Curriculum Vitæ et Studiorum di

Paolo D'Arco

2 Maggio 2023

1 Breve Biografia

Paolo D'Arco è nato a Salerno il 7 Luglio del 1972. Si è laureato (con lode) in Scienze dell' Informazione nel Maggio del 1997, presso l' Università degli Studi di Salerno. Nella stessa Università, nel Febbraio 2002, ha conseguito il Dottorato di Ricerca in Informatica, discutendo una tesi in Crittografia. Durante il corso di Dottorato ha partecipato a diverse scuole internazionali. Nell'ultimo anno del corso ha soggiornato un semestre presso l'Università di Waterloo, in Ontario (Canada) ed è stato per brevi periodi presso l'Università Politecnica di Catalunia a Barcellona (Spagna) e Telcordia Technologies (DIMACS, New Jersey, Stati Uniti). Da Novembre 2001 ad Ottobre 2002 è ritornato all'Università di Waterloo, in qualità di borsista post-dottorato presso il Centre for Applied Cryptographic Research (CACR), all'interno del Department of Combinatorics and Optimization, con il supporto e sotto la supervisione dal professor Douglas Stinson. Presso il Dipartimento di Informatica dell'Università degli Studi di Salerno è stato, dal 2005 al 2015 ricercatore universitario, dal 2015 al 2021 professore associato e da Dicembre 2021 ricopre il ruolo di professore ordinario.

I suoi interessi di ricerca riguardano principalmente la Crittografia. Si è occupato di progettazione ed analisi di schemi e primitive crittografiche incondizionatamente sicuri, in cui cioè il potere computazionale dell'avversario si assume potenzialmente infinito, e di schemi computazionalmente sicuri, in cui invece si assume che l'avversario possa utilizzare soltanto attacchi realistici, in termini di spazio e di tempo. Nel primo caso l'attenzione è stata focalizzata su schemi per la condivisione dei segreti, per la distribuzione di chiavi crittografiche, per il recupero privato di informazioni da un database e sull'oblivious transfer; nel secondo, su schemi per trasmissioni broadcast robuste e distribuite, per trasmissioni anonime e per l'autenticazione di dispositivi leggeri. Si è anche occupato di crittoanalisi di nuovi protocolli. Al momento sta lavorando su protocolli efficienti ed user-friendly per two-party e multi-party computation, e su protocolli sicuri in ambienti in cui la fiducia che si ripone nelle entità hardware e software è fortemente limitata.

Dal 2005 ad oggi ha fatto parte di circa 60 comitati di programma di conferenze internazionali, ed ha tenuto relazioni su invito a Stinson66 (2022), a SecITC (2018), a SecITC (2016), alla Smart University (2007), alla Third Pythagorean Conference on Geometry, Combinatorial Design and Cryptology (2003), ed al Summer Meeting della Canadian Mathematical Society (CMS) (2002). Da Dicembre 2008 è membro del Collegio dei Docenti del Dottorato in Informatica, presso l'Università di Salerno. Dall'anno accademico 2004/2005 ad oggi è stato titolare di corsi di insegnamento di Informatica di base, algoritmi, sistemi operativi, reti, sicurezza su reti e crittografia per i corsi di Laurea di Informatica e Matematica. È stato relatore di più di 70 Tesi di Laurea, e dal 2005 è tutor dipartimentale per il programma Erasmus. È stato coordinatore di due progetti per giovani ricercatori (anni 2001 e 2002) che hanno ricevuto finanziamento biennale, ed ha partecipato attivamente a progetti di ricerca nazionali ed internazionali (e.g., azioni integrate Italia-Spagna). In particolare, ha partecipato a tre PRIN, finanziati per i periodi 2006-2008, 2008-2010 e 2012-2014 su basi di dati crittografate, strumenti per la tutela della privacy, e computazioni su dati genomici, rispettivamente. Inoltre è stato membro del network europeo di eccellenza in crittografia (ECRYPT), IST-2002-507932, e del network (ECRYPT II), ICT-2007-216646, per i periodi 2004-2008 e 2008-2012. Infine, è stato membro dei comitati organizzatori delle conferenze Security in Communication Networks negli anni 1999, 2002, 2004, 2010, 2012, 2014, 2016, 2018 e del 17th International Symposium on Distributed Computing, nel 2003. Da Maggio 2014 a Dicembre 2018 è stato referente italiano (membro del management committee) della ICT COST Action IC1403 CRYPTACUS di durata quadriennale. Ha pubblicato più di 60 lavori in riviste di ottima qualità e in atti di conferenze internazionali di rilievo di Informatica Teorica, Crittografia e Sicurezza Dati.

Indice

2 Dati Personali

Nome: Paolo
Cognome: D'Arco
Data di nascita: 07/07/1972
Luogo di nascita: Salerno
Stato civile: di stato libero

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

Tel: 089 969718
Fax: 089 969600
e-mail: pdarco@unisa.it
URL: http://www.di.unisa.it/professori/paodar

3 Ruolo Attuale

Professore ordinario presso il Dipartimento di Informatica dell'Università di Salerno.

4 Interessi di Ricerca

Crittografia, algoritmi e sicurezza dei dati.

5 Borse di Studio

- Assegno di ricerca nel settore dell'Information and Communication Technology, conferito dal Centro di Competenza RCOST, con sede presso l'Università del Sannio. Periodo: Luglio 2004 - Dicembre 2004.
- Borsa Post-Dottorato, conferita dalla Facoltà di Scienze MM. FF. NN., presso il Dipartimento di Informatica ed Applicazioni dell'Università di Salerno. Periodo: Ottobre 2002 - Giugno 2004,
- **Post-Doctoral Fellowship**, conferita dal Centre for Applied Cryptographic Research (CACR), presso il Department of Combinatorics and Optimization of the University of Waterloo, Ontario, Canada. Periodo: Novembre 2001 - Ottobre 2002.

6 Formazione: Corsi, Titoli e Visite

- Ha conseguito l'abilitazione scientifica nazionale a professore ordinario, Bando D.D. 1532/2016, nel settore concorsuale 01/B1, valida dall'11-09-2019.
- Ha conseguito l'abilitazione scientifica nazionale a professore ordinario, Bando D.D. 1532/2016, nel settore concorsuale 09/H1, valida dal 26-07-2018.
- Ha conseguito l'abilitazione scientifica nazionale a professore associato, Bando D.D. 222/2012, nel settore concorsuale 01/B1, valida dal 29-01-2014.
- Ha conseguito l'abilitazione scientifica nazionale a professore associato, Bando D.D. 222/2012, nel settore concorsuale 09/H1, valida dal 03-12-2013.
- Dal 2011 al 2015, ogni anno, ha visitato il Mathematical Cryptology Group presso l' Universidad Rey Juan Carlos, Madrid, Spagna.
- Nell'Ottobre 2006 ha partecipato alla *Autumn International School on Zero Knowledge: Foundations and Applications*, Bertinoro, Bologna.
- L'8 Febbraio 2002 ha conseguito il **Dottorato di Ricerca** in Informatica presso l'Università degli Studi di Salerno, discutendo una tesi in Crittografia dal Titolo *Distribution and Obliviousness. The Key Establishment Problem.* Relatore: Prof. Carlo Blundo.
- Nel Giugno 2001 ha visitato *DIMACS (Telcordia Tecnologies)*, New Jersey, USA.
- Da Gennaio 2001 a Maggio 2001 ha svolto attività di ricerca al Centre for Applied Cryptographic Research, presso il Department of Combinatorics and Optimization dell' Università di Waterloo, Ontario, Canada, sotto la supervisione del Prof. Douglas Stinson.
- Nel Novembre 2000 ha visitato il *Departament de Matemàtica i Telemàtica* presso l'Universitat Politècnica de Catalunya, Barcellona, Spagna.
- Ha partecipato alla *12th International School for Computer Science Researchers on E-commerce and On-line Algorithms*, Lipari, 9-22 Luglio, 2000. Docenti: S. Micali, M. Bellare, T. Rabin, M. Yung, A. Borodin, A. Blum e J. Kleinberg.
- Ha partecipato alla *5th International Summer School on Distributed Computing: Advanced Distributed Computing*, Siena, 21-27 Giugno, 1999. Docenti: S. Dolev, C. Dwork, D. Peleg e N. Santoro.
- Ha partecipato alla *10th International School for Computer Science Researchers on Distributed Systems and Security*, Lipari, 5-18 Luglio, 1998. Docenti: A. Shamir, A. De Santis, S. Micali, P. Rogaway, R. Gennaro, M. Herlihy, L. Shrira e Y. Afek.
- Il 27 Maggio 1997 ha conseguito la **Laurea in Scienze dell'Informazione** presso l'Università degli Studi di Salerno, con votazione pari a 110/110 e lode, discutendo una tesi dal titolo *Crittografia Visuale. Il Contrasto negli Schemi a Soglia.* Relatore: Prof. Alfredo De Santis.

- Nel 1991 ha conseguito il diploma di **Maturità Scientifica** presso il Liceo Scientifico Statale "G. Da Procida" di Salerno con votazione pari a 60/60.

7 Lingue Straniere

Lingua Inglese.

8 Progetti di Ricerca Internazionali

- **Coordinatore** nazionale per l'Italia (management committee member) della ICT COST Action IC1403 Cryptanalysis of ubiquitous computing systems (CRYPTACUS), avente come responsabile europeo (project chair) il Prof. Gildas Avoine (University of Leuven). La ICT Action è partita nel Luglio del 2014 e si è conclusa a Dicembre 2018. Nel progetto sono state coinvolte 30 nazioni. Il budget complessivo allocato è stato di 541000 euro. Ogni anno si sono tenuti due meeting del comitato internazionale di gestione in una nazione diversa. Complessivamente il progetto ha visto la pubblicazione di 43 lavori, che raccolgono i risultati delle ricerche congiunte da parte dei gruppi di lavoro. L'output più visibile di CRYPTACUS é un libro (https://www.springer.com/us/book/9783030105907) open-access pubblicato dalla Springer. É co-autore di un capitolo. Ulteriori dettagli sono disponibili sul sito del progetto (https://www.cost.eu/actions/IC1403/).

- Membro dell'unità UNISA dello *European Network of Excellence in Cryptology - ECRYPT*, progetto n. IST-2002-507932, dal 1 Febbraio 2004 al 31 Luglio 2008.

- Membro dell'unità UNISA dello *European Network of Excellence in Cryptology - ECRYPT II*, progetto n. ICT-2007-216646, dal 1 Agosto 2008 al 31 Gennaio 2013.

- Collaboratore esterno, in qualità di esperto internazionale, al progetto di ricerca spagnolo MTM2012-15167, dal titolo *Seguridad Demostrable: validacin de herramientas criptogrficas a travs del lgebra y la matemtica discreta*, dal 01-01-2011 al 31-12-2013.

- Collaboratore esterno, in qualità di esperto internazionale, al progetto di ricerca spagnolo MTM2013-41426-R, dal titolo *eSAMCid: Hacia una sociedad digital segura: Avances matemticos en criptografa y su impacto en las tecnologas digitales*, dal 01-01-2014 al 31-12-2017.

- Collaboratore esterno, in qualità di esperto internazionale, al progetto di ricerca spagnolo MTM2016-77213-R, dal titolo *CArSD: Criptografa avanzada para afrontar nuevos retos de la sociedad digital*, dal 01-01-2017.

9 Progetti di Ricerca Nazionali

- É stato **responsabile** del progetto italiano *Oblivious Transfer e applicazioni al commercio elettronico*, presentato nell'ambito delle iniziative di ricerca condotte da giovani ricercatori, Università di Salerno, anno 2002.
- É stato **responsabile** del progetto italiano *Sistemi per il controllo proattivo di password*, presentato nell'ambito delle iniziative di ricerca condotte da giovani ricercatori, Università di Salerno, anno 2001.

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

- Progetto ex 60% - Università di Salerno, anno 1998: *Algoritmi: Progetto, Analisi e Sintesi.*
- Progetto ex 60% - Università di Salerno, anno 1999: *Algoritmi: Animazione, Compressione e Sicurezza con Applicazioni su Internet.*
- Progetto ex 60% - Università di Salerno, anno 2000: *Sicurezza, Codici e Compressione: Progetto, Analisi e Realizzazione.*
- Azioni Integrate Italia–Spagna - MIUR, anno 2000: *Schemi per la Distribuzione di Chiavi Crittografiche.*
- Progetto Giovani Ricercatori CNR Agenzia 2000: *Pubblicità Online: Nuove Misure per Nuovi Media. Auditing ed Accounting Sicuro sul Web.*
- Progetto ex 60% - Università di Salerno, anno 2001: *Computazione, Comunicazione e Sicurezza in Reti di Calcolatori.*
- Progetto ex 40% - MURST, anno 2001: *MEFISTO: Metodi Formali per la Sicurezza* (coordinatore scientifico: Prof. R. Gorrieri, Università di Bologna).
- Progetto ex 60% - Università di Salerno, anno 2002: *Sicurezza e Algoritmi in Protocolli di Comunicazione.*
- Progetto ex 60% - Università di Salerno, anno 2003: *Sicurezza Dati e Algoritmica.*
- Progetto ex 60% - Università di Salerno, anno 2004: *Sicurezza Dati, Computazione Distribuita e Compressione Dati.*
- Progetto ex 60% - Università di Salerno, anno 2005: *Sicurezza, Reti, e Compressione.*
- Progetto ex 60% - Università di Salerno, anno 2006: *Sicurezza delle reti, animazione di protocolli crittografici e algoritmi* .
- Progetto **PRIN**: Università di Bergamo, Università di Milano e Università di Salerno, anni 2006/2008:*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.*
- Progetto ex 60% - Università di Salerno, anno 2007: *Protocolli crittografici e algoritmi di compressione.*

- Progetto ex 60% - Università di Salerno, anno 2008: *Sicurezza, privatezza e compressione in documenti multimediali e tecnologia Rfid.*
- Progetto **PRIN**: Università di Bergamo, Università di Milano e Università di Salerno, anni 2008/2010:*Progettazione ed analisi di protocolli crittografici per la tutela della privacy personale e dei dati in basi di dati e dispositivi mobili.*
- Progetto ex 60% - Università di Salerno, anno 2009: *Algoritmi per la privacy, la compressione dati e la composizione musicale.*
- Progetto ex 60% - Università di Salerno, anno 2010: *Sicurezza dati, compressione dati e musimatica.*
- Progetto ex 60% - Università di Salerno, anno 2011: *Algoritmi e computazioni sicure.*
- Progetto ex 60% - Università di Salerno, anno 2012: *Protocolli sicuri, metodi per la digital forensics, tecniche di compressione e algoritmi per la musimatica.*
- Progetto FARB - Università di Salerno, anno 2013: *Tecniche e algoritmi per multiparty computation, analisi del traffico, digital forensic, compressione di immagini e musimatica.*
- Progetto **PRIN**: - Politecnico di Milano, Università di: Milano, Torino, Bergamo, Bologna, Roma 1, Roma 3, Salerno, della Calabria e vari enti di ricerca, anni 2013/2015: *Data-Centric Genomic Computing (GenData 2020).*
- Progetto FARB - Università di Salerno, anno 2014: *Metodi di Digital Forensics, Sicurezza Dati e Compressione Dati.*
- Progetto FARB - Università di Salerno, anno 2015: *Nuove metodologie e soluzioni per Sicurezza Dati, Digital Forensics, Telecomunicazioni, Compressione Dati, e Musimatica..*
- Progetto FARB - Università di Salerno, anno 2016: *Approcci innovativi per Reti di comunicazioni, Sicurezza, Compressione e Musimatica.*
- Progetto FARB - Università di Salerno, anno 2017: *Metodologie innovative per Sicurezza Dati, Digital Forensics, Reti, Compressione Dati, e Musimatica*
- 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*
- Progetto FARB - Università di Salerno, anno 2019: *Esplorazione di nuove frontiere della ricerca in ambito Cybersecurity, Crittografia, Algoritmi, Elaborazione ed Analisi Dati Eterogenei*
- 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*

- 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*

- 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*

- Progetto **PNRR** - Partenariato esteso (12 Università, aziende ed enti di ricerca), 2023-2025: SEcurity and RIghts in the CyberSpace - SERICS - PNRR MUR M4C2 - I 1.3., codice PE00000014, membro dell'unità UNISA coinvolta nello Spoke 5 "Secure and Traceable Identities in Distributed Environments"- STRIDE-

10 Editorial Board

1. Membro dell'editorial board della *Special Issue on Security and Privacy in Complex Systems*, IEEE Systems Journal, periodo 10/2011 – 10/2012.

2. Membro dell'editorial board della rivista *Security and Communication Networks*, Wiley-Hindawi, da Agosto 2016 a Novembre[1] 2020.

3. Membro dell'editorial board della rivista *Journal of Mathematical Cryptology*, De Gruyter, da Marzo 2020.

11 Comitati di Programma

1. Membro del comitato di programma della *16th International Conference on Information Technology and Communications Security*, (SecITC 2023), 23-24 Novembre, Bucarest, Romania, 2023.

2. Membro del comitato di programma della *The 5th IEEE International Conference on Decentralized Applications and Infrastructures* (IEEE DAPPS 2023), 17-20 Luglio, Atene, Grecia, 2023.

3. Membro del comitato di programma della *The 38th International Conference on ICT Systems, Security and Privacy Protection* (IFIP SEC 2023) 14-16 Giugno, Poznan, Polonia, 2023.

4. Membro del comitato di programma della *4th IEEE International Conference on Decentralized Applications and Infrastructures* (IEEE DAPPS 2022), 15-18 Agosto, Bay Area, CA, United States, 2022.

5. Membro del comitato di programma della *4th IEEE International Conference on Cyber Security and Resilience* (IEEE CSR 2022), 15-18 Agosto, Virtual Conference, 2022.

[1] Richiesta volontaria di uscire dall'editorial board. Alla luce di una riflessione più ampia, maturata negli anni recenti, sulle modalità di gestione e sugli aspetti degenerativi, legati alla proliferazione e al business delle pubblicazioni scientifiche, ho rifiutato inviti a partecipare ad editorial board di riviste (o a svolgere funzione di guest editor per special issue) in cui gli autori pagano contributi non trascurabili per la pubblicazione (APC, Article Processing Charge), o in cui le procedure di revisione non sono scrupolosamente approfondite.

6. Membro del comitato di programma della *37th International Conference on ICT Systems Security and Privacy Protection*, (IFIP SEC 2022),13-17 Giugno, Copenaghen, Danimarca, 2022.

7. Membro del comitato di programma della *36th International Conference on ICT Systems Security and Privacy Protection*, (IFIP SEC 2021), 22-24 Giugno, Oslo, Norvegia, 2021.

8. Membro del comitato di programma della *2021 IEEE International Conference on Cyber-Security and Resilience*, (IEEE CSR 2021), 22-24 Marzo, Rodi, Grecia, 2021.

9. Membro del comitato di programma della *23th International Conference on Information Security and Cryptology* (ICISC 2020), 4-5 Dicembre, 2020, Seoul, Corea del Sud.

10. Membro del comitato di programma della *13th International Conference on Information Technology and Communications Security*, (SecITC 2020), 19-20 Novembre, Bucarest, Romania, 2020.

11. Membro del comitato di programma della *35th International Information Security and Privacy Conference*, (IFIP SEC 2020), 26-28 Maggio, Maribor, Slovenia, 2020.

12. Membro del comitato di programma della *12th International Conference on Information Technology and Communications Security*, (SecITC 2019), 14-15 Novembre, Bucharest, Romania, 2019.

13. Membro del comitato di programma della *11th International Conference on Information Technology and Communications Security*, (SecITC 2018), 8-9 Novembre, Bucarest, Romania, 2018.

14. Membro del comitato di programma della *33rd IFIP TC-11 SEC 2018 International Conference on Information Security and Privacy Protection* (SEC 2018) 18-20 Settembre, Poznan, Poland, 2018.

15. Membro del comitato di programma della *20th International Conference on Information Security and Cryptology* (ICISC 2017), 29 Novembre - 1 Dicembre, 2017, Seoul, Corea.

16. Membro del comitato di programma della *10th International Conference on Information Theoretic Security* (**ICITS** 2017), 29 Novembre - 2 Dicembre, 2017, Hong Kong.

17. Membro del comitato di programma della *7th iCatse International Conference on IT Convergence and Security*, (ICITCS 2017), 25-28 Settembre 2017, Seoul, Corea.

18. Membro del comitato di programma della *10th International Conference on Information Technology and Communications Security*, (SecITC 2017), 8-9 Giugno 2017, Bucharest, Romania.

19. Membro del comitato di programma della *19th International Conference on Information Security and Cryptology* (ICISC 2016), 30 Novembre - 2 Dicembre 2017, Seoul, Corea.

20. Membro del comitato di programma della *19th Information Security Conference* (ISC 2016), 7-9 Settembre 2016, Honolulu, HI, USA.

21. Membro del comitato di programma della *9th International Conference on Information Security* (ICITS 2016), 9-12 Agosto 2016, Tacoma, Washington, USA.

22. Membro del comitato di programma della *9th International Conference on Information Technology and Communications Security* (SecITC 2016), 9-10 Giugno 2016, Bucarest, Romania.

23. Membro del comitato di programma della *18th International Conference on Information Security and Cryptology* (ICISC 2015), 25-27 Novembre 2015, Seoul, Corea.

24. Membro del comitato di programma della *18th Information Security Conference* (ISC 2015), 9-11 Settembre 2015, Trondheim, Norvegia.

25. Membro del comitato di programma della *8th International Conference on Information Theoretic Security* (**ICITS** 2015), 2-5 Maggio 2015, Lugano, Svizzera.

26. Membro del comitato di programma della *17th International Conference on Information Security and Cryptology* (ICISC 2014), 3-5 Dicembre 2014, Seoul, Corea.

27. Membro del comitato di programma del *1st International Conference on Cryptography and Information security* (BalkanCryptSec 2014), 16-17 Ottobre 2014, Istanbul, Turchia.

28. Membro del comitato di programma del *Twelfth annual Conference on Privacy, Security and Trust* (PST 2014), 23-24 Luglio 2014, Toronto, Canada.

29. Membro del comitato di programma del *2nd International Conference on Intelligent Information System and Technology* (ICIIST 2014), 26-28 Giugno 2014, Tsingdao, Cina.

30. Membro del comitato di programma del *16th International Conference on Information Security and Cryptology* (ICISC 2013), 27-29 Novembre 2013, Seoul, Corea.

31. Membro del comitato di programma del *10th European Workshop: Research and Applications* (EUROPKI 2013), 12-13 Settembre 2013, Rhul, Egham, UK.

32. Membro del comitato di programma della *International Conference on Intelligence Fusion* (ICIF 2013), 27-29 Giugno 2013, Jeju Island, Corea.

33. Membro del comitato di programma del *9th Workshop on Rfid Security* (RFIDSEC 2013), 9-11 Luglio 2013, Graz, Austria.

34. Membro del comitato di programma della *15th International Conference on Information Security and Cryptology* (ICISC 2012), 28-30 Novembre 2012, Seoul, Corea.

35. Membro del comitato di programma del *9th European Workshop on PKI: Research and Applications* (EUROPKI 2012), 13-14 Settembre 2012, Pisa, Italia

36. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ICISC 2011), 30 Novembre - 2 Dicembre 2011, Seoul, Corea.

37. Membro del comitato di programma della *International Conference on Computer Convergence Technology* (ICCCT 2011), 20-22 Ottobre 2011, Seoul, Corea.

38. Membro del comitato di programma della *The 2nd International Conference on Security-enriched Urban Computing and Smart Grids* (SUCOMS 2011), 21-23 Settembre 2011, Hualien, Taiwan.

39. Membro del comitato di programma del *8th European Workshop on PKI, Services and Applications* (EUROPKI 2011), 15-16 Settembre 2011, Leuven, Belgio.

40. Membro del comitato di programma della *International Conference on Security and Cryptography* (SECRYPT 2011), 16-18 Luglio 2011, Seviglia, Spagna.

41. Membro del comitato di programma della *5-th International Conference on Information Theoretic Security* (**ICITS** 2011), 21-24 Maggio 2011, Amsterdam, Olanda.

42. Membro del comitato di programma della *14th International Conference on Practice and Theory in Public Key Cryptography* (**PKC** 2011), 6-9 Marzo 2011, Taormina, Italia.

43. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ICISC 2010), 1-3 Dicembre 2010, Seoul, Corea.

44. Membro del comitato di programma della *International Conference on Security Technology* (SecTech 2010), 11-13 Novembre 2010, Bali, Indonesia.

45. Membro del comitato di programma della *First International Conference on Security-enriched Urban Computing and Smart Grid* (SUCOMS 2010), 15-17 Settembre 2010, Daejeon, Corea.

46. Membro del comitato di programma della *International Conference on Security and Cryptography* (SECRYPT 2010), 26-28 Luglio 2010, Atene, Grecia.

47. Membro del comitato di programma della *The 4th International Conference on Information Security and Assurance* (ISA 2010), 23-25 Giugno 2010, Miyazaki, Giappone.

48. Membro del comitato di programma della *International Conference on Security Technology* (SecTech 2009), 10-12 Dicembre 2009, Jeju Island, Corea.

49. Membro del comitato di programma della *International Conference on Information Theoretic Security* (**ICITS** 2009), 2-5 Dicembre 2009, Shizuoka, Giappone.

50. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ICISC 2009), 2-4 Dicembre 2009, Seoul, Corea.

51. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ISCISC 2009), 7-8 Ottobre 2009, Isfahan, Iran.

52. Membro del comitato di programma della *International Conference on Security and Cryptography* (SECRYPT 2009), 7-10 Luglio 2009, Milano, Italia.

53. Membro del comitato di programma di *International Workshop on Computer Graphics, Multimedia and Security* (CGMS-09), 25-27 Giugno 2009, Korea University, Seoul, Corea.

54. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ICISC 2008), 3-5 Dicembre 2008, Seoul, Corea.

55. Membro del comitato di programma della *International Conference on Information Theoretic Security* (**ICITS** 2008), 10-13 Agosto 2008, Calgary, Canada.

56. Membro del comitato di programma della *International Conference on Information Security and Cryptology* (ICISC 2007), 29-30 Novembre 2007, Seoul, Corea.

57. Membro del comitato di programma della *International Conference on Security and Cryptography* (SECRYPT 2007), 28-31 Luglio 2007, Barcellona, Spagna.

58. Membro del comitato di programma della *International Conference on Security and Cryptography* (SECRYPT 2006), 7-10 Agosto 2006, Setubal, Portogallo.

59. Membro del comitato di programma del 6-*th Workshop on Information Security Applications* (WISA 2005), 22-24 Agosto 2005, Jeju Island, Corea.

12 Presentazioni a Conferenze Internazionali su Invito

1. *Invited Speaker* alla conferenza *Stinson66 - New Advances in Designs, Codes and Cryptography* che si terrà al *The Fields Institute* in Toronto, Canada, dal 13 al 17 Giugno 2022. Titolo della presentazione: *Private computations on set intersection.*

2. *Keynote Speaker* alla 11th International Conference on Information Technology and Communications Security (secITC 2018), 8-10 Novembre, 2018, Bucharest, Romania. Titolo della presentazione: *Ultralightweight authentication protocols: a ten-year perspective.*

3. *Keynote Speaker* alla 9th International Conference on Information Technology and Communications Security (secITC 2016), 9-10 Giugno 2016, Bucarest, Romania. Titolo della presentazione: *Visual Cryptography: Models, Issues, Applications and New Directions.*

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

5. *Invited Speaker* alla Third Pythagorean Conference on Geometry, Combinatorial Design and Cryptology, $1-7$ Giugno 2003, Rodi, Grecia. Titolo della presentazione: *Key Distribution with Key-Recovery Techniques over Unreliable Networks.*

6. *Invited Speaker* al Summer Meeting of the Canadian Mathematical Society (CMS), University of Laval, 15-17 Giugno 2002, Quebec City, Quebec, Canada. Titolo della presentazione: *Distributed Oblivious Transfer and Applications to Cryptography.*

13 Attività Organizzativa

- Membro del comitato organizzativo locale della conferenza *SCN18, Security and Cryptography for Networks*, Amalfi (SA), 5-7 Settembre 2018.
- Membro del comitato organizzativo locale della conferenza *SCN16, Security and Cryptography for Networks*, Amalfi (SA), 31 Agosto – 2 Settembre 2016.
- Membro del comitato organizzativo locale della conferenza *SCN14, Security and Cryptography for Networks*, Amalfi (SA), 3–5 Settembre 2014
- Membro del comitato organizzativo locale della conferenza *SCN12, Security and Cryptography for Networks*, Amalfi (SA), 5–7 Settembre 2012
- Membro del comitato organizzativo locale della conferenza *SCN10, Security and Cryptography for Networks,* Amalfi (SA), 13–15 Settembre 2010.
- Membro del comitato organizzativo locale della conferenza *SCN04, Security in Communication Networks,* Amalfi (SA), 8–10 Settembre 2004.
- Membro del comitato organizzativo locale della conferenza *DISC 2003, 17th International Symposium on Distributed Computing,* Sorrento (NA), 1–3 Ottobre 2003.
- Membro del comitato organizzativo locale della conferenza *SCN02, Security in Communication Networks,* Amalfi (SA), 12–13 Settembre 2002.
- Membro del comitato organizzativo locale della conferenza *SCN99, Security in Communication Networks,* Amalfi (SA), 16–17 Settembre 1999.

14 Attività Didattica

- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2022/23.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2022/23.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2021/22.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2021/22.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2020/21.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2020/21.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2019/20.

- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2019/20.
- Crittografia Moderna, **Corso di Dottorato** in Informatica ed Ingegneria dell'Informazione - Ciclo XXXIII, dal 13-02-2018 al 02-03-2018 (3 CFU, 18 ore di lezione frontale).
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2018/19.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2018/19.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2017/18.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2017/18.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, primo semestre, anno accademico 2016/17.
- Fondamenti di Informatica e Laboratorio, Corso di Laurea Triennale in Matematica, Dipartimento di Matematica, primo semestre, anno accademico 2016/17.
- Elementi di Crittografia, Corso di Laurea Magistrale in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2015/16.
- Introduzione agli algoritmi e alle strutture di dati. Corso di Laurea in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2015/16.
- Laboratorio di Reti di Calcolatori, Corso di Laurea in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2014/15.
- Introduzione agli algoritmi e alle strutture di dati. Corso di Laurea in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2014/15.
- Laboratorio di Reti di Calcolatori, Corso di Laurea in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2013/14.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Dipartimento di Informatica, secondo semestre, anno accademico 2013/14.
- Laboratorio di Reti di Calcolatori, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2012/13.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2012/13.
- Corso di Sistemi Operativi, Master in Ricerca e Innovazione nelle Scienze della Salute, Facoltà di Medicina, Luglio 2012.
- Laboratorio di Reti di Calcolatori, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2011/12.

- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2011/12.
- Laboratorio di Reti di Calcolatori, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2009/10.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2009/10.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2008/09.
- Corso di Sistemi Operativi, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2008/09.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2007/08.
- Corso di Sistemi Operativi, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2007/08.
- Corso di Complementi di Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2006/07.
- Corso di Sistemi Operativi, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2006/07.
- Corso di Sistemi Operativi, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2005/06.
- Corso di Esercitazioni di Algoritmi. Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., secondo semestre, anno accademico 2004/05.
- Cicli di Seminari per l'insegnamento Sicurezza su Reti, Corso di Laurea in Informatica, Facoltà di Scienze MM. FF. NN., Università di Salerno, anni accademici 1999/2000 e 2000/2001. Argomenti trattati: Crittografia Visuale, Watermarking Technology.

Nota: all'indirizzo *http://www.di-srv.unisa.it/professori/paodar/teaching.html* sono disponibili le pagine contenenti informazioni organizzative, programmi, slide e materiale didattico, usato per ogni singolo corso (istanza più recente).

15 Dottorato di Ricerca

- Partecipazione al Collegio 2008: Titolo: "INFORMATICA", Ateneo proponente: Università degli Studi di SALERNO. Anno accademico di inizio: 2008 - Ciclo: XXIV - Durata: 3 anni, dal 04-12-2008 al 31-12-2011
- Partecipazione al Collegio 2009: Titolo: "TEORIE, METODOLOGIE E APPLICAZIONI AVANZATE PER LA COMUNICAZIONE, L'INFORMATICA E LA FISICA". Ateneo proponente: Università degli Studi di SALERNO. Anno accademico di inizio: 2009 - Ciclo: XXV - Durata: 3 anni, dal 04-12-2009 al 31-12-2012

- Partecipazione al Collegio 2010: Titolo: "INFORMATICA", Ateneo proponente: Università degli Studi di SALERNO. Anno accademico di inizio: 2010 - Ciclo: XXVI - Durata: 3 anni, dal 02-02-2010 al 31-12-2013

- Partecipazione al Collegio 2011: Titolo: "INFORMATICA", Ateneo proponente: Università degli Studi di SALERNO. Anno accademico di inizio: 2011 - Ciclo: XXVII - Durata: 3 anni, dal 17-11-2011 al 31-10-2014

- Partecipazione al Collegio 2012: Titolo: "INFORMATICA", Ateneo proponente: Università degli Studi di SALERNO.Anno accademico di inizio: 2012 - Ciclo: XXVIII - Durata: 3 anni, dal 12-10-2012 al 31-10-2015

- Partecipazione al Collegio 2013: Titolo: "INFORMATICA E INGEGNERIA DELL' INFORMAZIONE". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2013 - Ciclo: XXIX - Durata: 3 anni, dal 05-09-2013 al 31-10-2016

- Partecipazione al Collegio 2014: Titolo: "INFORMATICA E INGEGNERIA DELL' INFORMAZIONE". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2014/15 - Ciclo: XXX - Durata: 3 anni, dal 06-05-2014 al 31-10-2017

- Partecipazione al Collegio 2015: Titolo: "INFORMATICA E INGEGNERIA DELL' INFORMAZIONE". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2015/16 - Ciclo: XXXI - Durata: 3 anni, dal 21-04-2015 al 31-10-2018

- **Componente effettivo della sottocommissione esaminatrice** per il curriculum INFORMATICA per il ciclo XXXI del Dottorato di ricerca in Informatica ed Ingegneria dell'Informazione, dal 23-09-2015 al 06-10-2015.

- Partecipazione al Collegio 2016: Titolo: "INFORMATICA E INGEGNERIA DELL' INFORMAZIONE". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2016/17 - Ciclo: XXXII - Durata: 3 anni, dal 07-04-2016 al 31-10-2019.

- Partecipazione al Collegio 2017: Titolo: "INFORMATICA E INGEGNERIA DELL' INFORMAZIONE". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2017/18 - Ciclo: XXXIII - Durata: 3 anni, dal 25-05-2017 al 31-10-2020

- Partecipazione al Collegio 2018: Titolo: "INFORMATICA". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2018/19 - Ciclo: XXXIV - Durata: 3 anni, dal 13-03-2018 al 31-10-2021

- Partecipazione al Collegio 2019: Titolo: "INFORMATICA". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2019/20 - Ciclo: XXXV - Durata: 3 anni, dal 10-04-2019

- Partecipazione al Collegio 2020: Titolo: "INFORMATICA". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2020/21 - Ciclo: XXXVI - Durata: 3 anni, dal 17-04-2020

- Partecipazione al Collegio 2021: Titolo: "INFORMATICA". Ateneo proponente: Università degli Studi di Salerno. Anno accademico di inizio: 2021/22 - Ciclo: XXXVII - Durata: 3 anni, dal 21-03-2021

16 Commissioni e Tutoraggio

- È stato **tutor** della dottoressa *Zahra Ebadi Ansaroudi*, che ha conseguito il Dottorato in Informatica, ciclo XXXIV, presso l'Università di Salerno, in data 23-05-2022.
- Per il biennio 2016-2017 è stato membro della **Commissione Nazionale** per la conferma in ruolo dei ricercatori universitari, relativamente al settore scientifico disciplinare INF01.
- Nel Dicembre 2015 è stato **presidente della commissione** per l'assegnazione del Ph.D al candidato Matteo Signorini, presso l'Universidad Pompeu Fabra, Barcellona, Spagna. Tesi difesa il 10 Dicembre 2015 a Barcellona.
- Dal 2008 al 2012 è stato membro della Commissione Scientifica dell'Ateneo Salernitano per l'Area 01 (Comitato d'area di Scienze Matematiche e Informatiche) per la valutazione dei progetti FARB.
- Dal 2008 al 2013 è stato membro della Commissione della Facoltà di Scienze Matematiche Fisiche e Naturali per il supporto alla disabilità.
- Dal 2014 è membro delle commissioni dipartimentali per la razionalizzazione spazi e per i test di ingresso.
- Dal 2016 è membro della commissione dipartimentale per la valutazione dei progetti FARB.
- Ha seguito, in qualità di relatore, dal 2005 ad oggi più di settanta tesisti. Inoltre, dalla stessa data, è tutor dipartimentale per il programma Erasmus.

17 Lavoro di Referaggio

- Ha svolto revisioni di lavori per le seguenti riviste (principali): 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 e Mathematical Cryptology.

- Ha svolto revisioni di lavori per le seguenti conferenze e workshop (principali, non coinvolto come membro del comitato di programma): 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.

- Ha recensito, in qualità di esperto internazionale, la Tesi di Ph.D. (conseguito nel 2004 presso l'Universitat Politècnica de Catalunya (Spagna)) della Dr.ssa Vanessa Daza, per l'assegnazione di un premio da parte del ministero della ricerca scientifica spagnolo.

- Da Gennaio 2005 è revisore esterno per conto del *Research Grants Council* (RGC) di Hong Kong. Tale organismo è la principale fonte di finanziamento pubblico a supporto della ricerca accademica in Hong Kong. In media recensisce due proposte progettuali all'anno.

- Ha recensito a Settembre 2009, in qualità di revisore esterno, la Tesi di Ph.D di Leonor Vazquez Gonzalez, Universitat Politècnica de Catalunya (Spagna).

18 Attività di Ricerca

I suoi interessi di ricerca principali sono la crittografia ed, in parte, gli algoritmi e la sicurezza dei dati. In particolare, nel corso degli anni ha lavorato sulle tematiche brevemente descritte di seguito.

Visual Cryptography. La crittografia visuale è una tecnica di cifratura per immagini in cui l'*operazione di decifratura* richiede soltanto l'uso dell'*occhio umano*. Pertanto, ha il vantaggio di essere fruibile anche da persone che *non* dispongono di dispositivi di calcolo e di conoscenze crittografiche.

Nel modello di base, un'immagine in bianco e nero viene decomposta/cifrata in due immagini, dette *share*, che singolarmente appaiono come *collezioni casuali* di punti. Una soltanto delle due share non fornisce alcuna informazione sull'immagine cifrata. D'altra parte, le due share, stampate su dei lucidi, sovrapposte e perfettamente allineate, riproducono l'immagine di partenza.

Diverse estensioni del modello di base sono state studiate sino ad oggi. Per esempio, negli *schemi a soglia* l'immagine segreta è decomposta in n share, e solo quando k di esse vengono sovrapposte l'immagine segreta viene ricostruita. La sovrapposizione di un numero inferiore di share non dà alcuna informazione sull'immagine segreta.

Negli *schemi per strutture d'accesso generali*, invece di una *soglia* che abilita alla ricostruzione dell'immagine segreta, esiste una *specifica* degli insiemi di immagini cifrate che rendono possibile la ricostruzione. Tale specifica è detta *struttura d'accesso*.

Negli *schemi estesi* le share non si presentano come semplici collezioni casuali di punti ma sono immagini *significative* e.g., una casa, un albero, etc.

Infine, sono stati proposti vari modelli e costruzioni, che permettono di cifrare immagini a colori o in toni di grigio, piuttosto che semplici immagini in bianco e nero e sono state studiati modelli alternativi (e.g., probabilistico, random grid) al modello deterministico.

Il miglioramento della *qualità visiva* delle immagini segrete che vengono ricostruite e l'individuazione di *ambiti applicativi* in cui le caratteristiche di questa tecnica possano essere utili sono i maggiori obiettivi che la ricerca cerca di perseguire in questa area. Lavori: Tesi di Laurea e [24, 39, 40, 9, 6, 38, 37].

Key Distribution. Un gruppo di utenti di una rete che vuole comunicare riservatamente e, per ragioni di *efficienza*, decide di utilizzare algoritmi *simmetrici* piuttosto che algoritmi a chiave pubblica, necessita di *chiavi crittografiche comuni* per cifrare, decifrare e autenticare i messaggi che gli utenti si scambiano. Occorre, allora, un protocollo per *fornire le chiavi* ad ogni utente del gruppo.

In modelli tradizionali di reti di comunicazione, la distribuzione delle chiavi viene effettuata da un server, chiamato *Key Distribution Center* (KDC), che implementa uno schema di distribuzione, detto *Key Distribution Scheme* (KDS). La struttura dello schema dipende da molteplici fattori. Se il server lavora on-line, solitamente è prevista interazione tra gli utenti ed il server. Se, invece, il server è off-line, lo schema prevede due fasi: una fase di inizializzazione, in cui il server è attivo e distribuisce privatamente informazioni ai singoli utenti della rete, ed una fase di calcolo delle chiavi comuni, che può richiedere o meno interazione tra gli utenti, ed è basata sulle informazioni private ricevute in fase di inizializzazione dagli utenti.

Un approccio alternativo consiste nella realizzazione di un *centro distribuito*. Precisamente, un Distributed Key Distribution Center (DKDC) è un insieme di n server che in *modo congiunto* realizza la stessa funzione di un KDC. In questo ambiente, un utente che necessita di una chiave comune, invia una richiesta ad un sottoinsieme degli n server. Elaborando le risposte ricevute dai server interrogati, l'utente è in grado di calcolare la chiave. I vantaggi principali associati a questo approccio sono: nessun server da solo conosce le chiavi; gli utenti possono inviare richieste a server diversi, con conseguente distribuzione del traffico nel sistema; le richieste possono essere inviate in parallelo, senza alcuna perdita in tempo rispetto ad un ambiente centralizzato. Infine, il centro mantiene la propria funzionalità anche in presenza della rottura o indisponibilità di pochi server.

L'attività di ricerca in questo campo è stata incentrata essenzialmente sulla modellizzazione, sulla realizzazione e sull'analisi di schemi efficienti e sicuri per DKDC. Lavori: Tesi di Dottorato e [26, 62, 64, 61, 60, 55, 23, 20, 65, 19, 16].

Broadcast Encryption. Lo sviluppo di applicazioni che richiedono trasferimenti di grosse quantità di dati da una entità trasmittente ad un insieme più o meno ampio di entità riceventi (e.g., pay-per-view TV, distribuzione di contenuti tramite CD, DVD, HD-DVD, etc), in gergo dette applicazioni *broadcast*, ha richiesto lo studio di speciali protocolli che assicurino la sicurezza delle trasmissioni in questo scenario. Fondamentalmente, un *broadcast encryption scheme* (BES) permette ad un sottoinsieme privilegiato di riceventi ed all'unità trasmittente di stabilire chiavi comuni con cui cifrare, e quindi proteggere, la comunicazione rispetto agli utenti non autorizzati della rete. I parametri che vengono utilizzati per valutare l'efficienza di tali schemi sono: complessità di comunicazione per stabilire una chiave comune, quantità di memoria richiesta dallo schema

all'entità trasmittente e alle unità riceventi, ed efficienza delle computazioni. La ricerca è stata incentrata sulla individuazione di schemi efficienti e sicuri. L'attenzione è stata anche posta sul disegno di schemi che funzionino in presenza di rotture parziali della rete e di perdite di pacchetti e su schemi che risultano robusti rispetto a specifiche tipologie di attacco non considerate da modelli passati. Lavori: [52, 53, 51, 21, 50, 14, 48, 43, 10, 5, 34].

Anonymous Communication. In tutte le sue forme, la *privacy* è diventata una questione imprescindibile all'interno di ogni riflessione sull'ICT. Molteplici eventi negli ultimi anni, quali *Wikileaks* e l'affare *Snowden*, per citarne alcuni, hanno mostrato che le autorità hanno accesso a chiamate telefoniche, e-mail e ad altri mezzi di comunicazione, ben oltre i limiti imposti dalle costituzioni nazionali. In generale, entità avverse, per svariate ragioni, possono tracciare o costruire un profilo dell'utente e dei suoi comportamenti. Attacchi di questo tipo sono una minaccia concreta alla libertà degli individui. È, pertanto, necessario individuare metodi per garantire la privacy dell'utente e protocolli che permettano *computazioni e comunicazioni anonime*. Alcune nozioni generali e metodi efficienti per costruire applicazioni che preservano la privacy e garantiscono l'anonimato sono state introdotte in letteratura. Ma molte questioni e, sopratutto, protocolli efficienti sono ancora una sfida aperta. Lavori: [63, 39, 8, 7]

Private Information Retrieval. Un aspetto estremamente importante inerente alla protezione della privacy degli utenti in reti di comunicazione riguarda il *recupero di informazioni* da database pubblici. Infatti, un gestore curioso di un database potrebbe osservare le richieste/letture che l'utente effettua, in modo da carpirne interessi e bisogni. Per percepire la natura dei problemi che questa operazione comporta, si pensi ad un database contenente informazioni aggiornate su malattie terminali e che il gestore sia intenzionato a vendere le proprie osservazioni a compagnie assicurative.

Uno schema per Private Information Retrieval (PIR) permette all'utente di recuperare informazione *privatamente* rispetto al gestore del database. Enfasi in questo settore di ricerca viene posta sulla realizzazione di schemi PIR efficienti dal punto di vista della *complessità di comunicazione*. L'esigenza di privacy impone, infatti, limitazioni non banali ai costi dell'interazione utente-database. Lavori: [25].

Oblivious Transfer. L'Oblivious Transfer è uno dei concetti più interessanti e fecondi introdotti nella ricerca crittografica. Brevemente può essere descritto come segue: un trasmittente possiede *alcune* informazioni, ed una ricevente è interessata in *una* di esse. Il trasmittente vuole rilasciare l'informazione che la ricevente desidera, ma *solo e solo* quella. D'altra parte, la ricevente non vuole che il trasmittente sappia a *quale* delle sue informazioni ella è interessata. Un protocollo che realizza questo trasferimento asimmetrico di conoscenza viene detto *oblivious transfer* (OT). Da un punto di vista teorico, avere un protocollo che realizza l'OT significa avere la possibilità di risolvere *moltissimi* problemi di computazione sicura in presenza di più parti i.e., Multi-Party Computation (MPC). Precisamente, l'OT è una *primitiva completa* per SFE (Secure Function Evaluation). Da un punto di vista pratico, molti protocolli disegnati per risolvere problemi specifici, che non fanno uso delle soluzioni generali per MPC, implementano una qualche forma di oblivious transfer.

Obiettivo principale della ricerca in questo ambito è trovare implementazioni nuove

o con particolari proprietà, efficienti e sicure di questa primitiva crittografica. Lavori: [58, 24, 13].

Proactive Password Checking. Uno dei meccanismi più semplici ed usati per proteggere l'accesso a risorse condivise è il meccanismo delle *password*. Solitamente, in sistemi in cui l'accesso è protetto da una password, un'informazione predefinita viene cifrata usando come chiave crittografica la password ed, eventualmente, informazioni aggiuntive, e viene mantenuta su qualche dispositivo di memorizzazione del sistema. Quando l'utente ha necessità di accedere alle risorse, il sistema di protezione chiede all'utente la password, ricalcola la cifratura dell'informazione predefinita e controlla che la cifratura ottenuta coincida con la cifratura memorizzata. La password garantisce, quindi, che l'utente che richiede l'uso della risorsa sia effettivamente l'utente reale (i.e., garantisce l'identificazione e l'autenticazione dell'utente).

Purtroppo, il meccanismo delle password è anche uno dei punti di attacco principali che gli hacker scelgono per guadagnare l'accesso a sistemi o a risorse riservate.

L'attività di ricerca è stata volta principalmente all'analisi del modello delle password e alla proposta di approcci e soluzioni che, pur mantenendo il modello di protezione delle password, ne rafforzassero la sicurezza. Lavori: [22, 56, 59, 15].

Secret Sharing. Uno schema per la condivisione dei segreti (secret sharing scheme) abilita una entità, detta *dealer*, a condividere un segreto tra un insieme di partecipanti. Precisamente, il dealer distribuisce riservatamente informazioni, dette share, ad ognuno dei partecipanti. Successivamente, alcuni sottoinsiemi di partecipanti, usando le share ricevute dal dealer, ricostruiscono il segreto; altri, dall'analisi delle share disponibili, non ottengono alcuna informazione sul segreto. La crittografia visuale descritta in precedenza è una forma visuale di secret sharing.

Un problema importante che è stato per anni oggetto di attenzione negli studi sugli schemi per la condivisione di segreti è il problema della presenza di partecipanti scorretti, in gergo detto problema del *cheating*, che possono fornire, in fase di ricostruzione del segreto, share false che portano alla ricostruzione di un segreto differente da quello originale. Successivamente, questi partecipanti, da tale segreto e dalle share originali, potrebbero essere gli unici a carpire informazioni (eventualmente ricostruire) sul segreto originario.

Schemi che sono intrinsecamente in grado di far fronte a tale problema sono detti *cheating-immune*. In parole povere, in uno schema di questo tipo, partecipanti disonesti, nel sottomettere share corrotte, non hanno alcun vantaggio rispetto a partecipanti onesti. Tale approccio al disegno di schemi per la condivisione di segreti è stato oggetto di attenta investigazione.

In lavori più recenti attenzione è stata, invece, rivolta a modelli di secret sharing più generali: modelli in cui la ricostruzione è *probabilistica* e modelli in cui l'insieme dei partecipanti è dinamico, cresce nel tempo, ed è *potenzialmente infinito*. Lavori: [54, 17, 35, 33, 3].

Public-Key Cryptography and Chaos Theory. Un trend corrente nelle ricerche crittografiche è rinvenibile nel tentativo di trovare *nuove assunzioni e problemi matematici difficili* che possano essere usati per implementazioni efficienti e sicure di primitive crittografiche. In particolare, la teoria del Caos è stata oggetto di notevole attenzione negli

ultimi anni. Infatti, diversi modelli caotici presentano proprietà quali comportamento aleatorio ed estrema sensibilità alle condizioni iniziali, che risultano utili in crittografia.

I polinomi di Chebyshev, per esempio, sono stati usati nel disegno di sistemi di crittografia a chiave pubblica. Questi polinomi soddisfano una proprietà di semigruppo, che rende possibile l'implementazione di una funzione con trapdoor e, quindi, della crittografia a chiave pubblica.

Nella nostra attività di ricerca abbiamo studiato alcune primitive crittografiche basate su di essi: un crittosistema a chiave pubblica, uno schema di firma digitale, uno schema di accordo su chiavi segrete, ed uno schema di autenticazione. La nostra analisi ha mostrato che, seppur efficienti e basate su un'idea interessante e nuova, tutte le realizzazioni delle precedenti primitive sono *insicure*. Abbiamo mostrato che esiste un attacco efficiente e realistico che può essere usato per rompere gli schemi proposti e alcune possibili generalizzazioni basate su meccanismi simili. Lavori: [18].

RFID Technology. Negli ultimi anni le tecniche RFID (Radio-Frequency Identification) di identificazione automatica di oggetti hanno avuto uno sviluppo pervasivo della società e del mercato. I tag RFID, piccole etichette dotate di microchip e di antenna, memorizzano informazioni relative agli oggetti a cui sono attaccate (e.g., categoria d'appartenenza, proprietà , identificativo, ...). Essi interagiscono con i reader, dispositivi in grado di leggerne il contenuto a distanza e, quindi, di identificare gli oggetti a cui i tag sono fisicamente associati (spesso incollati).

Purtroppo, i tag possono esser letti da qualsiasi dispositivo che abbia le capacità di un reader. Sono, quindi, possibili diversi attacchi che minano la privacy dell'utente in possesso di oggetti muniti di tag (e.g, profiling degli interessi personali, tracciamento degli spostamenti ...). Inoltre i tag possono essere facilmente clonati e contraffatti.

Alla base di tutto ciò è rinvenibile un problema ben noto in crittografia: il problema dell'identificazione e dell'autenticazione. Far cioè in modo che il contenuto di un tag possa esser letto soltanto da reader autorizzati e, d'altro canto, che i reader autorizzati possano distinguere tra tag autentici e tag contraffatti.

La ricerca è stata incentrata sia sulla modellizzazione delle proprietà che uno schema di autenticazione RFID deve esibire, sia sulla realizzazione che sulla (critto)-analisi di protocolli efficienti, che possano essere usati vantaggiosamente nelle applicazioni. Particolare attenzione è stata posta sui protocolli leggeri ed ultraleggeri. Lavori: [49, 46, 47, 11, 36, 44, 32, 31, 30, 66].

Access Control. Il controllo dell'accesso a risorse condivise è un problema di base nella realizzazione di un sistema sicuro. Diversi approcci sono stati perseguiti in letteratura. Uno di questi è basato sull'uso di chiavi crittografiche. Più precisamente, ogni risorsa è protetta/cifrata attraverso una chiave, e solo gli utenti che dispongono di una copia della chiave possono accedere ad essa. Uno *schema di assegnamento di chiavi crittografiche* fornisce ad ogni utente *tutte e sole* le chiavi che abilitano all'accesso alle risorse a cui ha diritto. Molto spesso gli utenti e le risorse di un sistema sottostanno ad una organizzazione di tipo gerarchico e possono pertanto essere rappresentati attraverso strutture parzialmente ordinate. Akl and Taylor nel 1983 furono i primi a suggerire l'uso di tecniche crittografiche per garantire il controllo dell'accesso in strutture gerarchiche. Da allora diversi schemi sono stati proposti al fine di ottenere un controllo efficiente e sicuro. D'altra parte è stato mostrato che molti di essi non raggiungono i requisiti

per cui sono stati realizzati. Schemi di assegnamento di chiavi in strutture gerarchiche sono inoltre anche stati usati come primitive o blocchi di base nella realizzazione di protocolli più complessi o pensati per problemi diversi. La ricerca è stata incentrata sulla progettazione e l'analisi di schemi flessibili, sicuri ed efficienti. Lavori: [45,12]

Two-party Computation. Le tecniche generali per computazioni sicure tra due parti si basano in larga misura sulla costruzione circuitale di Yao, proposta negli anni 80 ed usata ampiamente successivamente. Oggi, a seguito di ottimizzazioni di vario tipo e della crescita delle capacità computazionali dei dispositivi, è nuovamente al centro delle attenzioni. Nuove primitive crittografiche ed applicazioni che ne fanno uso sono state recentemente proposte. Per problemi specifici, d'altra parte, per ragioni di efficienza, piuttosto che far uso delle tecniche generali spesso si individuano costruzioni ad-hoc, che possano essere utili per classi di problemi che condividono caratteristiche comuni. Uno di questi è il problema del calcolo sicuro dell'intersezione (e funzioni simili) tra due insiemi di valori, uno posseduto dalla prima parte, e l'altro dalla seconda. Date le ricadute importanti in diversi ambiti applicativi (e.g., computazioni su dati genomici sicure) il problema ha ricevuto notevole attenzione dalla comunità scientifica. Lavori: [42, 4]

Blockchain. Il concetto di blockchain, dalla sua introduzione ed uso nel protocollo Bitcoin in poi, ha ricevuto un'attenzione spasmodica: in parole povere, si tratta di una catena di blocchi di dati che realizza un libro mastro (ledger) pubblico, distribuito, resistente a tentativi di contraffazione, mantenuto e replicato interamente e consistentemente da una rete peer-to-peer, debolmente sincronizzata, di nodi anonimi, non autenticati e potenzialmente non fidati. Varianti diverse del concetto sono state proposte per aumentare l'efficienza nell'uso delle risorse e per fornire supporto alla progettazione di applicazioni nel nuovo ecosistema computazionale (e.g., programmabilità della blockchain, introduzione degli smart contract). Problemi fondamentali nelle blockchain realizzate sul modello della blockchain di Bitcoin sono l'inefficienza energentica del metodo di estensione del ledger, basato su proof-of-work, e il basso numero di transazioni per secondo supportate. Sono stati oggetto di attenzione. Lavori: [28, 29] e il draft della ricerca completa disponibile in archivio https://eprint.iacr.org/2020/1262 (e sottomesso per pubblicazione).

19 Elenco delle Pubblicazioni

Riviste Internazionali

1. Z. Ebadi Ansaroudi, R. Zaccagnino e 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 e 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, e R. Steinwandt.
Private Set Intersection: New Generic Constructions and Feasability Results.
Advances in Mathematics of Communications, pp. 481 - 502, Vol. 11, N. 3, Agosto 2017.

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

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

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

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

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

10. P. D'Arco e 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 e 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 e 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, e D. R. Stinson.
On Unconditionally Secure Distributed Oblivious Transfer.
Journal of Cryptology, Vol. 20, N. 3, pp. 323–375, 2007.

14. C. Blundo, P. D'Arco, e 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, e 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, e 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 e 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 e 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, e 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 e 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 e C. Padrò.
A Ramp Model for Distributed Key Distribution Schemes.
Discrete Applied Mathematics, Vol. 128, pp. 47–64, 2003.

24. C. Blundo, P. D'Arco, A. De Santis e D. R. Stinson.
Contrast Optimal Threshold Visual Cryptography Schemes.
SIAM Journal on Discrete Mathematics, Vol. 16, pp. 224 – 261, 2003.

25. C. Blundo, P. D'Arco e A. De Santis.
A t-Private k-Database Information Retrieval Scheme.
International Journal of Information Security, Vol. 1, pp. 64–68, 2001.

26. C. Blundo, P. D'Arco e A. Giorgio Gaggia.
A τ-restricted key agreement scheme.
The Computer Journal, Vol. 42, pp. 51–61, 1999.

Conferenze Internazionali

27. P. D'Arco e A. De Santis.
Private computations on set intersection.
Sottomesso per pubblicazione, 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 e 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 e 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 e 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.
Proceedings 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.
Proceedings 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.
Proceedings 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.
Proceedings of MFCS2018, Vol. 117, pp.1-16, 2018.

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

37. P. D'Arco, R. De Prisco e 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 e 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. XXXX, pp. X-X, Springer Verlag, 201X.

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

42. P. D'Arco, M. I. Gonzalez Vasco, A. L. Perez del Pozo, e 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 e 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.

44. 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.

45. P. D'Arco, A. De Santis, A. L. Ferrara e B. Masucci.
Security and Tradeoffs of the Akl-Taylor Scheme and Its Variants.

Proceedings del 34th International Symposium on Mathematical Foundations of Computer Science - MFCS 2009, Lecture Notes in Computer Science, Vol. 5734, pp. 247257, 2009.

46. P. D'Arco, A. Scafuro e I. Visconti.
Revisiting DoS Attacks and Privacy in RFID-Enabled Networks .
Proceedings del 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks, (Algosensor 2009), Lecture Notes in Computer Science. Vol. 5304, pp. 7687, 2009.

47. P. D'Arco, A. Scafuro e I. Visconti.
Semi-Destructive Privacy in RFID Systems. Proceedings del 5-th Workshop on RFID Security (RFIDSec '09), 30 Giugno - 2 Luglio 2009, Leuven, Belgio.

48. P. D'Arco e A. De Santis.
Optimising SD and LSD in presence of non-uniform probabilities of revocation.
Proceedings della International Conference on Information Theoretic Security (ICITS 2007), Lecture Notes in Computer Science, Vol. 4883, pp. 46–64, 2009.

49. P. D'Arco e 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.

50. C. Blundo, P. D'Arco, e A. De Santis.
Definitions and Bounds for Self-healing Key Distribution.
Proceedings del 31st International Colloquium on Automata, Languages, and Programming (ICALP 2004), Lecture Notes in Computer Science, Vol. 3142, pp. 234-246, Springer-Verlag, 2004.

51. C. Blundo, P. D'Arco, e M. Listo.
A New Self-healing Key Distribution Scheme.
Proceedings dell'IEEE Symposium on Computers and Communications (ISCC 2003), pp. 803-808, 2003.

52. P. D'Arco e D. Stinson.
Fault Tolerant and Distributed Broadcast Encryption.
Proceedings della Cryptographers' Track RSA Conference 2003 (CT-RSA 2003), Lecture Notes in Computer Science, Vol. 2612, pp. 262-279, Springer Verlag, 2003.

53. C. Blundo, P. D'Arco e M. Listo.
A Flaw in a Self-Healing Key Distribution Scheme.
Proceedings del 2003 IEEE Information Theory Workshop (ITW '03), pp. 163-166, 2003.

54. P. D'Arco, W. Kishimoto, e D. Stinson.
On Cheating-Immune Secret Sharing.
Proceedings dell' International Workshop on Coding and Cryptography (WCC 2003), pp. 111-120, 2003.

55. P. D'Arco e D. Stinson.
On Unconditionally Secure Distributed Key Distribution Centers.
Proceedings di ASIACRYPT 2002, Lecture Notes in Computer Science, Vol. 2501, pp. 346-363, Springer Verlag, 2002.

56. C. Blundo, P. D'Arco, A. De Santis e C. Galdi.
A Novel Approach to Proactive Password Checking.
Proceedings della *Infrastructure Security Conference* (INFRASEC 2002), Lecture Notes in Computer Science, Vol. 2437, pp.30–39, Springer Verlag, 2002.

57. C. Blundo, P. D'Arco, A. De Santis e D. Stinson.
New Results on Unconditionally Secure Distributed Oblivious Transfer.
Proceedings di *Selected Areas in Cryptography* (SAC 2002), Lecture Notes in Computer Science, Vol. 2595, pp. 291-309, Springer Verlag, 2003.

58. P. D'Arco e D. Stinson.
Generalized Zig-zag Functions and Oblivious Transfer Reductions.
Proceedings di *Selected Areas in Cryptography* (SAC2001), Lecture Notes in Computer Science, Vol. 2259, pp. 87-102, Springer Verlag, 2002.

59. C. Blundo, P. D'Arco, A. De Santis e C. Galdi.
Hyppocrates: A New Proactive Password Checker.
Proceedings della *Information Security Conference* (ISC 2001), Lecture Notes in Computer Science, Vol. 2200, pp. 63–80, Springer Verlag, 2001.

60. C. Blundo, P. D'Arco V. Daza e C. Padrò.
Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures.
Proceedings della *Information Security Conference* (ISC 2001), Lecture Notes in Computer Science, Vol. 2200, pp. 1–17, Springer Verlag, 2001.

61. C. Blundo, P. D'Arco e C. Padrò.
A Ramp Model for Distributed Key Distribution Schemes.
Proceedings del *International Workshop on Coding and Cryptography (WCC2001)*, pp. 93–102, 2001.

62. C. Blundo e P. D'Arco.
An Information Theoretic Model for Distributed Key Distribution.
Proceedings del *IEEE International Symposium on Information Theory (ISIT2000)*, p. 267, 2000.

Conferenze Nazionali

63. S. Cimato, P. D'Arco, e I. Visconti.
Anonymous Group Communication for Mobile Networks.
Proceedings della Italian Conference on Theoretical Computer Science (ICTCS 2003), Lecture Notes in Computer Science, Vol. 2814, pp. 316–328, Springer-Verlag, 2003

64. P. D'Arco.
On the Distribution of a Key Distribution Center.

Proceedings della Italian Conference on Theoretical Computer Science (ICTCS 2001), Lecture Notes in Computer Science, Vol. 2202, pp. 357–369, Springer Verlag, 2001.

Capitoli di libri

65. C. Blundo e P. D'Arco.
The Key Establishment Problem.
FOSAD02, Lecture Notes in Computer Science (Tutorial), Vol. 2946, pp. 44–90, Springer-Verlag, 2004.

66. X. Carpenter, P. D'Arco e R. De Prisco.
Ultra-lightweight Authentication.
Nel volume *Security of Ubiquitous Computing Systems*, ISBN 978-3-030-10591-4, 2021.

Traduzioni di libri

67. *Introduzione alla teoria della computazione* di Michael Sipser, Maggioli Editore, 2016. Edizione italiana a cura di Clelia De Felice, Luisa Gargano e Paolo D'Arco.

Prefazioni a libri

68. Prologo a *Criptografia esencial. Principios basicos para el diseno de esquemas y protocolos seguros* di Maria Isabel Gonzalez Vasco e Angel Luis Perez del Pozo, Ra-Ma editore, 2021. Testo introduttivo alla Crittografia, ad uso di Ingegneri Informatici in Università spagnole.

Luogo e Data: Salerno, 2 Maggio 2023.