Curriculum Vitæ et Studiorum

Paolo D'Arco

May 2nd, 2023

1 Short Biography

Paolo D'Arco was born in Salerno (Italy), on July 7, 1972. He received a Master degree, with honors, in Computer Science in May 1997, and a PhD in Computer Science in February 2002, both from the University of Salerno. During the PhD program, he attended a few schools for PhD students on algorithms and cryptography: he was a visiting researcher for a semester at the University of Waterloo, in Ontario (Canada). He also had two short-term visits at the University of Catalunya (Spain), and at Telcordia Technologies - DIMACS- (USA). From November 2001 to October 2002, he was a post-doctoral fellow at the Centre for Applied Cryptographic Research (CACR), in the Department of Combinatorics and Optimization (University of Waterloo), under the supervision of professor Douglas Stinson. In the Computer Science department at the University of Salerno, from 2005 to 2015 he was an assistant professor, from 2015 to 2021 an associate professor, and since 2021 he is a full professor in computer science.

His main research interests are in cryptography. He has worked on the design and the analysis of cryptographic primitives and protocols. A few topics of attention have been secret sharing, key distribution, authentication, anonymous communication, oblivious transfer, private information retrieval, visual cryptography, robust and distributed broadcast and multicast communication. He has also done some cryptanalysis of lightweight and ultralightweight protocols. Currently, he is interested in secure multi-party computation, in blockchain technologies, and in post-quantum techniques.

Since 2005 he has joined 59 program committees of international conferences, and he has been a keynote speaker at SecITC (2018), at SecITC (2016), and an invited speaker at Stinson66 (2022), 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 in the PhD Faculty Board for the PhD program in Computer Science, at the University of Salerno. From 2004 he has taught classes in algorithms and data structures, operating systems, network and network security, and cryptography for undergraduate and graduate programs in Computer Science. He has been tutoring more than 60 students for their end-of-degree exams. 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 three Italian PRIN projects on encrypted databases, user privacy and genomic computing, funded for the periods 2006-2008, 2008-2010, and 2012-2014, respectively. He has been a member of the network of excellence in cryptography ECRYPT, IST-2002-507932, and of the network ECRYPT II, ICT-2007-216646, funded for the periods 2004-2008 and 2008-2012, respectively. From 2014 to 2018 he was the national coordinator for Italy of the COST Action IC1403 on Cryptanalysis of ubiquitous computing systems (CRYPTACUS). He has also been a member of the local organizing committees for the SCN conferences, in 1999, 2002, 2004, 2010, 2012 and 2014, 2016, and 2018, and for DISC, in 2003. He has published more than sixty papers in well-reputed international journals and in the proceedings of conferences on theoretical computer science, cryptography and data security.

Contents

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
Università degli Studi di Salerno
Via Giovanni Paolo II, 132
84084 Fisciano (SA)

Phone: +39 089 969718
Fax: +39 089 969600
E-mail: pdarco@unisa.it
URL: http://www.di-srv.unisa.it/professori/paodar

3 Current Position

Full Professor at *Dipartimento di Informatica*, University of Salerno, Italy.

4 Research Interests

Cryptography, algorithms, and data security.

5 Previous Positions

- Associate professor at *Dipartimento di Informatica*, Università degli Studi di Salerno, Italy. Period: March 2015 - Dicember 2021.
- Assistant professor at *Dipartimento di Informatica*, Università degli Studi di Salerno, Italy. Period: January 2005 - February 2015.
- 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

- From 2011 to 2015, every year, visiting researcher at the *Mathematical Cryptology Group* at the Universidad Rey Juan Carlos, Madrid, Spain.
- In October 2006 participant at the *Autumn International School on Zero Knowledge: Foundations and Applications*, Bertinoro, Bologna, Italy.
- 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.
- 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 Tecnologies)*, New Jersey, USA.
- In November 2000, visiting researcher at the *Departament de Matemàtica i Telemàtica* at the Universitat Politècnica de Catalunya, Barcelona, Spain.
- In July 2000, participant at the *12th International School for Computer Science Researchers on E-commerce and On-line Algorithms*, Lipari, Italy, 2000. Lectures given by: S. Micali, M. Bellare, T. Rabin, M. Yung, A. Borodin, A. Blum e J. Kleinberg.
- In June 1999, participant at the *5th International Summer School on Distributed Computing: Advanced Distributed Computing*, Siena, Italy. Lectures given by: S. Dolev, C. Dwork, D. Peleg e N. Santoro
- In July 1998 participant at the *10th International School for Computer Science Researchers on Distributed Systems and Security*, Lipari, Italy. Lectures given by: A. Shamir, A. De Santis, S. Micali, P. Rogaway, R. Gennaro, M. Herlihy, L. Shrira e Y. Afek.
- On May 1997, Master (with Honors) 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.

7 Languages

Italian (mother tongue) and English (fluent).

8 Editorial Boards

1. Editorial board member for the *Special Issue on Security and Privacy in Complex Systems*, IEEE Systems Journal, period: 10/2011 – 10/2012.
2. Editorial board member for the journal *Security and Communication Networks*, Wiley-Hindawi, from August 2016 to November 2020.
3. Editorial board member for the *Journal of Mathematical Cryptology*, De Gruyter, since August 2020.

9 Program Committees

1. Program Committee member of the *16th International Conference on Information Technology and Communications Security*, (SecITC 2023), November 23-24, Bucharest, Romania, 2023.
2. Program Committee member of the *The 5th IEEE International Conference on Decentralized Applications and Infrastructures* (IEEE DAPPS 2023), July 17-20, Athens, Greece, 2023.
3. Program Committee member of the *The 38th International Conference on ICT Systems, Security and Privacy Protection* (IFIP SEC 2023) June 14-16, Poznan, Poland, 2023.
4. Program Committee member of the *4th IEEE International Conference on Decentralized Applications and Infrastructures* (IEEE DAPPS 2022), August 15-18, Bay Area, CA, United States, 2022.
5. Program Committee member of the *4th IEEE International Conference on Cyber Security and Resilience* (IEEE CSR 2022), July 27-29, Virtual Conference, 2022.
6. Program Committee member of the *37th International Conference on ICT Systems Security and Privacy Protection*, (IFIP SEC 2022), June 13-15, Copenaghen, Denmark, 2022.
7. Program Committee member of the *36th International Conference on ICT Systems Security and Privacy Protection*, (IFIP SEC 2021), June 22-24, Oslo, Norway, 2021.
8. Program Committee member of the *2021 IEEE International Conference on Cyber-Security and Resilience*, (IEEE CSR 2021), March 22-24, Rodhes, Greece, 2021.
9. Program Committee member of the *23th International Conference on Information Security and Cryptology* (ICISC 2020), December 4-5, 2020, Seoul, Korea.

10. Program Committee member of the *13th International Conference on Information Technology and Communications Security*, (SecITC 2020), November 19-20, Bucharest, Romania, 2020.

11. Program Committee member of the *35th International Information Security and Privacy Conference*, (IFIP SEC 2020), May 26-28, Maribor, Slovenia, 2020.

12. Program Committee member of the *12th International Conference on Information Technology and Communications Security*, (SecITC 2019), November 14-15, Bucharest, Romania, 2019.

13. Program Committee member of the *22th International Conference on Information Security and Cryptology* (ICISC 2019), December 4-5, 2020, Seoul, Korea.

14. Program Committee member of the *11th International Conference on Information Technology and Communications Security*, (SecITC 2018), November 8-9, Bucharest, Romania, 2018.

15. Program Committee member of the *33rd IFIP TC-11 SEC 2018 International Conference on Information Security and Privacy Protection* (SEC 2018) September 18-20, Poznan, Poland, 2018.

16. Program Committee member of the *20th International Conference on Information Security and Cryptology* (ICISC 2017), November 29 - December 1, 2017, Seoul, Korea.

17. Program Committee member of the *10th International Conference on Information Theoretic Security* (ICITS 2017), November 29 - December 2, 2017, Hong Kong.

18. Program Committee member of the *7th iCatse International Conference on IT Convergence and Security*, (ICITCS 2017), September 25-28, Seoul, Republic of Korea, 2017.

19. Program Committee member of the *10th International Conference on Information Technology and Communications Security*, (SecITC 2017), June 8-9, Bucharest, Romania, 2017.

20. Program Committee member of the *19th International Conference on Information Security and Cryptology* (ICISC 2016), November 30 - December 2, Seoul, Korea.

21. Program Committee member of the *19th Information Security Conference* (ISC 2016), September 7-9, 2016, Honolulu, HI, USA.

22. Program Committee member of the *9th International Conference on Information Security* (ICITS 2016), August 9-12, 2016, Tacoma, Washington, USA.

23. Program Committee member of the *9th International Conference on Information Technology and Communications Security* (secITC 2016), June 9-10, 2016, Bucharest, Romania.

24. Program Committee member of the *18th International Conference on Information Security and Cryptology* (ICISC 2015), November 25-27, 2015, Seoul, Korea.

25. Program Committee member of the *18th Information Security Conference* (ISC 2015), September 9-11, 2015, Trondheim, Norway

26. Program Committee member of the *8th International Conference on Information Security* (ICITS 2015), May 2-5, 2015, Lugano, Switzerland.

27. Program Committee member of the *17th International Conference on Information Security and Cryptology* (ICISC 2014), December 3-5, 2014, Seoul, Korea.

28. Program Committee member of the *1st International Conference on Cryptography and Information security* (BalkanCryptSec 2014), October 16-17, 2014, Istanbul, Turkey.

29. Program Committee member of the *Twelfth annual Conference on Privacy, Security and Trust* (PST 2014), July 23 - 24, 2014, Toronto, Canada.

30. Program Committee member of the *2nd International Conference on Intelligent Information System and Technology* (ICIIST 2014), June 26 - 28, 2014, Tsingdao, China.

31. Program Committee member of the *16th International Conference on Information Security and Cryptology* (ICISC 2013), November 27 - 29, 2013, Seoul, Korea.

32. Program Committee member of the *10th European Workshop: Research and Applications* (EUROPKI 2013), September 12-13, 2013, Rhul, Egham, UK.

33. Program Committee member of the *International Conference on Intelligence Fusion* (ICIF 2013), June 27-29, 2013, Jeju Island, Korea.

34. Program Committee member of the *9th Workshop on Rfid Security* (RFIDSEC 2013), July 9-11, 2013, Graz, Austria.

35. Program Committee member of the *15th International Conference on Information Security and Cryptology* (ICISC 2012), November 28-30, 2012, Seoul, Corea.

36. Program Committee member of the *9th European Workshop on PKI: Research and Applications* (EUROPKI 2012), September 13-14, 2012, Pisa, Italia

37. Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2011), November 30 - December 2, 2011, Seoul, Korea.

38. Program Committee member of the *International Conference on Computer Convergence Technology* (ICCCT 2011), October $20 - 22$, 2011, Seoul, Korea.

39. Program Committee member of the *2nd International Conference on Security-enriched Urban Computing and Smart Grids* (SUCOMS 2011), September $21 - 23$, 2011, Hualien, Taiwan.

40. Program Committee member of the *8th European Workshop on PKI, Services and Applications* (EUROPKI 2011), September $15 - 16$, 2011, Leuven, Belgium.

41. Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2011), July 16 – 18, 2011, Seville, Spain.

42. Program Committee member of the *5-th International Conference on Information Theoretic Security* (ICITS 2011), May 21 – 24, 2011, Amsterdam, Holland.

43. Program Committee member of the *14th International Conference on Practice and Theory in Public Key Cryptography* (PKC 2011), March 6 – 9, 2011, Taormina, Italy.

44. Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2010), December 1 – 3, 2010, Seoul, Korea.

45. Program Committee member of the *International Conference on Security Technology* (SecTech 2010), November 11 – 13, 2010, Bali, Indonesia.

46. Program Committee member of the *First International Conference on Security-enriched Urban Computing and Smart Grid* (SUCOMS 2010), September 15 – 17, 2010, Daejeon, Korea.

47. Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2010), July 26 – 28, 2009, Athens, Greece.

48. Program Committee member of the *The 4th International Conference on Information Security and Assurance* (ISA 2010), June 23 – 25, 2010, Miyazaki, Japan.

49. Program Committee member of the *International Conference on Security Technology* (SecTech 2009), December 10 – 12, 2009, Jeju Island, Korea.

50. Program Committee member of the *International Conference on Information Theoretic Security* (ICITS 2009), December 2 – 5, 2009, Shizuoka, Japan.

51. Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2009), December 2 – 4, 2009, Seoul, Korea

52. Program Committee member of the *International Conference on Information Security and Cryptology* (ISCISC 2009), October 7 – 8, 2009, Isfahan, Iran.

53. Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2009), July 7 – 10, 2009, Milan, Italy.

54. Program Committee member of the *International Workshop on Computer Graphics, Multimedia and Security* (CGMS-09), June 25 – 27, 2009, Korea University, Seoul, Korea.

55. Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2008), December 3 – 5, 2008, Seoul, Korea

56. Program Committee member of the *International Conference on Information Theoretic Security* (ICITS 2008), August 10 – 13, 2008, Calgary, Canada.

57. Program Committee member of the *International Conference on Information Security and Cryptology* (ICISC 2007), November 29 – 30, 2007, Seoul, Korea.

58. Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2007), July 28 – 31, 2007, Barcelona, Spain.

59. Program Committee member of the *International Conference on Security and Cryptography* (SECRYPT 2006), August 7-10, 2006, Setubal, Portugal.

60. Program Committee member of the 6-*th Workshop on Information Security Applications* (WISA 2005), August 22-24, 2005, Jeju Island, Korea.

10 Invited Lectures

1. *Invited Speaker* at Stinson66 - New Advances in Designs, Codes and Cryptography June 13 - 17, 2022, The Fields Institute, Toronto, Canada. Title of the Lecture: *Private computations on set intersection.*

2. *Keynote Speaker* at the 11th International Conference on Information Technology and Communications Security (secITC 2018), Nov 8-10, 2018, Bucharest, Romania. Title of the Lecture: *Ultralightweight authentication protocols: a ten-year perspective.*

3. *Keynote Speaker* at the 9th International Conference on Information Technology and Communications Security (secITC 2016), June 9-10, 2016, Bucharest, Romania. Title of the Lecture: *Visual Cryptography: Models, Issues, Applications and New Directions.*

4. *Invited Speaker* at the Smart University, track *Digital Rights Management, From Research to Implementations*, September 17-20, 2007, Sophia Antipolis, French Riviera. Title of the Lecture: *After the Gutman report: Perspectives of OS-level support for DRMs.*

5. *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.*

6. *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.*

11 Teaching Activity

- *Cryptography*, graduate, 2022-2023, 2021-2022, 2020-2021, 2019-2020, 2018-2019, 2017-2018, 2016-2017, 2015-2016, University of Salerno.

- *Introduction to C Programming*, undergraduate, 2022-2023, 2021-2022, 2020-2021, 2019-2020, 2018-2019, 2017-2018, 2016-2017, University of Salerno.
- *Introduction to algorithms and data structures*, undergraduate, 2014-2015, 2015-2016, University of Salerno.
- *Unix Network Programming*, undergraduate, 2009-2010, 2011-2012, 2012-2013, 2013-2014, 2014-2015, University of Salerno.
- *Network Security Complements*, undergraduate, 2006-2007, 2007-2008, 2008-2009, 2009-2010, 2011-2012, 2012-2013, 2013-2014, University of Salerno.
- *Operating System*, undergraduate, 2005-2006, 2006-2007, 2007-2008, 2008-2009, University of Salerno.
- *Algorithms*, undergraduate, 2004-2005, University of Salerno.

12 International Project Coordination

1. National coordinator for Italy (management committee member) of the ICT COST Action IC1403 *Cryptanalysis of ubiquitous computing systems* (CRYPTACUS). Project chair: Prof. Gildas Avoine (University of Leuven). The ICT Action started in July 2014, and ended in December 2018. In the project were involved 30 countries. The total budget allocated was of 541,000 euro. Every year two international board meetings were held in a different country. Overall, 43 papers were published with the findings of the research efforts from the working groups. The most visible outcome of Cryptacus is the open-access book published by Springer (https://www.springer.com/us/book/9783030105907). I am a co-author of the first chapter. More details can be found at: *https://www.cost.eu/actions/IC1403/*

13 National Project Coordination

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). .

14 Participation to International and National Projects

1. Member of Progetto ex 60% - Università di Salerno, anno 1998. Title: *Algoritmi: Progetto, Analisi e Sintesi.*

2. Member of Progetto ex 60% - Università di Salerno, anno 1999. Title: *Algoritmi: Animazione, Compressione e Sicurezza con Applicazioni su Internet.*

3. Member of Progetto ex 60% - Università di Salerno, anno 2000. Title: *Sicurezza, Codici e Compressione: Progetto, Analisi e Realizzazione.*

4. Member of the Joint Action Italy–Spain - MIUR, anno 2000. Title: *Schemi per la Distribuzione di Chiavi Crittografiche.*

5. Member of Progetto Giovani Ricercatori CNR Agenzia 2000: Title: *Pubblicità Online: Nuove Misure per Nuovi Media. Auditing ed Accounting Sicuro sul Web.*

6. Member of Progetto ex 60% - Università di Salerno, anno 2001. Title: *Computazione, Comunicazione e Sicurezza in Reti di Calcolatori.*

7. Member of Progetto ex 40% - MURST, anno 2001: *MEFISTO: Metodi Formali per la Sicurezza* (coordinatore scientifico: Prof. R. Gorrieri, Università di Bologna).

8. Member of Progetto ex 60% - Università di Salerno, anno 2002. Title: *Sicurezza e Algoritmi in Protocolli di Comunicazione.*

9. Member of Progetto ex 60% - Università di Salerno, anno 2003. Title: *Sicurezza Dati e Algoritmica.*

10. Member of the *European Network of Excellence in Cryptology - ECRYPT*, IST-2002-507932.

11. Member of Progetto ex 60% - Università di Salerno, anno 2004. Title: *Sicurezza Dati, Computazione Distribuita e Compressione Dati.*

12. Member of Progetto ex 60% - Università di Salerno, anno 2005. Title: *Sicurezza, Reti, e Compressione.*

13. Member of Progetto ex 60% - Università di Salerno, anno 2006: Title: *Sicurezza delle reti, animazione di protocolli crittografici e algoritmi .*

14. 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.*

15. Member of Progetto ex 60% - Università di Salerno, anno 2007. Title: *Protocolli crittografici e algoritmi di compressione.*

16. Member of the *European Network of Excellence in Cryptology - ECRYPT II*, ICT-2007-216646.

17. Member of Progetto ex 60% - Università di Salerno, anno 2008. Title: *Sicurezza, privatezza e compressione in documenti multimediali e tecnologia Rfid.*

18. 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.*

19. Member of Progetto ex 60% - Università di Salerno, anno 2009: *Algoritmi per la privacy, la compressione dati e la composizione musicale.*

20. Member of Progetto ex 60% - Università di Salerno, anno 2010: *Sicurezza dati, compressione dati e musimatica.*

21. Member of Progetto ex 60% - Università di Salerno, anno 2011: *Algoritmi e computazioni sicure.*

22. Member of Progetto ex 60% - Università di Salerno, anno 2012: *Protocolli sicuri, metodi per la digital forensics, tecniche di compressione e algoritmi per la musimatica.*

23. Spanish project supported by "Ministerio de Economa y Competitividad", Grant MTM-2012-15167, years 2011-2013: *Provable secure cryptography.*

24. Member of Progetto PRIN: - 10 Universities and a few research institutes, years 2012/2014: *Data-Centric Genomic Computing (GenData 2020).*

25. Member of Progetto FARB - Università di Salerno, anno 2013: *Tecniche e algoritmi per multiparty computation, analisi del traffico, digital forensics, compressione immagini e musimatica.*

26. Member of Progetto FARB - Università di Salerno, anno 2014: *Metodi di digital forensics, sicurezza dati, compressione dati e musimatica.*

27. Spanish project supported by "Ministerio de Economa y Competitividad" MTM2013-41426-R, years 2014-2017: *eSAMCid: Hacia una sociedad digital segura: Avances matemticos en criptografa y su impacto en las tecnologas digitales.*

28. Member of Progetto FARB - Università di Salerno, anno 2015: *Nuove metodologie e soluzioni per Sicurezza Dati, Digital Forensics, Telecomunicazioni, Compressione Dati, e Musimatica..*

29. Member of Progetto FARB - Università di Salerno, anno 2016: *Approcci innovativi per Reti di comunicazioni, Sicurezza, Compressione e Musimatica.*

30. Spanish project supported by "Ministerio de Economa y Competitividad" MTM2016-77213-R, from 2017, on going: *CArSD: Criptografa avanzada para afrontar nuevos retos de la sociedad digital.*

31. Member of Progetto FARB - Università di Salerno, anno 2017: *Metodologie innovative per Sicurezza Dati, Digital Forensics, Reti, Compressione Dati, e Musimatica*

32. Member of Progetto FARB - Università di Salerno, anno 2018: *Studio ed analisi di problematiche e soluzioni innovative in ambito Cybersecurity, Crittografia, Algoritmi, Elaborazione ed Analisi Dati Eterogenei*

33. Member of Progetto FARB - Università di Salerno, anno 2019: *Esplorazione di nuove frontiere della ricerca in ambito Cybersecurity, Crittografia, Algoritmi, Elaborazione ed Analisi Dati Eterogenei*

34. Member of Progetto FARB - Università di Salerno, anno 2020: *Nuove prospettive di ricerca in ambito sicurezza dei dati e delle infrastrutture, algoritmi innovativi, ed elaborazione ed analisi dati eterogenei*

35. Member of Progetto FARB - Università di Salerno, anno 2021: *Nuove frontiere della ricerca nei settori della sicurezza dei sistemi, dei dati e delle telecomunicazioni, sistemi intelligenti, algoritmi, modelli ed architetture avanzati per lanalisi e il trattamento di dati eterogenei*

36. Member of Progetto FARB - Università di Salerno, anno 2022: *Nuovi scenari di ricerca in ambito Cybersecurity, Crittografia, Reti di Telecomunicazioni/IoT, Algoritmi, Elaborazione ed Analisi Dati Eterogenei*

37. Member of Progetto **RRNP**, 2023-2025: SEcurity and RIghts in the CyberSpace - SERICS - PNRR MUR M4C2 - I 1.3., cod. PE00000014, member of the UNISA unit involved in Spoke 5 "Secure and Traceable Identities in Distributed Environments"- STRIDE-

15 Organizing Activity

1. Member of the local organizing committee for the conference *SCN 18, Security and Cryptography for Networks,* Amalfi (SA), September 5-7, 2018.

2. Member of the local organizing committee for the conference *SCN 16, Security and Cryptography for Networks,* Amalfi (SA), August 31- September 2, 2016.

3. Member of the local organizing committee for the conference *SCN 14, Security and Cryptography for Networks,* Amalfi (SA), September 3–5, 2014.

4. Member of the local organizing committee for the conference *SCN 12, Security and Cryptography for Networks,* Amalfi (SA), September 5–7, 2012.

5. Member of the local organizing committee for the conference *SCN 10, Security and Cryptography for Networks,* Amalfi (SA), September 13–15, 2010.

6. Member of the local organizing committee for the conference *SCN 04, Security in Communication Networks,* Amalfi (SA), September 8–10, 2004.

7. Member of the local organizing committee for the conference *DISC 2003, 17th International Symposium on Distributed Computing,* Sorrento (NA), Ottobre 1–3, 2003.

8. Member of the local organizing committee for the conference *SCN 02, Security in Communication Networks,* Amalfi (SA), September 12–13, 2002.

9. Member of the local organizing committee for the conference *SCN 99, Security in Communication Networks,* Amalfi (SA), September 16–17, 1999.

16 Referee for Conferences and Journals

- Journals for which papers have been reviewed: ACM Transactions on Information and System Security, Siam Journal on Discrete Mathematics, IEEE Transactions on Information Theory, IEEE Transactions on Mobile Computing, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Industrial Informatics, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Signal Processing, IEEE Transactions on Circuits and Systems, IEEE Transactions on Wireless Communications, Theoretical Computer Science, Discrete Mathematics, 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 (not involved as PC member): CCS2016, ESORICS 2012, SAC 2011, DISC 2011, ESORICS 2011, ASIACRYPT 2010, PKC2010, 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, ASIACRYPT 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.

- In December 2015, Chair of the Committee for the Ph.D Thesis of Matteo Signorini at Universidad Pompeu Fabra, Barcelona, Spain.

- In 2016 and 2017, member of the National Committee for Computer Science for the evaluation of Assistant Professors after their first three years of enrollment.
- From 2018 to 2021 **tutor** of *Zahra Ebadi Ansaroudi*, for the Ph.D Program in Computer Science (Dottorato in Informatica, ciclo XXXIV) at the Università di Salerno. Zahra Ebadi Ansaroudi got her Ph.D on May 23, 2022.

17 Publications

Journals:

1. Z. Ebadi Ansaroudi, R. Zaccagnino and P. D'Arco.
Pseudorandomness and Deep Learning: a case study.
Applied Science, 2023, 13(5), 3372.

2. P. D'Arco, R. De Prisco, Z. Ebadi Ansaroudi e R. Zaccagnino.
Gossamer: weaknesses and performance.
International Journal of Information Security, Vol. 21, pp. 669–687, 2022.

3. P. D'Arco, R. De Prisco, A. De Santis.
Secret sharing schemes for infinite sets of participants: A new design technique.
Theorical Computer Science, N. 859, pp. 149-161, 2021.

4. P. D'Arco, M.I. Gonzalez Vasco, A.L. Perez del Pozo, C. Soriente, and R. Steinwandt.
Private Set Intersection: New Generic Constructions and Feasability Results.
Advances in Mathematics of Communications, pp. 481 - 502, Vol. 11, Issue 3, August 2017.

5. A. Castiglione, P. D'Arco, A. De Santis, and R. Russo.
Secure group communication schemes for dynamic heterogeneous distributed computing.
Future Generation Computer Systems, pp. 313-324, Vol. 74, September 2017.

6. P. D'Arco and R. De Prisco.
Secure Computation without Computers.
Theoretical Computer Science, Vol. 651, pp. 11-36, 2016.

7. P. D'Arco, N. N. Esfahani, D. R. Stinson.
All or Nothing at All. The Electronic Journal of Combinatorics, Vol. 23, Issue 4, 2016.

8. P. D'Arco and A. De Santis.
Anonymous Protocols: Notions and Equivalence.
Theoretical Computer Science, Vol. 581, pp. 9-25, May 2015.

9. P. D'Arco, R. De Prisco and A. De Santis.
Measure-independent Characterization of Contrast Optimal Visual Cryptography Schemes.
The Journal of Systems and Software, Vol. 95, pp. 89-99, 2014.

10. P. D'Arco and A. P. Del Pozo.
Towards tracing and revoking schemes secure against collusion and any form of secret information leakage.
International Journal of Information Security, Vol. 12, N. 1, pp. 1-17, Springer-Verlag, 2013.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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

22. C. Blundo, P. D'Arco, A. De Santis and C. Galdi.
Hyppocrates: A New Proactive Password Checker.
Journal of Systems and Software, Vol. 71, pp. 163–175, 2004.

23. 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.

24. 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.

25. 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.

26. 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

27. P. D'Arco e A. De Santis.
Private computations on set intersection.
Submitted for publication, 2023.

28. P. D'Arco e F. Mogavero.
On multi-stage Proof-of-Works.
Blockchain and Applications. BLOCKCHAIN 2021. Lecture Notes in Networks and Systems, vol 320, pp. 91-105, Springer, 2022.

29. P. D'Arco and Z. Ebadi Ansaroudi.
Security Attacks on Multi-stage Proof-of-Work.
Proc. of the IEEE Percom Workshop on Security, Privacy, and Trust in the Internet of Things (SPT-IoT), 2021.

30. P. D'Arco and Z. Ebadi Ansaroudi.
Secret disclosure attacks on a recent ultra-lightweight mutual RFID authentication protocol for blockchain-enabled supply chains.
Proc. of the 16th International Conference on Information Assurance and Security (IAS 2020), 2020.

31. P. D'Arco and M. Nilo.
A New Instance of a Lightweight Authentication Protocol Based on the LPN Problem.
Pervasive Systems, Algorithms and Networks, Proc. of I-SPAN 2019, CCIS 1080, pp. 118-132, 2019.

32. P. D'Arco.
Ultralightweight Cryptography - Some Thoughts on Ten Years of Efforts.
Proc. of the 11th International Conference on Information Technology and Communications Security (secITC 2018), Lecture Notes in Computer Science, Vol. 11359, pp. 1-16, Springer Verlag, 2018.

33. P. D'Arco, R. De Prisco, A. De Santis.
On the Equivalence of 2-Threshold Secret Sharing Schemes and Prefix Codes.
Proc. of CSS2018, Lecture Notes in Computer Science, Springer Verlag, Vol. 11161,pp. 157-167, 2018.

34. P. D'Arco, R. De Prisco,A. L. Prez del Pozo.
An Efficient and Reliable Two-Level Lightweight Authentication Protocol.
Proc. of CSS2018, Lecture Notes in Computer Science, Springer Verlag, Vol. 11161,pp. 168-180, 2018.

35. P. D'Arco, R. De Prisco,A. De Santis,A. L. Prez del Pozo,U. Vaccaro.
Probabilistic Secret Sharing.
Proc. of MFCS2018, Vol. 117, pp.1-16, 2018.

36. P. D'Arco and R. De Prisco.
Design Weaknesses in Recent Ultralightweight RFID Authentication Protocols.
Proc. of SEC2018, IFIP AICT, Springer, Vol. 529, pp. 3-17, 2018.

37. P. D'Arco, R. De Prisco and Y. Desmedt.
Private Visual Share-Homomorphic Computation and Randomness Reduction in Visual Cryptography
Proc. of the 9th International Conference on Information Theoretic Security (ICITS 2016), Lecture Notes in Computer Science, Vol. 10015, pp. 95-113, Springer Verlag, 2016.

38. P. D'Arco and R. De Prisco.
Visual Cryptography: Models, Issues, Applications and New Directions.
Proc. of the 9th International Conference on Information Technology and Communications Security (secITC 2016), Lecture Notes in Computer Science, Vol. 10006, pp. 20-39, Springer Verlag, 2016.

39. P. D'Arco and R. De Prisco.
Secure Two-party Computation: a visual way
Proc. of the 7th International Conference on Information Theoretic Security (ICITS2013), Lecture Notes in Computer Science, Vol. 8317, pp. 18-34, Springer Verlag, 2014.

40. P. D'Arco, R. De Prisco and A. De Santis.
Measure-independent Characterization of Contrast Optimal Visual Cryptography Schemes
Proc. of the 7th International Conference on Information Theoretic Security (ICITS2013), Lecture Notes in Computer Science, Vol. 8317, pp. 39-55, Springer Verlag, 2014.

41. P. D'Arco and A. De Santis.
Key Privacy and Anonymous Protocols,
Proc. of the IEEE 11th International Conference on Privacy, Security and Trust (PST2013), July 10-12, 2013. ISBN 978-1-4673-5839-2.

42. P. D'Arco, M. I. Gonzalez Vasco, A. L. Perez del Pozo, and C. Soriente
Size-Hiding in Private Set Intersection: Existential Results and Constructions
Proc. of the 5th International Conference on Cryptology (Africacrypt 2012). Lecture Notes in Computer Science, Vol. 7374, pp. 378-394, Springer Verlag, 2012.

43. P. D'Arco and Angel L. Perez del Pozo
Fighting Pirates 2.0.
Proc. 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.

44. P. D'Arco
An Almost-Optimal Forward-Private Rfid Mutual Authentication Protocol with Tag Control.
Proc. 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.

45. 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.

46. 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).

47. 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.

48. 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.

49. 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 (ICITS07) Lecture Notes in Computer Science, Vol. 4883, pp. 46–64, 2009.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. P. D'Arco, W. Kishimoto, and D. Stinson.
On Cheating-Immune Secret Sharing.
Proc. of the International Workshop on Coding and Cryptography (WCC 2003), pp. 111-120, 2003.

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.

64. 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

65. 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: Signature
May 2nd, 2023.