26 – 28, 2009, Athens, Greece.
- Program Committee member of the *The 4th International Conference on Information Security and Assurance* (ISA 2010), June 23 – 25, 2010, Miyazaki, Japan.
- Program Committee member of the *International Conference on Security Technology* (SecTech 2009), December 10 – 12, 2009, Jeju Island, Korea.
- Program Committee member of the *International Conference on Information Theoretic Security* (ICITS 2009), December 2 – 5, 2009, Shizuoka, Japan.
- Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2009), December 2 – 4, 2009, Seoul, Korea.
- Program Committee member of the *International Conference on Information Security and Cryptology* (ISCISC 2009), October 7 – 8, 2009, Isfahan, Iran.
- Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2009), July 7 – 10, 2009, Milan, Italy.
- Program Committee member of the *International Workshop on Computer Graphics, Multimedia and Security* (CGMS-09), June 25 – 27, 2009, Korea University, Seoul, Korea.
- Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2008), December 3 – 5, 2008, Seoul, Korea.
- Program Committee member of the *International Conference on Information Theoretic Security* (ICITS 2008), August 10 – 13, 2008, Calgary, Canada.

- Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2007), November 29 – 30, 2007, Seoul, Korea.
- Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2007), July 28 – 31, 2007, Barcelona, Spain.
- Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2006), August 7-10, 2006, Setubal, Portugal.
- Program Committee member of the *6-th Workshop on Information Security Applications* (WISA 2005), August 22-24, 2005, Jeju Island, Korea.

9 Invited Lectures

1. *Invited Speaker* at the Smart University, track *Digital Rights Management, From Research to Implementations*, September 17-20, 2007, Sophia Antipolis, French Riviera. Title fo the Lecture: *After the Gutman report: Perspectives of OS-level support for DRMs*.
2. *Invited Speaker* at the Third Pythagorean Conference on Geometry, Combinatorial Design and Cryptology, Rhodes, Greece, June 1-7, 2003. Title of the Lecture: *Key Distribution with Key-Recovery Techniques over Unreliable Networks*.
3. *Invited Speaker* at the Summer Meeting of the Canadian Mathematical Society (CMS), University of Laval, Quebec City, Quebec, Canada, June 15-17, 2002. Title of the Lecture: *Distributed Oblivious Transfer and Applications to Cryptography*.

10 Teaching Activity

- *Unix Network Programming*, undergraduate, 2009-2010, University of Salerno.
- *Network Security Complements*, undergraduate, 2006-2007, 2007-2008, 2008-2009, 2009-2010, University of Salerno.
- *Operating System*, undergraduate, 2005-2006, 2006-2007, 2007-2008, 2008-2009, University of Salerno.
- *Algorithms and Data Structures I*, undergraduate, 2004-2005, University of Salerno.

11 Projects

1. Coordinator of the Italian Project *Sistemi per il controllo proattivo di password* (Proactive Password Checking Systems). The project received a two-year grant in June 2001 from the *Ministero della Università e della Ricerca Scientifica* (Italian Ministry of University and Scientific Research).
2. Coordinator of the Italian Project *Oblivious Transfer e Applicazioni al Commercio Elettronico* (Oblivious Transfer and Applications to e-Commerce). The project received a two-year grant in June 2002 from the *Ministero della Università e della Ricerca Scientifica* (Italian Ministry of University and Scientific Research). .
3. Member of Progetto ex 60% - Università di Salerno, anno 1998. Title: *Algoritmi: Progetto, Analisi e Sintesi*.
4. Member of Progetto ex 60% - Università di Salerno, anno 1999. Title: *Algoritmi: Animazione, Compressione e Sicurezza con Applicazioni su Internet*.
5. Member of Progetto ex 60% - Università di Salerno, anno 2000. Title: *Sicurezza, Codici e Compressione: Progetto, Analisi e Realizzazione*.
6. Member of the Joint Action Italy–Spain - MIUR, anno 2000. Title: *Schemi per la Distribuzione di Chiavi Crittografiche*.
7. Member of Progetto Giovani Ricercatori CNR Agenzia 2000: Title: *Pubblicità Online: Nuove Misure per Nuovi Media. Auditing ed Accounting Sicuro sul Web*.
8. Member of Progetto ex 60% - Università di Salerno, anno 2001. Title: *Computazione, Comunicazione e Sicurezza in Reti di Calcolatori*.
9. Member of Progetto ex 40% - MURST, anno 2001: *MEFISTO: Metodi Formali per la Sicurezza* (coordinatore scientifico: Prof. R. Gorrieri, Università di Bologna).
10. Member of Progetto ex 60% - Università di Salerno, anno 2002. Title: *Sicurezza e Algoritmi in Protocolli di Comunicazione*.
11. Member of Progetto ex 60% - Università di Salerno, anno 2003. Title: *Sicurezza Dati e Algoritmica*.
12. Member of the *European Network of Excellence in Cryptology - ECRYPT*, IST-2002-507932.
13. Member of Progetto ex 60% - Università di Salerno, anno 2004. Title: *Sicurezza Dati, Computazione Distribuita e Compressione Dati*.
14. Member of Progetto ex 60% - Università di Salerno, anno 2005. Title: *Sicurezza, Reti, e Compressione*.
15. Member of Progetto ex 60% - Università di Salerno, anno 2006: Title: *Sicurezza delle reti, animazione di protocolli crittografici e algoritmi* .

16. Member of Progetto PRIN: Università di Bergamo, Università di Milano e Università di Salerno, 2006-2008. Title: *Progettazione, analisi ed implementazione di protocolli crittografici per la protezione dei dati sensibili e la gestione dei privilegi per il controllo degli accessi in basi di dati distribuite*.
17. Member of Progetto ex 60% - Università di Salerno, anno 2007. Title: *Protocolli crittografici e algoritmi di compressione*.
18. Member of the *European Network of Excellence in Cryptology - ECRYPT II*, ICT-2007-216646.
19. Member of Progetto ex 60% - Università di Salerno, anno 2008. Title: *Sicurezza, privacy e compressione in documenti multimediali e tecnologia Rfid*.
20. Member of Progetto PRIN: Università di Bergamo, Università di Milano e Università di Salerno, 2008-2010. Title: *Progettazione ed analisi di protocolli crittografici per la tutela della privacy personale e dei dati in basi di dati e dispositivi mobili*.

12 Organizing Activity

1. Member of the local organizing committee for the conference *SCN 10, Security and Cryptography for Networks*, Amalfi (SA), September 13–15, 2010.
2. Member of the local organizing committee for the conference *SCN 04, Security in Communication Networks*, Amalfi (SA), September 8–10, 2004.
3. Member of the local organizing committee for the conference *DISC 2003, 17th International Symposium on Distributed Computing*, Sorrento (NA), Ottobre 1–3, 2003.
4. Member of the local organizing committee for the conference *SCN 02, Security in Communication Networks*, Amalfi (SA), September 12–13, 2002.
5. Member of the local organizing committee for the conference *SCN 99, Security in Communication Networks*, Amalfi (SA), September 16–17, 1999.

13 Membership

- IACR (International Association for Cryptologic Research)
- EATCS (European Association for Theoretical Computer Science)

14 Referee for Conferences and Journals

- Journals for which papers have been reviewed: Theoretical Computer Science, ACM Transactions on Information and System Security, ACM Transactions on Dependable and Secure Computing, Siam Journal on Discrete Mathematics, IEEE Transactions on Information Theory, IEEE Transactions on Signal Processing, IEEE Transactions on Circuits and Systems, Journal of Theoretical Informatics and Applications, Information and Computation, Journal of Mathematical Cryptology, Journal of Systems and Software, Information Processing Letters, Design, Codes and Cryptography, Australasian Journal of Combinatorics, Journal of Network Security.
- Conferences for which papers have been reviewed: SAC 2011, DISC 2011, ESORICS 2011, ASIACRYPT 2010, PKC 2010, ESORICS 2010, ICALP 2010, ASIACRYPT 2009, PKC 2009, ASIACRYPT 2008, DISC 2008, ASIACCS 2008, ICISC 2007, ICICS 2006, PKC 2006, SPA 2005, ICALP 2005, SIROCCO 2005, STACS 2005, WMAN 2005, SAC 2004, DISC 2003, DNS 2003, PODC 2003, Asiacypt 2003, Esorics 2002, SAC02, SCN02, IEEE ISIT2002, Crypto 2001, Eurocrypt 2001, IEEE ISIT2000, CIAC 2000, SCN99, Eurocrypt 1999.
- From January 2005 external reviewer for the *Research Grants Council* (RGC) of Hong Kong city.

15 Publications

Journals:

- P. D'Arco and A. De Santis.
On Ultra-Lightweight RFID Authentication Protocols.
IEEE Transactions on Dependable and Secure Computing, Vol. 8, N. 4, pp. 548-563, 2011.
- 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, N. 441, pp. 213–227, 2010.
- C. Blundo, P. D'Arco, A. De Santis, and D. Stinson.
On Unconditionally Secure Distributed Oblivious Transfer.
Journal of Cryptology, Vol 20, N. 3, pp. 323-375, 2007.
- C. Blundo, P. D'Arco, and A. De Santis.
On Self-healing Key Distribution Schemes.
IEEE Transactions on Information Theory, Vol. 52, N. 12, pp., 5455-5468, 2006.
- A. Ciaramella, P. D'Arco, A. De Santis, C. Galdi, and R. Tagliaferri.
Neural Network Techniques for Proactive Password Checking.
IEEE Transactions on Dependable and Secure Computing, Vol. 3, N. 4, pp. 219-233, 2006.

- S. Cimato, A. Cresti, e P. D'Arco.
A Unified Model for Unconditionally Secure Key Distribution.
Journal of Computer Security, Vol. 14, n.1, pp. 45–64, 2006.
- P. D'Arco, W. Kishimoto, and D. Stinson.
Properties and Constraints of Cheating-Immune Secret Sharing Scheme.
Discrete Applied Mathematics, Vol. 154, pp. 219–233, 2006.
- P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev.
Security of Public Key Cryptosystems based on Chebyshev Polynomials.
IEEE Transactions on Circuits and Systems I, Vol. 52, N. 7, pp. 1382–1393, 2005.
- C. Blundo and P. D'Arco.
Analysis and Design of Distributed Key Distribution Centers.
Journal of Cryptology, Vol. 18, N. 4, pp. , 391–414, 2005.
- C. Blundo, P. D'Arco V. Daza and C. Padrò.
Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures.
Theoretical Computer Science, Vol. 320, pp. 269–291, 2004.
- C. Blundo, P. D'Arco, A. De Santis, and M. Listo.
Design of Self-healing Key Distribution Schemes.
Design, Codes, and Cryptography, Vol. 32, pp. 15–44, 2004
- C. Blundo, P. D'Arco, A. De Santis and C. Galdi.
Hippocrates: A New Proactive Password Checker.
Journal of Systems and Software, Vol. 71, pp. 163–175, 2004.
- C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson.
Contrast Optimal Threshold Visual Cryptography Schemes.
SIAM Journal on Discrete Mathematics, Vol. 16, Issue 2, pp. 224–261, 2003.
- C. Blundo, P. D'Arco and C. Padrò.
A Ramp Model for Distributed Key Distribution Schemes.
Discrete Applied Mathematics, Vol. 128, pp. 47–64, 2003.
- C. Blundo, P. D'Arco and A. De Santis.
A t -Private k -Database Information Retrieval Scheme.
International Journal of Information Security (IJIS), Vol. 1, Issue 1, pp. 64–68, 2001.
- C. Blundo, P. D'Arco and A. Giorgio Gaggia.
A τ -Restricted Key Agreement Scheme.
The Computer Journal, Vol. 42, Issue 1, pp. 51–61, 1999.

Conferences:

- P. D'Arco and Angel L. Perez del Pozo
Fighting Pirates 2.0.
Proceedings of the 9th International Conference on Applied Cryptography and Network Security (ACNS 2011). Lecture Notes in Computer Science, Vol. 6715, pp. 359-376, Springer Verlag, 2011.
- P. D'Arco
An Almost-Optimal Forward-Private Rfid Mutual Authentication Protocol with Tag Control.
Proceedings of the 5th Workshop in Information Security Theory and Practise (WISTP 2011), Lecture Notes in Computer Science, Vol. 6633, pp. 69-84, Springer Verlag, 2011.
- P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci.
Security and Tradeoffs of the Akl-Taylor Scheme and its Variants.
Proc. of the 34th International Symposium on Mathematical Foundations of Computer Science (MFCS 2009). Lecture Notes in Computer Science, Vol. 5734, pp. 247-257, Springer Verlag, 2009.
- P. D'Arco, A. Scafuro and I. Visconti.
Semi-Destructive Privacy in RFID Systems.
Proc. of the 5-th Workshop on RFID Security (RFIDSec '09).
- P. D'Arco, A. Scafuro and I. Visconti.
Revisiting DoS Attacks and Privacy in RFID-Enabled Networks.
Proc. of the 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS '09). Lecture Notes in Computer Science, Vol.5304, pp. 76-87, 2009.
- P. D'Arco and A. De Santis.
Weaknesses in a Recent Ultra-lightweight RFID Authentication Protocol.
Progress in Cryptology - AfricaCrypt 2008, Lecture Notes in Computer Science, Vol. 5023, pp. 27-39, 2008.
- P. D'Arco and A. De Santis.
Optimising SD and LSD in presence of non-uniform probabilities of revocation.
Proc. of the 1st International Conference on Information Theoretic Security (IC-ITS07) Lecture Notes in Computer Science, Vol. 4883, pp. 46-64, 2009.
- C. Blundo, P. D'Arco, and A. De Santis.
Definitions and Bounds for Self-healing Key Distribution.
Proc. of the 31st International Colloquium on Automata, Languages, and Programming (ICALP 2004). Lecture Notes in Computer Science, Vol. 3142, pp. 234-246, Springer-Verlag, 2004.
- S. Cimato, P. D'Arco, and I. Visconti.
Anonymous Group Communication for Mobile Networks.
Proc. of the Italian Conference on Theoretical Computer Science (ICTCS 2003). Lecture Notes in Computer Science, Vol. 2814, pp. 316-328, Springer-Verlag, 2003.

- C. Blundo, P. D'Arco, and M. Listo.
A New Self-healing Key Distribution Scheme.
Proc. of IEEE Symposium on Computers and Communications (ISCC 2003), Vol. 1, pp. 803-808, 2003.
- P. D'Arco and D. Stinson.
Fault Tolerant and Distributed Broadcast Encryption.
Proc. of the Cryptographers' Track RSA Conference 2003 (CT-RSA 2003). Lecture Notes in Computer Science, Vol. 2612, pp. 262-279, Springer Verlag, 2003.
- C. Blundo, P. D'Arco and M. Listo.
A Flaw in a Self-Healing Key Distribution Scheme.
Proc. of the 2003 IEEE Information Theory Workshop (ITW '03), Vol. 1, pp. 163-166, 2003.
- P. D'Arco, W. Kishimoto, and D. Stinson.
On Cheating-Immune Secret Sharing.
Proceedings of the International Workshop on Coding and Cryptography (WCC 2003), pp. 111-120, 2003.
- P. D'Arco and D. Stinson.
On Unconditionally Secure Distributed Key Distribution Centers.
Proc. of ASIACRYPT 2002. Lecture Notes in Computer Science, Vol. 2501, pp. 346-363, Springer Verlag, 2002.
- C. Blundo, P. D'Arco, A. De Santis and D. Stinson.
New Results on Unconditionally Secure Distributed Oblivious Transfer.
Proc. of *Selected Areas in Cryptography* (SAC 2002). Lecture Notes in Computer Science, Vol. 2595, pp. 291-309, Springer Verlag, 2003.
- C. Blundo, P. D'Arco, A. De Santis and C. Galdi.
A Novel Approach to Proactive Password Checking.
Proc. of the *Infrastructure Security Conference* (INFRASEC 2002). Lecture Notes in Computer Science, Vol. 2437, pp.30–39, Springer Verlag, 2002.
- P. D'Arco and D. Stinson.
Generalized Zig-zag Functions and Oblivious Transfer Reductions.
Proc. of *Selected Areas in Cryptography* (SAC2001). Lecture Notes in Computer Science, Vol. 2259, pp. 87-102, Springer Verlag, 2002.
- C. Blundo, P. D'Arco and C. Padrò.
A Ramp Model for Distributed Key Distribution Schemes.
Proc. of the *International Workshop on Coding and Cryptography (WCC2001)*, pp. 93-102, 2001.
- C. Blundo, P. D'Arco, A. De Santis and C. Galdi.
Hyppocrates: A New Proactive Password Checker.
Proc. of the Information Security Conference (ISC 2001). Lecture Notes in Computer Science, vol. 2200, pp. 63-80, Springer Verlag, 2001.

- P. D'Arco.
On the Distribution of a Key Distribution Center.
Proc. of the Italian Conference on Theoretical Computer Science (ICTCS 2001).
Lecture Notes in Computer Science, Vol. 2202, pp. 357-369, Springer Verlag, 2001.
- C. Blundo, P. D'Arco V. Daza and C. Padrò.
Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures.
Proc. of the Information Security Conference (ISC 2001). Lecture Notes in Computer Science, Vol. 2200, pp. 1-17 , Springer Verlag, 2001.
- C. Blundo and P. D'Arco.
An Information Theoretic Model for Distributed Key Distribution.
Proc. of the IEEE International Symposium on Information Theory (ISIT2000),
p. 267, 2000.

Tutorial

- C. Blundo and P. D'Arco.
The Key Establishment Problem.
Lecture Notes in Computer Science (Tutorial), Vol. 2946, pp. 44 – 90, Springer-Verlag, 2004.

Date:
September 7, 2011.

Signature