UNIVERSITÀ DEGLI STUDI DI MILANO
Procedura di valutazione per la chiamata a professore I fascia da ricoprire ai sensi dell'art. 24, comma 6, della Legge n. 240/2010 per il settore concorsuale 01/B1-Informatica (settore scientifico-disciplinare INF/01-Informatica) presso il Dipartimento di Informatica Giovanni Degli Antoni, Codice concorso 4927.

Curriculum vitae
Valentina Ciriani

Indice

1 Informazioni personali

Cognome: Ciriani

Nome: Valentina

Data e luogo di nascita: 19 gennaio 1974, Pisa

Indirizzo: Dipartimento di Informatica "Giovanni Degli Antoni"
Università degli Studi di Milano,
Via Celoria, 18 - 20133 Milano (MI)

Telefono: 02 503 16257

E-mail: valentina.ciriani@unimi.it

URL: http://www.di.unimi.it/ciriani

2 Formazione e stato di servizio

2.1 Formazione universitaria

luglio 1998. Ha conseguito la *Laurea* con lode in Informatica (5 anni) presso l'Università di Pisa, discutendo la tesi "Hash su grafi e confronto tra sequenze", relatore Prof. F. Luccio.

marzo 2003. Ha conseguito il titolo di *Dottore di Ricerca in Informatica*, presso l'Università di Pisa, con la tesi "Three-Level Logic Synthesis: Algebraic Approach and Minimization Algorithms", advisor: Prof. F. Luccio.

2.2 Stato di servizio

Posizione attuale

Il primo marzo 2015 ha preso servizio come *Professore di II Fascia* S.S.D. INF01 presso il Dipartimento di Informatica "Giovanni Degli Antoni" dell'Università degli Studi di Milano.

Abilitazioni

gennaio 2014. Ha conseguito l'abilitazione scientifica nazionale a *Professore di II Fascia* per il settore concorsuale 01/B1.

gennaio 2020. Ha conseguito l'abilitazione scientifica nazionale a *Professore di I Fascia* per il settore concorsuale 01/B1.

Posizioni ricoperte

gennaio 2003 – febbraio 2003. È stata titolare di *contratto di ricerca* nell'ambito del progetto "Indicizzazione, compressione e ricerca per grandi insiemi di dati" presso il Dipartimento di Informatica dell'Università di Pisa.

marzo 2003 – dicembre 2004. È stata titolare di un *assegno di ricerca* in Informatica presso il Dipartimento di Informatica dell'Università di Pisa.

gennaio 2005 – febbraio 2015. È stata *Ricercatore* S.S.D. INF01 – Informatica (confermata il 3 gennaio 2008) presso il Dipartimento di Tecnologie dell'Informazione dell'Università degli Studi di Milano - sede di Crema.

3 Attività di ricerca e titoli scientifici

3.1 Partecipazione a comitati editoriali di riviste

- Dal luglio 2019 è Associate Editor (Editorial Board Member) della rivista Elsevier "Microprocessors and Microsystems - Embedded Hardware Design". ISSN: 0141-933. La rivista è indicizzata sia da Scopus che da WOS.

3.2 Organizzazione di conferenze scientifiche

1. È program chair del *International Workshop on Logic and Synthesis, IWLS 2022*, San Francisco, CA (US).
2. È stata program chair della Special Section "Emerging technologies and circuit synthesis (ETCS)" della conferenza *Euromicro Conference on Digital System Design, DSD 2015*, Funchal, Madeira, Portogallo.
3. È stata program co-chair per il track "Logic Synthesis and Timing Analysis" della conferenza *Design, Automation and Test in Europe, DATE 2014*, Dresden, Germania.
4. È stata program chair della Special Section "Emerging technologies and circuit synthesis (ETCS)" della conferenza *Euromicro Conference on Digital System Design, DSD 2014*, Verona, Italia.
5. È stata promotrice, organizzatrice e program chair delle *Giornate Nazionali di Sintesi Logica*, GNSL:
    - Prima Giornata Nazionale di Sintesi Logica, 25 giugno 2005, Dipartimento di Tecnologie dell'Informazione, Crema, Università degli Studi di Milano.
    - Seconda Giornata Nazionale di Sintesi Logica, 15 giugno 2006, Dipartimento di Informatica, Università di Pisa.
    - Terza Giornata Nazionale di Sintesi Logica, 21 giugno 2007, Dipartimento di Informatica, Università degli Studi di Verona.
    - Quarta Giornata Nazionale di Sintesi Logica, 30 giugno 2008, Dipartimento di Elettronica ed Informazione, Politecnico di Milano.
    - Quinta Giornata Nazionale di Sintesi Logica, 10 giugno 2009, Dipartimento di Informatica, Università di Pisa.
    - Sesta Giornata Nazionale di Sintesi Logica, 23 giugno 2010, Dipartimento di Informatica, Università di Roma "La Sapienza".
    - Settima Giornata Nazionale di Sintesi Logica, 21 giugno 2011, Dipartimento di Tecnologie dell'Informazione, Crema, Università degli Studi di Milano.
    - Ottava Giornata Nazionale di Sintesi Logica, 4 luglio 2012, Dipartimento di Fisica, Milano, Università degli Studi di Milano.
    - Nona Giornata Nazionale di Sintesi Logica, 20 giugno 2013, Dipartimento di Automatica e Informatica, Torino, Politecnico di Torino.
    - Decima Giornata Nazionale di Sintesi Logica, 29 agosto 2014, Dipartimento di Informatica, Verona, Università degli Studi di Verona.
    - Undicesima Giornata Nazionale di Sintesi Logica, 25 giugno 2015, Dipartimento di Informatica, Roma, Università di Roma, La Sapienza.
    - Dodicesima Giornata Nazionale di Sintesi Logica, 5 luglio 2016, Dipartimento di Informatica, Pisa, Università di Pisa.
    - Tredicesima Giornata Nazionale di Sintesi Logica, 22 giugno 2017, Dipartimento di Informatica, Crema, Università degli Studi di Milano.

3.3 Membro di comitati di programma

1. È stata membro del comitato di programma della conferenza PSAI 2008, *Workshop on Privacy and Security by means of Artificial Intelligence*, 4-7 marzo 2008, Barcellona Spagna.
2. È stata membro del comitato di programma della conferenza *Euromicro Conference on Digital System Design* (Special Session Logic Synthesis Hot Anew), 27-29 agosto 2009, Patras Grecia.
3. È stata membro del comitato di programma della conferenza *Workshop on Data Privacy Management (DPM)*, 24 settembre 2009, Saint Malo, Francia.
4. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 8-12 marzo 2010, Dresden, Germania.
5. È stata membro del comitato di programma della conferenza *Workshop on Privacy and Security by means of Artificial Intelligence*, 15-18 febbraio 2010, Krakow, Polonia.
6. È stata membro del comitato di programma della conferenza *Data Privacy Management (DPM)*, 23 settembre 2010, Atene, Grecia.
7. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 14-18 marzo 2011, Grenoble, Francia.
8. È stata membro del comitato di programma della conferenza 1st International *Workshop on Model-Based and Policy-Based Engineering in Information Security (MPEIS)* special section di ICETE, 18-21 luglio 2011, Seville, Spagna.
9. È stata membro del comitato di programma della conferenza *Data Privacy Management (DPM)*, 15-16 settembre 2011, Leuven, Belgio.
10. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE*), 12-16 marzo 2012, Dresden, Germania.
11. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 18-22 marzo 2013, Grenoble, Francia.
12. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 24-28 marzo 2014, Dresden, Germania.
13. È stata membro del comitato di programma della conferenza *Euromicro Conference on Digital System Design DSD* (Emerging technologies and circuit synthesis (ETCS)), 27-29 agosto 2014, Verona, Italy.
14. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 9-13 marzo 2015, Grenoble, Francia.
15. È stata membro del comitato di programma della conferenza *Euromicro Conference on Digital System Design DSD* (Emerging technologies and circuit synthesis (ETCS)), 26-28 agosto 2015, Funchal, Madeira, Portugal.
16. È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 14-18 marzo 2016, Dresden, Germania.
17. È stata membro del comitato di programma della conferenza *International Workshop on Boolean Problems (IWSBP)*, 19-21 settembre 2018, Bremen, Germania.
18. È stata membro del comitato di programma della conferenza DSD Euromicro special session *Future Trends in Emerging Technologies (FTET)*, 29-31 agosto 2018, Prague, Repubblica Ceca.

19. È stata membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 20-22 giugno 2018, Barcelona, Spagna.
20. È stata membro del comitato di programma della conferenza *Reed-Muller 2019 Workshop (RM2019)*, 23-24 maggio 2019, Bremen, Germania.
21. È stata membro del comitato di programma della conferenza DSD Euromicro special session *Future Trends in Emerging Technologies (FTET)*, 28-30 agosto 2019, Kallithea, Grecia.
22. È stata membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 22-24 maggio 2019, Amsterdam, Olanda.
23. È stata membro del comitato di programma della conferenza *Design Automation Conference* (DAC), Late Breaking Results, 19-23 luglio 2020 San Francisco, CA (US).
24. È stata membro del comitato di programma della conferenza *EEE International Conference on Electrical Engineering and Electronics*, 13-15 agosto 2020, Prague, Repubblica Ceca.
25. È stata membro del comitato di programma della conferenza DSD Euromicro special session *Future Trends in Emerging Technologies (FTET)*, 26-28 agosto 2020, Portorož, Slovenia.
26. È stata membro del comitato di programma della conferenza *International Workshop on Boolean Problems (IWSBP)*, 24-25 settembre 2020, Bremen, Germania.
27. È stata membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 21-23 ottobre 2020, Tenerife (Canary islands), Spagna.
28. È stata membro del comitato di programma della conferenza *EEE International Conference on Electrical Engineering and Electronics*, 29-31- luglio 2021, Prague, Repubblica Ceca.
29. È stata membro del comitato di programma della conferenza DSD Euromicro special session *Future Trends in Emerging Technologies (FTET)*, 1-3 settembre 2021, Palermo, Italia.
30. È membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 15-17 giugno 2022, Corfu, Grecia.
31. È del comitato di programma della conferenza *EEE International Conference on Electrical Engineering and Electronics*, 28-30- luglio 2022, Prague, Repubblica Ceca.
32. È membro del comitato di programma della conferenza *Design Automation Conference* (DAC), 10-14 luglio 2022 San Francisco, CA (US).

3.4 Attività di revisione e valutazione

Attività di revisione per riviste internazionali

È stata revisore delle seguenti riviste internazionali:

- ACM Transactions on Algorithms (TALG)
- ACM Transactions on Knowledge Discovery from Data (TKDD)
- ACM Transactions on Database Systems (TODS)
- IEEE Transactions on Computers (TC)
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- Proceeding IEEE
- Theory of Computing Systems (TOCS)
- International Journal of Information Security
- Information Processing Letters
- Engineering Science and Technology, an International Journal, Elsevier
- Microprocessors and Microsystems, Elsevier
- Parallel Computing Systems & Applications (PARCO)
- Studia Logica
- Information Sciences
- International Journal of Circuit Theory and Applications
- IEICE Transactions on Information and Systems
- Journal of Circuits, Systems and Computers
- IET Computers & Digital Techniques

Attività di revisione per conferenze internazionali

È stata revisore per le seguenti conferenze internazionali:

- Symposium of Discrete Algorithms (SODA)
- ACM/IEEE Design Automation Conference (DAC)
- Design, Automation and Test in Europe (DATE)
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD)
- International Conference on Very Large Data Bases (VLDB)
- International Workshop on Logic and Synthesis (IWLS)
- Workshop on Algorithm Engineering and Experimentation (ALENEX)
- Workshop on Privacy and Security by means of Artificial Intelligence (PSAI)
- Fun with Algorithms (FUN)
- Workshop on Algorithm Engineering (WAE)
- ACM Symposium on Parallelism in Algorithms and Architectures (SPAA)
- Int. Colloquium on Structural Information and Communication Complexity (SIROCCO)
- International Symposium on Theoretical Aspects of Computer Science (STACS)
- International Symposium on Circuits and Systems (ISCAS)
- European Symposium on Algorithms (ESA)
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)
- IEEE International Conference on Advanced Information Networking and Applications (AINA)
- International Conference on Extending Database Technology (EDBT)
- ACM SIGMOD Conference (SIGMOD)
- IEEE Computer Security Foundations Symposium (CSF)

- Reed-Muller Workshop (RM)
- Italian Conference on Theoretical Computer Science (ICTCS)
- International Workshop on Boolean Problems (IWSBP)
- IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)
- International Symposium on Formal Methods (FM)
- International Symposium on Mathematical Foundations of Computer Science (MFCS)

Altre attività di revisione e valutazione

- Nel 2009 è stata membro del comitato di revisione del libro "Advances in Artificial Intelligence for Privacy Protection and Security", A. Solanas and , Martínez-Ballesté (eds), 2009, World Scientific Publishing Company.
- Nel 2014 è stata valutatore del progetto PISCOPIA Fellowship Programme cofinanziato da Marie Curie Actions.
- Dal 2013 è revisore di progetti per il MIUR (registro dei revisori REPRISE) per la ricerca di base.

3.5 Principali invited talk in conferenze internazionali

- 10-11/12/2015 EPFL Workshop on Logic Synthesis & Verification. Invited talk dal titolo: "Logic Synthesis via Boolean Relations".
- 29/03/2019 DATE 2019 Friday Workshop: Quo Vadis, Logic Synthesis? Invited talk dal titolo: "XOR Gates in Emerging Technologies".

3.6 Progetti di ricerca

È stata *responsabile per l'unità di ricerca* dell'Università degli Studi di Milano per il seguente progetto europeo H2020 approvato e finanziato:

> *Titolo Progetto*: Synthesis and Performance Optimization of a Switching Nano-crossbar Computer (NANOxCOMP)
>
> *Ruolo*: Responsabile scientifico di unità di ricerca (Università degli Studi di Milano, beneficiario)
>
> *Programma*: H2020-MSCA-RISE-2015 (Research and Innovation Staff Exchange)
>
> *Durata*: 48 mesi, 1 dicembre 2015 – 30 novembre 2019
>
> *Finanziamento totale*: 724.500 Euro. Il finanziamento MSCA-RISE-2015 prevede una quota del 45% per viaggi di scambio di ricercatori e una quota del 55% per spese di ricerca (missioni, organizzazione di conferenze, ecc.) e management
>
> *Quota finanziamento, spettante all'Università degli Studi di Milano, gestita dalla candidata*: 99.000 Euro, di cui 44.000 Euro per viaggi all'estero (secondment) e 55.000 Euro per ricerca e management

È stata *responsabile per l'unità di ricerca* dell'Università degli Studi di Milano per il seguente progetto *non* ammesso al finanziamento, ma con una valutazione positiva:

> *Titolo Progetto*: Ottimizzazione Logica per Strutture Regolari
>
> *Ruolo*: Responsabile scientifico di unità di ricerca (Università degli Studi di Milano)

Programma: PRIN 2009

Valutazione: 56/60

È stata coinvolta, in qualità di *partecipante*, in unità di ricerca di progetti approvati e finanziati, tra i quali:

- Progetto di ricerca SEED (Università degli Studi di Milano): "Sentinel: Situational awareness in critical Infrastructure Environment" (approvato a marzo 2020).
- Progetto di ricerca PRIN: "AMANDA: Algorithmics for MAssive and Networked DAta" (2014-2017).
- Progettodi ricerca Europeo FP7-ICT: "PrimeLife - Privacy and Identity Management in Europe for Life" (2008-2011).
- Progetto di ricerca PRIN: "Cryptographic databases" (2007-2009).
- Progetto di ricerca Vigoni/DAAD: "Sintesi di circuiti logici non ridondanti e con un numero limitato di livelli" (2005-2006).
- Progetto di ricerca MIUR: "Enhanced Content Delivery" (2004-2005).
- Progetto di ricerca FIRB: "Enabling Platforms for High-Performance Computational Grids Oriented to Scalable Virtual Organizations" (2002-2005).
- Progetto di ricerca MIUR: "ALINWEB: Algorithmics for Internet and the Web" (2002-2004).
- Progetto di ricerca MIUR: "High-Performance Distributed Platform" (2001-2004).
- Progetto di ricerca MURST: "Algoritmi per grandi insiemi di dati: scienza e ingegneria" (2000-2002).

3.7 Gruppi di ricerca e collaborazioni scientifiche

Coordinamento di gruppi di ricerca

- Dal 2009 al 2015 è stata *responsabile e coordinatore* del Laboratorio ALOS (Algorithms and Logic Synthesis Lab.) presso il Dipartimento di Informatica, sede di Crema. Il principale interesse di ricerca nel laboratorio ALOS è lo studio di modelli, algoritmi e strutture dati per la sintesi efficiente di circuiti logici compatti e testabili a basso ritardo di propagazione e basso consumo energetico. Altri argomenti di ricerca comprendono lo studio di proprietà di funzioni booleane regolari per la sintesi di circuiti logici, lo studio di strutture dati resilienti agli errori e le applicazioni di tecniche tipiche dalla sintesi logica ad altri settori di ricerca; tra i quali il data mining, la sicurezza informatica e la biologia sintetica.
- Dal 2015 è *co-responsabile* del Laboratorio di ricerca FALSE (Formal methods and Algorithms for Large-Scale systEms) presso il Dipartimento di Informatica "Giovanni Degli Antoni" sede di Milano. Le attività di ricerca nel laboratorio FALSE riguardano la definizione e l'applicazione di metodi formali e di algoritmi nel contesto di moderni sistemi SW ed HW. Tali sistemi sono caratterizzati da ampia scalabilità e complessità, architetturale e comportamentale, sia ad alto livello di applicazioni SW (Systems of Systems, SoS) che a basso livello di architetture HW (Very Large Scale Integration Systems, VLSI). Nell'ambito del laboratorio è responsabile della parte scientifica che riguarda principalmente: 1) lo studio delle Tecnologie Emergenti e 2) le applicazioni a problemi di Sicurezza Informatica.

L'attività di coordinamento dei laboratori ha portato alla supervisione e co-supervisione di 4 tesi di dottorato:

1. Supervisore della dottoranda Asma Taheri Monfared sul tema: "Synthesis of quantum circuits".
2. Co-supervisore della dottoranda Maryam Ehsanpour sul tema: "Toward Lower Communication Garbled Circuit Evaluation".
3. Co-supervisore del dottorando Luca Frontini sul tema: "Synthesis and Design of High Density Integrated Circuits".
4. Co-supervisore della dottoranda Maria Chiara Molteni sul tema: "On the security of cryptographic circuits: protection against probing attacks and performance improvement of garbled circuits".

Ulteriori dettagli relativi alla supervisione di tesi di laurea e di dottorato svolte nell'ambito dell'attività di ricerca dei suddetti laboratori sono riportati nella sezione 5.3.

Partecipazione alle attività di gruppi di ricerca

- Dal 1998 al 2004 è stata membro del gruppo di ricerca "Algorithms and Data Structures" del Dipartimento di Informatica, Università di Pisa.
- Dal 2005 è membro del gruppo di ricerca sulla "Sintesi Logica" che coinvolge l'Università degli Studi di Milano, l'Università di Pisa e l'Università degli Studi di Verona (ultraespresso.di.univr.it).
- Dal 2007 ha collaborato con il laboratorio di ricerca "Security, Privacy, and Data Protection Laboratory" (SPDP Lab) del Dipartimento di Informatica dell'Università degli Studi di Milano.

Collaborazioni scientifiche

Principali collaborazioni di ricerca in ambito *accademico*:

internazionali

- R. K. Brayton (UC Berkeley, US)
- R. Drechsler, G. Fey (University of Bremen, Germania)
- J. Cortadella (Universitat Politècnica de Catalunya, Spagna)
- S. Jajodia (George Mason University, US)
- P. Fiser (Czech Technical University in Prague, Repubblica Ceca)
- S. Muthukrishnan (Rutgers, The State University of New Jersey, US)
- M. Altun (Istanbul Technical University, Turchia)
- L. Anghel, (Grenoble Institute of Technology, Francia)
- M.B. Tahoori, (Karlsruhe Institute of Technology, Germania)

nazionali

- A. Bernasconi, P. Ferragina, F. Luccio, L. Pagli, N. Pisanti (Università di Pisa, Italia)
- T. Villa (Università degli Studi di Verona, Italia)
- S. Paraboschi (Università degli Studi di Bergamo, Italia)

Principali collaborazioni di ricerca in ambito *industriale*:

- V. Kravets (IBM TJ Watson Research Center, US) collaborazione sul tema "Decomposition Thecniques for Logic Synthesis Applied to Compex Benchmarks" . L'obiettivo principale della collaborazione è stato l'applicazione sperimentale di tecniche di decomposizioni, sviluppate dal gruppo di ricerca in ALOS Lab, a funzioni booleane di grosse dimensioni, fornite da IBM, allo scopo di minimizzare l'area del circuito risultante (2014).
- D. Alexandrescu (IROC Techonogies, Francia) collaborazione sul tema "Synthesis and Performance Optimization of a Switching Nano-Crossbar Computer" nell'ambito del progetto europeo H2020-MSCA-RISE-2015 (2015-2019).

3.8 Conseguimento di premi e riconoscimenti per l'attività scientifica

- Dicembre 2003. Riceve il grant (di 600 Euro) per le migliori tesi di PhD attribuita dal IFIP Working Group 10.5 al PhD Forum della International Conference on Very Large Scale Integration 1-3 dicembre 2003, Darmstadt, Germany.
- Dal 2019 è Senior Member IEEE.

3.9 Soggiorni presso centri di ricerca esteri

- Dal 06-06-2005 al 10-06-2005 ha visitato, nell'ambito del progetto Vigoni 2005, il dipartimento di Computer Science della University of Bremen (Germania). L'attività di ricerca, svolta in collaborazione con il Prof. Rolf Drechsler, direttore del Gruppo di Architetture dello stesso dipartimento, è stata rivolta allo studio della sintesi di circuiti logici non ridondanti e con un numero limitato di livelli.
- Dal 10-07-2006 al 14-07-2006 ha visitato, nell'ambito del progetto Vigoni 2006, il dipartimento di Computer Science della University of Bremen (Germania). L'attività di ricerca, svolta in collaborazione con il Prof. Rolf Drechsler e del suo gruppo di ricerca, è stata rivolta allo studio di nuovi metodi di sintesi di circuiti logici non ridondanti basati sulle strutture dati BDD (Binary Decision Diagrams).

3.10 Descrizione dell'attività di ricerca

I suoi principali interessi di ricerca sono nei seguenti ambiti: 1) progettazione e sintesi di circuiti logici; 2) metodi booleani per la sicurezza informatica; 3) algoritmi per la gestione di grandi quantità di dati. La maggior parte dei risultati sono stati ottenuti, oltre che nell'ambito puramente teorico, anche tramite la progettazione e la realizzazione di sistemi software.

Sintesi di circuiti e Computer Aided Design (CAD)

La sintesi logica consiste nel trasformare una funzione booleana, descritta ad alto livello, in un circuito logico equivalente, minimizzandone il costo. Il costo può dipendere da vari fattori quali l'area del circuito, il tempo di propagazione del segnale o la potenza dissipata.

1. Sintesi di reti logiche con un numero costante di livelli
L'attività di ricerca in questo ambito ha avuto inizio con la modellazione delle forme SPP mediante spazi affini e l'introduzione dei *circuiti 2-SPP* (che utilizzano solo porte EXOR con 2

ingressi) per garantirne la realizzazione pratica nell'attuale tecnologia CMOS, dove è richiesto l'utilizzo di porte EXOR con un numero limitato di ingressi [1, 40, 44, 46, 102]. Gli studi teorici e i risultati sperimentali hanno mostrato come i circuiti SPP e 2-SPP consentano di rappresentare funzioni booleane in modo molto più compatto rispetto alle classiche rappresentazioni a due livelli (la dimensione si riduce in media del 50%) e anche rispetto ad altre rappresentazioni a più livelli [1, 3, 40, 44, 46].

Oltre ai circuiti SPP e 2-SPP, sono state proposte e studiate altre forme a tre o quattro livelli che utilizzano le proprietà strutturali delle funzioni da sintetizzare per ottenere, con brevi tempi di elaborazione, rappresentazioni più compatte [9, 11, 52, 57, 59, 63, 65, 78]. In particolare per alcuni modelli, nonostante l'elevata complessità dei problemi di minimizzazione corrispondenti (che risultano essere NP^{NP}-hard) è stato possibile progettare algoritmi di approssimazione polinomiali, caratterizzati da rapporti di approssimazione costanti [10, 33, 49, 53, 54, 55, 67, 104]. Sono state inoltre proposte delle soluzioni euristiche efficienti per la sintesi di forme DSOP (Disjoint Sum of Product) [17, 56, 99] e tecniche di sintesi di celle resistenti alle radiazioni [80]. In fine alcuni studi hanno utilizzato le tecniche tipiche della sintesi logica in altri contesti, quali l'allineamento di sequenze [47] e il data mining [63].

Già da diversi anni è prassi comune, nella progettazione e nella sintesi automatica dei circuiti, prendere in considerazione da subito gli aspetti legati alla collaudabilità nei modelli statici di errore *stuck-at-0-1* (guasti per segnali fissi a 0 o a 1) e *cellular fault*. In questo ambito sono state analizzate, realizzate e sperimentate procedure di sintesi logica che producono circuiti a tre livelli caratterizzati da buone proprietà di collaudabilità [6, 9, 30, 45, 48, 52].

Recentemente lo studio della sintesi logica si è concentrato sulla minimizzazione di circuiti approssimati, nei quali è tollerato un certo grado di errore nell'output. Molte applicazioni, come ad esempio quelle audio e video, non necessitano di output sempre esatti e questa caratteristica può essere utilizzata per sintetizzare circuiti più compatti [28, 78, 93, 97].

I risultati di questo settore sono stati finanziati da vari progetti di ricerca (MURST, MIUR, Vigoni e FIRB) in cui la candidata è stata coinvolta (per maggiori dettagli si veda la sezione 3.6).

Il principale contributo originale in questo settore è lo studio formale di nuove circuiti compatti a più livelli e l'approccio innovativo alla minimizzazione logica utilizzando gli spazi affini.

2. Sintesi di funzioni regolari

La sintesi logica è un problema computazionalmente molto difficile, per questo motivo sono state studiate molte strategie per ridurre il tempo di calcolo e, allo stesso tempo, ricavare forme più compatte. L'utilizzo delle "regolarità" delle funzioni booleane per la loro sintesi sembra essere un approccio molto promettente. La ragione è che le funzioni non random che codificano problemi "reali", come sono, in generale, le funzioni che descrivono i circuiti integrati, spesso presentano una struttura regolare che può essere utilizzata nel processo di sintesi.

Al fine di migliorare ulteriormente i tempi di minimizzazione delle reti logiche, è stato quindi studiato il concetto di "autosimmetria", una proprietà che cattura la "regolarità" delle funzioni booleane e che può essere utilizzata per semplificare il problema della sintesi SPP [2, 5, 8, 19, 42, 46, 66, 82, 100, 103]. Gli studi sperimentali hanno mostrato che una percentuale considerevole di funzioni benchmark presenta proprietà più o meno marcate di autosimmetria; per queste funzioni i tempi di minimizzazione SPP si riducono drasticamente. Un secondo tipo di regolarità proposta e studiata è la D-riducibilità (ovvero la riducibilità della Dimensione) che consente di ridurre il numero di variabili che descrivono una funzione, in quanto è possibile individuare alcune variabili

che sono una combinazione lineare delle altre [13, 19, 50, 64, 69, 72].
Entrambi i tipi di regolarità sono abbastanza comuni nei benchmark classici di circuiti logici e gli algoritmi che individuano tali regolarità hanno complessità polinomiale.

Il principale contributo originale, in questo settore, è la proposta di utilizzare le regolarità e le simmetrie delle funzioni booleane per la loro sintesi logica.

3. Decomposizione e proiezione di circuiti
Per poter sintetizzare una funzione con un alto numero di variabili di input è spesso necessario scomporre la funzione in alcune funzioni più piccole la cui sintesi sia più facile.

L'obiettivo della ricerca in questa area è quindi l'indagine sistematica di tecniche di ristrutturazione basate sulla decomposizione, fattorizzazione e proiezione, con l'obiettivo di minimizzare l'area dei circuiti [10, 26, 33, 36, 39, 49, 53, 54, 55, 75, 81, 86, 107] o con lo scopo di spostare segnali critici verso l'uscita [15, 18, 21, 37, 58, 59, 67, 70, 73, 74, 105, 106]. Una specifica applicazione è la sintesi atta a ridurre l'attività di commutazione di un circuito (per ottenere bassa dissipazione di potenza) mantenendo l'area del circuito più compatta possibile.

I contributi principali a questa area di ricerca sono l'uso di strategie di proiezione nella sintesi logica, l'uso di specifiche condizioni "don't care", la modellazione dei problemi di sintesi con le relazioni booleane e la descrizione di nuove reti a più livelli a bassa dissipazione di potenza.

4. Sintesi logica nelle tecnologie emergenti
Nell'ultimo decennio sono state proposte molteplici nuove tecnologie per la realizzazione di circuiti elettronici. Le tecnologie emergenti si basano su nuove strutture logiche che richiedono nuovi paradigmi per la progettazione di circuiti efficienti. Di conseguenza diventa necessario lo sviluppo di una nuova generazione di strumenti di sintesi logica, di progettazione finisca e di collaudo.

Tra le tante tecnologie emergenti proposte negli ultimi anni, una particolarmente promettente si basa sui switching lattice (reticoli di commutazione). Un switching lattice è un reticolo bidimensionale di celle, ciascuna contenete un interruttore collegato alle quattro celle vicine nel reticolo, in modo che queste celle siano tutte collegate o tutte disconnesse. Una funzione booleana può essere implementata da un reticolo che associa ogni interruttore a un letterale booleano, in modo che se il letterale assume il valore 1 l'interruttore corrispondente è acceso e collegato ai suoi quattro vicini, altrimenti non è collegato. La funzione valuta 1 se e solo se esiste un percorso, interamente formato da interruttori accesi, tra due bordi opposti del reticolo.

Il problema di sintesi su un reticolo consiste quindi nel trovare un'assegnazione di letterali agli interruttori al fine di implementare una data funzione target con un reticolo di dimensioni minime. La ricerca in questo contesto ha riguardato 1) la sintesi di reticoli con tecniche di decomposizione [24, 85, 87, 89]; 2) lo studio dei reticoli in caso di simmetrie e regolarità [25, 83]; 3) la collaudabilità dei reticoli [23, 27, 29, 84, 87, 91, 92, 94, 96].

Questo tema di ricerca è stato finanziato dal progetto di ricerca europeo H2020-MSCA-RISE NANOxCOMP (si veda la sezione 3.6).

Il contributo principale questo settore è la definizione di un sistema complessivo per la sintesi e il collaudo di reticoli per la tecnologia basata sui array nano-crossbar.

Sicurezza e protezione dati

1. Protezione di informazioni sensibili
Oltre all'obiettivo primario di proteggere le informazioni sensibili, è sempre più critica la necessità di poter distribuire i microdati che le contengono, per consentirne l'analisi. Per rispondere a queste due esigenze opposte sono stati proposti molti metodi di protezione dei microdati. In questo contesto k-anonymity è una tecnica molto usata e studiata. Per proteggere l'identità degli individui, il possessore dei dati spesso rimuove o cifra le informazioni che si riferiscono direttamente all'individuo, come ad esempio il nome e il cognome. Questi dati privi delle identità esplicite non danno però garanzia di anonimità. Infatti la combinazione di attributi come la razza, il sesso e il codice postale con dati disponibili pubblicamente può portare all'identificazione dei singoli individui. Una possibile soluzione a questo problema è data dalla definizione di k-anonymity: una tabella è k-anonima se ogni sua riga (ovvero ogni singolo individuo) non può essere associata a meno di k individui quando essa è combinata con risorse esterne.

La ricerca in questo ambito ha quindi studiato e catalogato gli approcci proposti per garantire la proprietà di k-anonymity e ha proposto nuovi metodi e algoritmi per la frammentazione e cifratura nella memorizzazione dei dati [12, 14, 31, 32, 34, 35, 51, 60, 61, 62]. Sono state inoltre utilizzate strutture dati compatte come le BDD per la descrizione e la manipolazione di funzioni booleane [16, 68].

Questo tema di ricerca è stato finanziato dal progetto di ricerca europeo FP7-ICT: "PrimeLife" e dal progetto di ricerca PRIN: "Cryptographic databases" (si veda la sezione 3.6).

Il contributo principale questo settore è la descrizione di algoritmi efficienti e di strutture compatte per la frammentazione dei dati per garantire la k-anonymity.

2. Secure multyparty computation
L'obiettivo dei protocolli di Secure Multiparty Computation (SMC) è quello consentire, a un insieme di parti, di calcolare una funzione congiunta mantenendo i propri input privati. Uno dei possibili approcci per risolvere il problema SMC è basato sul protocollo *Garbled Circuit* (GC), che consente la valutazione sicura di una qualsiasi funzione utilizzando un circuito booleano che la rappresenti. Il costo del protocollo (ovvero il numero di messaggi utilizzati per la comunicazione tra le varie parti) dipende direttamente dal numero di porte del circuito che rappresenta la funzione. È stato dimostrato che, in questo protocollo, le porte XOR del circuito non hanno costi di comunicazione, mentre la computazione con le altre porte (AND, OR, ecc.) ha un costo maggiore di zero. Per minimizzare la complessità del protocollo, è quindi importante descrivere la funzione con un circuito che abbia il minimo numero di porte non-XOR.

In questo contesto, la ricerca ha prodotto alcuni risultati sulla riduzione di porte non-XOR in Garbled Circuit [38, 79, 90, 95, 98, 101] e sulla soluzione del problema di Secure Multiparty Computation, utilizzando circuiti multivalore anziché booleani [88].

I contributi principali a questo settore sono lo studio di nuovi metodi di sintesi che minimizzino il numero di porte non-XOR in un circuito booleano e la descrizione del protocollo Garbled Circuit nel contesto multivalore.

3. Strutture dati resilienti agli errori
La sicurezza di un sistema dipende anche dal suo grado di resilienza ai guasti. Per questo motivo la ricerca di algoritmi e strutture dati resilienti agli errori di memoria è sempre più importante. Tali algoritmi devono completare le operazioni per le quali sono stati progettati

anche in presenza di errori, funzionando correttamente sul sottoinsieme dei valori non corrotti. La ricerca in questo settore ha presentato il primo studio sistematico sulla resilienza ai guasti di strutture dati compatte come i Diagrammi Binari di Decisione (BDD) e una loro variante ovvero i Diagrammi Binari di Decisione Zero-suppressed (ZDD), che usualmente sono utilizzati per la rappresentazione e la gestione di funzioni booleane e insiemi di insiemi [20, 22, 71, 76, 77]. Le ridondanze intrinseche della rappresentazione e le proprietà strutturali dei BDD e ZDD sono state utilizzare per definire nuove strutture canoniche e resilienti agli errori.

Questo tema di ricerca è stato finanziato dal progetto di ricerca PRIN: "AMANDA" (si veda la sezione 3.6).

Il contributo principale in questo settore è la definizione e lo studio di nuove strutture dati, canoniche e resilienti agli errori, per la rappresentazioni di funzioni booleane.

Algoritmi per la gestione di grandi quantità di dati

Lo sviluppo di strutture dati e algoritmi efficienti per problemi di ricerca su grandi quantità di dati testuali riveste oggi un ruolo strategico determinante. Esistono molteplici tipi di dati testuali come ad esempio le biblioteche on-line, le basi di dati biologiche, i cataloghi di prodotti, i log di web-server e altri dati derivanti dal traffico internet. Lo studio di questi argomenti ha condotto ad alcuni risultati nel campo degli algoritmi auto-organizzanti per memoria esterna [7, 43]. È stata infatti descritta una struttura dati auto-organizzante (SASL) per la manipolazione efficiente di stringhe su disco che si basa sulla struttura dati randomizzata skip list.

In presenza di grandi quantità di dati non è chiaramente possibile utilizzare algoritmi di complessità esponenziale. Nel caso di problemi complessi è quindi utile classificare specifiche istanze polinomiali e descrivere algoritmi polinomiali per la loro risoluzione. In questo ambito è stato studiato il Quadratic Assignment Problem (QAP) (un problema difficile di programmazione lineare intera) [4, 41].

I principali contributi, in questo settore, sono stati la descrizione di una struttura di dati auto-organizzante per la gestione dinamica di stringhe in memoria esterna e definizione di un'istanza polinomiale del Quadratic Assignment Problem.

4 Pubblicazioni scientifiche

4.1 Classificazione delle pubblicazioni

L'attività di ricerca ha dato luogo a 99 pubblicazioni (e 3 articoli accettati per la pubblicazione), tra le quali:

- *28 pubblicazioni referate su riviste internazionali (e 1 articolo accettato e pubblicato su Early Access area di IEEE Xplore), tutte indicizzate Scopus o WOS.* Tra queste appaiono: IEEE Transactions on Computer (TC), ACM Transactions on Information and System Security (TISSEC), Journal of Computer Security, ACM Transactions on Algorithms (TALG), IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD).
- *10 capitoli invitati su libri a livello internazionale e soggetti a revisione.*
- *61 pubblicazioni referate in atti di conferenze internazionali (e 2 articoli accettati per la pubblicazione).* Tra queste appaiono: IEEE Symposium on Foundations of Computer Science (FOCS), Design Automation Conference (DAC), International Conference on Distributed Computing Systems (ICDCS), Design Automation and Test in Europe (DATE).

4.2 Articoli invitati in special issue con revisione

Gli articoli [42, 41, 45, 49, 52, 51, 62, 68, 67, 70, 66, 73, 79, 84, 85, 89, 86, 94] sono stati selezionati tra i migliori articoli presentati alle relative conferenze e invitati, come versione estesa, in special issue di riviste internazionali o capitoli di libri [2, 4, 30, 33, 11, 12, 14, 16, 15, 18, 19, 37, 38, 23, 24, 25, 39, 27]; dove sono stati soggetti ad ulteriore revisione.

4.3 Articoli invitati in conferenze internazionali

- "Locally Free Substitutions are not so Free: an Open Problem in Sequence Alignment", invitato alla conferenza *Third International Conference on FUN with Algorithms*, 2004 [47].
- "Exploiting Flexibility in Circuit Optimization Using Boolean Relations (Abstract)", invitato alla conferenza *EURO XXVI*, 2013 [105].
- "A multiple valued logic approach for the synthesis of garbled circuits", invitato alla conferenza *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, 2017 [88].

4.4 Elenco delle pubblicazioni

Articoli in riviste internazionali

[1] Valentina Ciriani. "Synthesis of SPP Three-Level Logic Networks using Affine Spaces", in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, volume 22 issue 10, pp. 1310-1323, 2003, ISSN: 0278-0070.

[2] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli, "Three-Level Logic Minimization Based on Function Regularities", in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, volume 22 issue 8, pp. 1005-1016, 2003, ISSN: 0278-0070.

[3] Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "Synthesis of Integer Multipliers in Sum of Pseudoproducts Form" in *Integration - the VLSI Journal*, volume 36 issue 3, pp. 103-118, 2003, ISSN: 0167-9260.

[4] Valentina Ciriani, Nadia Pisanti, and Anna Bernasconi. "Room Allocation: a Polynomial subcase of the Quadratic Assignment Problem", in *Discrete Applied Mathematics*, volume 144 issue 3, pp. 263-269, 2004, ISSN: 0166-218X.

[5] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "Exploiting Regularities for Boolean Function Synthesis". *Theory of Computing Systems*, volume 39 issue 4, pp. 485–501, 2006, ISSN: 1432-4350.

[6] Valentina Ciriani, Anna Bernasconi, and Rolf Drechsler. "Testability of SPP Three-Level Logic Networks in Static Fault Models". *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, volume 25 issue 10, pp. 2241–2248, 2006, ISSN: 0278-0070.

[7] Valentina Ciriani, Paolo Ferragina, Fabrizio Luccio, and S. Muthukrishnan. "A Data Structure for a Sequence of String Accesses in External Memory". *ACM Transactions on Algorithms (TALG)*, volume 3 issue 1, 2007, ISSN: 1549-6325.

[8] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "Synthesis of Autosymmetric Functions in a New Three-Level Form". *Theory of Computing Systems*, volume 42 issue 4, pp. 450–464, 2008, ISSN: 1432-4350.

[9] Anna Bernasconi, Valentina Ciriani, Rolf Drechsler, and Tiziano Villa. "Logic Minimization and Testability of 2-SPP Networks", in *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, volume 27 issue 7, pp. 1190–1202, 2008, ISSN: 0278-0070.

[10] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "The optimization of kEP-SOPs: computational complexity, approximability and experiments", in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, volume 13 issue 2, 2008, ISSN: 1084-4309.

[11] Goerschwin Fey, Anna Bernasconi, Valentina Ciriani, and Rolf Drechsler. "On the Construction of Small Fully Testable Circuits with Low Depth", in *Microprocessors and Microsystems*, Elsevier, volume 32 issue 5-6, pp. 263–269, 2008, ISSN: 0141-9331.

[12] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Combining Fragmentation and Encryption to Protect Privacy in Data Storage", in *ACM Transactions on Information and System Security (TISSEC)*, 2010, ISSN:1094-9224.

[13] Anna Bernasconi and Valentina Ciriani, "Dimension-reducible Boolean Functions based on Affine Spaces", in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, volume 16 issue 2, 2011, ISSN: 1084-4309.

[14] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Selective Data Outsourcing for Enforcing Privacy", in *Journal of Computer Security*, 2011, ISSN: 0926-227x.

[15] Anna Bernasconi, Valentina Ciriani, Valentino Liberali, Gabriella Trucco, and Tiziano Villa, "Synthesis of P-Circuits for Logic Restructuring", in *Integration - the VLSI Journal*, vol. 45, p. 282-293, 2012, ISSN: 0167-9260.

[16] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati. "An OBDD approach to enforce confidentiality and visibility constraints in data publishing", in *Journal of Computer Security*, vol. 20, p. 463-508, 2012, ISSN: 0926-227X.

[17] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli, "Compact DSOP and Partial DSOP Forms", in *Theory of Computing Systems*, 2013, ISSN: 1432-4350.

[18] Anna Bernasconi, Valentina Ciriani, Valentino Liberali, Gabriella Trucco, and Tiziano Villa. "SOP Restructuring by Exploiting Don't Cares", in *Embedded Hardware Design (Microprocessors and Microsystems)*, Elsevier, 2013, ISSN: 0141-9331.

[19] Anna Bernasconi and Valentina Ciriani, "Autosymmetric and Dimension Reducible Multiple-Valued Functions", in *Journal of Multiple-Valued Logic and Soft Computing*, 2014, ISSN: 1542-3980.

[20] Anna Bernasconi, Valentina Ciriani, Lorenzo Lago, "On the Error Resilience of Ordered Binary Decision Diagrams", in *Theoretical Computer Science (TCS)*, 2015, ISSN: 0304-3975.

[21] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa, "Using Flexibility in P-Circuits by Boolean Relations", in *IEEE Transactions on Computers (TC)*, 2015, ISSN: 0018-9340.

[22] Anna Bernasconi and Valentina Ciriani. "Index-Resilient Zero-Suppressed BDDs: Definition and Operations", in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2016, ISSN: 1084-4309.

[23] Dan Alexandrescu, Mustafa Altun, Lorena Anghel, Anna Bernasconi, Valentina Ciriani, Luca Frontini, Mehdi B. Tahoori, "Logic synthesis and testing techniques for switching nano-crossbar arrays", in *Microprocessors and Microsystems*, 2017, ISSN: 0141-9331.

[24] Anna Bernasconi, Valentina Ciriani, Luca Frontini, Valentino Liberali, Gabriella Trucco, and Tiziano Villa. "Enhancing logic synthesis of switching lattices by generalized Shannon decomposition methods", in *Microprocessors and Microsystems*, 2018, ISSN: 0141-9331.

[25] Anna Bernasconi, Valentina Ciriani, Luca Frontini, and Gabriella Trucco. "Composition of switching lattices for regular and for decomposed functions", in *Microprocessors and Microsystems*, 2018, ISSN: 0141-9331.

[26] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, Tiziano Villa. "Boolean Minimization of Projected Sums of Products via Boolean Relations", in *IEEE Transactions on Computers (TC)*, 68(9): 1269-1282, 2019, ISSN: 0018-9340.

[27] Lorena Anghel, Anna Bernasconi, Valentina Ciriani, Luca Frontini, Gabriella Trucco, Ioana I. Vatajelu. "Stuck-At Fault Mitigation of Emerging Technologies based Switching Lattices", in *Journal of Electronic Testing*, Springer, 36(3), pp. 313-326, 2020, ISSN:0923-8174.

[28] Anna Bernasconi, Valentina Ciriani, and Tiziano Villa. "Exploiting Symmetrization and D-reducibility for Approximate Logic Synthesis", in *IEEE Transactions on Computers (TC)*, accettato per la pubblicazione il 6 dicembre 2020 e pubblicato on-line il 9 dicembre 2020 su Early Access area di IEEE Xplore, ISSN: 0018-9340.

[29] M. Ceylan Morgul, Luca Frontini, Onur Tunali, Lorena Anghel, Valentina Ciriani, E. Ioana Vatajelu, Csaba Andras Moritz, Mircea R. Stan, Dan Alexandrescu, and Mustafa Altun. "Circuit Design Steps for Nano-Crossbar Arrays: Area-Delay-Power Optimization with Fault Tolerance", in *IEEE Transactions on Nanotechnology (TNANO)*, vol. 20, pp. 39-53, 2021, ISSN: 1536-125x.

Capitoli invitati in libri internazionali

[30] Valentina Ciriani, Anna Bernasconi, and Rolf Drechsler. "Stuck-At-Fault Testability of SPP Three-Level Logic Forms", in *VLSI-SoC: From Systems to Chips*, M. Glesner, R. Reis, L. Indrusiak, V. Mooney, H. Eveking (eds), Kluwer-Springer, 2006, ISBN: 0-387-33402-5.

[31] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. "k-Anonymity", in *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia (eds), Springer-Verlag, 2007, ISBN: 978-0-387-27694-6.

[32] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. "Microdata Protection", in *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia (eds), Springer-Verlag, 2007, ISBN: 978-0-387-27694-6.

[33] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "Logic Synthesis of EXOR Projected Sum of Products", in *VLSI-SoC: Research Trends in VLSI and Systems on Chip*, G. De Micheli, S. Mir, R. Reis (eds), Springer-Verlag, 2008, ISBN: 978-0-387-74908-2.

[34] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. "k-Anonymous Data Mining: A Survey", in *Privacy-Preserving Data Mining: Models and Algorithms*, Charu C. Aggarwal and Philip S. Yu (eds), Springer-Verlag, 2008, ISBN: 978-0-387-70991-8.

[35] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. "Theory of Privacy and Anonymity" in *Algorithms and Theory of Computation Handbook, second edition*, M. Atallah and M. Blanton (eds), CRC Press, 2009, ISBN: 978-1-58488-820-8.

[36] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, Tiziano Villa. "Logic Synthesis by Signal-Driven Decomposition", in *Advanced Techniques in Logic Synthesis, Optimizations and Applications*, Sunil Khatri and Kanupriya Gulati (eds.), Springer, 2011, ISBN: 978-1-4419-7517-1.

[37] Anna Bernasconi, Valentina Ciriani, Petr Fiser, and Gabriella Trucco. "Weighted Don't Cares in Logic Synthesis", in *Recent Progress in the Boolean Domain*, Bernd Steinbach (ed.), Cambridge Scholars Publishing, 2014, ISBN: 978-1-4438-5638-6.

[38] Stelvio Cimato, Valentina Ciriani, and Matteo Moroni. "Minimization of ESOP Forms for Secure Computation", in *Problems and New Solutions in the Boolean Domain*, Bernd Steinbach (ed.), Cambridge Scholars Publishing, 2016, ISBN: 1443889474.

[39] Anna Bernasconi, Robert. K. Brayton, Valentina. Ciriani, Gabriella Trucco, and Tiziano Villa. "Synthesis of Complemented Circuits", in *Further Improvements in the Boolean Domain*, Bernd Steinbach (ed.), Cambridge Scholars Publishing, 2018, ISBN: 1527503712.

Articoli in atti di conferenze internazionali

[40] Valentina Ciriani. "Logic Minimization using Exclusive OR Gates". *ACM/IEEE 38th Design Automation Conference (DAC)*, pp. 115–120, 2001, ISBN: 1-58113-297-2.

[41] Valentina Ciriani, Nadia Pisanti, and Anna Bernasconi. "Efficient Optimal Greedy Algorithms for Room Allocation". *Fun with Algorithms II*, Carleton Scientific, pp. 43–60, 2001, ISBN: 1-894145-09-7.

[42] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "Fast Three-Level Logic Minimization Based on Autosymmetry". *39th ACM/IEEE Design Automation Conference (DAC)*, pp. 425–430, 2002, ISBN: 1-58113-461-4.

[43] Valentina Ciriani, Paolo Ferragina, Fabrizio Luccio, and S. Muthu Muthukrishnan. "Static Optimality Theorem for External Memory String Access". *43rd IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 219–227, 2002, ISBN: 0-7695-1822-2.

[44] Valentina Ciriani and Anna Bernasconi. "2-SPP: a practical trade-off between SP and SPP synthesis", *International Workshop on Boolean Problems (IWSBP)*, 133-140, 2002, ISBN: 3-86012-180-4.

[45] Valentina Ciriani, Anna Bernasconi, and Rolf Drechsler. "Testability of SPP Three-Level Logic Networks". *12th IFIP International Conference on Very Large Scale Integration (VLSI-SoC)*, pp. 331–336, 2003, ISBN: 3-901882-17-0.

[46] Valentina Ciriani. "Three-Level Logic Synthesis: Algebraic Approach and Minimization Algorithms". Ph.D. Forum della conferenza VLSI-SoC 2003. *IFIP International Conference on Very Large Scale Integration (VLSI-SoC)*, p. 455, 2003, ISBN: 3-901882-17-0.

[47] Fabrizio Luccio, Sara Brunetti, Valentina Ciriani, Elena Lodi, and Nadia Pisanti. "Locally Free Substitutions are not so Free: an Open Problem in Sequence Alignment", su invito alla *Third International Conference on FUN with Algorithms*, Edizioni Plus, pp. 5–6, 2004, ISBN: 88-8492-150-3.

[48] Anna Bernasconi, Valentina Ciriani, Rolf Drechsler, and Tiziano Villa. "Efficient Minimization of Fully Testable 2-SPP Networks". *Design, Automation and Test in Europe (DATE)*, pp. 1300–1305, 2006, ISBN: 3-9810801-0-6.

[49] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "EXOR Projected Sum of Products". *14th International Conference on Very Large Scale Integration (VLSI-SoC)*, pp. 284–289, 2006, ISBN: 3-901882-19-7.

[50] Anna Bernasconi and Valentina Ciriani. "DSOP: Synthesis of a new class of regular functions". *9th Euromicro Conference on Digital Systems Design: Architectures, Methods and Tools (DSD)*, pp. 377–384, 2006, ISBN: 0-7695-2609-8.

[51] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pieragela Samarati, "Fragmentation and Encryption to Enforce Privacy in Data Storage", *12th European Symposium On Research In Computer Security (ESORICS)*, pp. 171–187, 2007, ISBN: 978-3-540-74834-2.

[52] Goerschwin Fey, Anna Bernasconi, Valentina Ciriani, and Rolf Drechsler. "On the Construction of Small Fully Testable Circuits with Low Depth", *Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD)*, pp. 563–569, 2007, ISBN: 0-7695-2978-X.

[53] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "An Approximation Algorithm for Fully Testable kEP-SOP". *14th ACM Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 417–422, 2007, ISBN: 978-1-59593-605-9.

[54] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "On Projecting Sums of Products". *Euromicro Conference on Digital Systems Design: Architectures, Methods and Tools (DSD)*, pp. 787–794, 2008, ISBN: 987-0-7695-3277-6.

[55] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "An Approximation Algorithm for Generalized EXOR Projected Sum of Products". *16th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, 2008, ISBN: 978-3-901882-32-6.

[56] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "A New Heuristic for DSOP Minimization". *International Workshop on Boolean Problems (IWSBP)*, 2008, ISBN: 987-3-86012-346-1.

[57] Giorgio Boselli, Valentina Ciriani, Gabriella Trucco, and Valentino Liberali. "A comparison between two logic synthesis forms from the digital switching noise viewpoint". *International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, 2008, ISBN: 978-3-540-95947-2.

[58] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa. "On Decomposing Boolean Functions via Extended Cofactoring". *Design, Automation and Test in Europe (DATE)*, 2009, ISBN: 978-3-9810801-5-5.

[59] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, Tiziano Villa. "Logic Minimization and Testability of 2SPP-P-Circuits". *Euromicro Conference on Digital Systems Design (DSD): Architectures, Methods and Tools*, 2009, ISBN: 978-0-7695-3782-5.

[60] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Fragmentation Design for Efficient Query Execution over Sensitive Distributed Databases". *29th International Conference on Distributed Computing Systems (ICDCS)*, 2009, ISBN: 978-0-7695-3659-0.

[61] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Keep a Few: Outsourcing Data while Maintaining Confidentiality". *14th European Symposium On Research In Computer Security (ESORICS)*, 2009, ISBN: 978-3-642-04443-4.

[62] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Enforcing Confidentiality Constraints on Sensitive Databases with Lightweight Trusted Clients". *23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)*, 2009, ISBN: 978-3-642-03006-2.

[63] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, Linda Pagli. "Fun at a Department Store: Data Mining Meets Switching Theory". *International Conference on FUN with Algorithms*, Lecture Notes in Computer Science, volume 6099, Springer 2010, ISBN: 978-3-642-13121-9.

[64] Anna Bernasconi, Valentina Ciriani. "Logic Synthesis and Testability of D-Reducible Functions". *IEEE/IFIP International Conference on Very Large Scale Integration*, 2010, ISBN: 978-1-4244-6471-5.

[65] Valentina Ciriani and Anna Bernasconi. "SEPP: a New Compact Three-Level Logic Form". *International Workshop on Boolean Problems (IWSBP)*, 2010, ISBN: 987-3-86012-404-8.

[66] Anna Bernasconi and Valentina Ciriani, "Autosymmetric Multiple-Valued Functions: Theory and Spectral Characterization". *IEEE 41st International Symposium on Multiple-Valued Logic (ISMVL)*, 2011, ISBN: 978-1-4577-0112-2.

[67] Anna Bernasconi, Valentina Ciriani, Valentino Liberali, Gabriella Trucco, and Tiziano Villa, "An Approximation Algorithm for Cofactoring-Based Synthesis". *21st Great Lakes Symposium on VLSI (GLSVLSI)*, 2011, ISBN: 978-1-4503-0667-6.

[68] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati, "Enforcing Confidentiality and Data Visibility Constraints: An

OBDD Approach". *25th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2011)*, 2011, ISBN: 978-3-6422-2347-1.

[69] Anna Bernasconi and Valentina Ciriani, "Compact and Testable Circuits for Regular Functions". *Exploiting Regularity in the Design of IPs, Architectures and Platforms (ERDIAP)*, 2011, ISBN: 978-3-8007-3333-0.

[70] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa, "Projected don't cares". *15th Euromicro Conference on digital system design (DSD)*, 2012, ISBN: 978-0-7695-4798-5.

[71] Lorenzo Lago, Anna Bernasconi, and Valentina Ciriani, "Error-resilient BDDs : a preliminary study". *Proceedings of the work in progress session held in connection with SEAA and DSD*, 2012, ISBN: 978-3-9024-5733-2.

[72] Anna Bernasconi, Valentina Ciriani, and Lorenzo Lago, "Compact OBDDs for 2D-Reducible Functions". *10th Inter. workshop on Boolean problems*, 2012, ISBN: 978-3-8601-2438-3.

[73] Anna Bernasconi, Valentina Ciriani, Petr Fiser, and Gabriella Trucco, "Weighted don't cares". *10th International workshop on Boolean problems*, 2012, ISBN: 978-3-8601-2438-3.

[74] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa, "Miminization of P-Circuits using Boolean Relations". *Design, Automation and Test in Europe (DATE)*. Best Paper Candidate, 2013, ISBN: 978-3-9815-3700-0.

[75] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa, "Minimization of EP-SOPs via Boolean Relations" . *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. 2013, ISBN: 978-1-4799-0522-5.

[76] Anna Bernasconi, Valentina Ciriani, Lorenzo Lago, "Error Resilient OBDDs". *IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, 2013, ISBN: 978-1-4673-6135-4.

[77] Anna Bernasconi and Valentina Ciriani. "Zero-Suppressed Binary Decision Diagrams Resilient to Index Faults". *Theoretical Computer Science (TCS2014)*, 2014, ISBN: 978-3-6624-4601-0.

[78] Anna Bernasconi and Valentina Ciriani. "2-SPP Approximate Synthesis for Error Tolerant Applications". *Euromicro Conference on Digital Systems Design (DSD): Architectures, Methods and Tools*, 2014, ISBN: 978-1-4799-5793-4.

[79] Stelvio Cimato, Valentina Ciriani, and Matteo Moroni. "ESOP Synthesis for Secure Computation". *Int. Workshop on Boolean Problems*, 2014, ISBN: 978-3-86012-488-8.

[80] Valentina Ciriani, Luca Frontini, Valentino Liberali, Seyedruhollah Shojaii, Alberto Stabile, and Gabriella Trucco. "Radiation-Tolerant Standard Cell Synthesis using Double-Rail Redundant Approach". *21st IEEE International Conference on Electronics Circuits and Systems (ICECS14)*, 2014, ISBN: 978-1-4799-4242-8.

[81] Anna Bernasconi, Valentina Ciriani, Robert Brayton, Gabriella Trucco, and Tiziano Villa. "Bi-Decomposition using Boolean Relations". *Euromicro Conference on Digital Systems Design (DSD): Architectures, Methods and Tools*, 2015, ISBN: 978-1-4673-8035-5.

[82] Anna Bernasconi, Valentina Ciriani, and Gabriella Trucco. "Biconditional-BDD Ordering for Autosymmetric Functions". *Euromicro Conference on Digital Systems Design (DSD): Architectures, Methods and Tools*, 2015, ISBN: 978-1-4673-8035-5.

[83] Anna Bernasconi, Valentina Ciriani, Luca Frontini, and Gabriella Trucco. "Synthesis on switching lattices of Dimension-reducible Boolean functions". *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. 2016, ISBN: 978-1-5090-3561-8.

[84] Dan Alexandrescu, Mustafa Altun, Lorena Anghel, Anna Bernasconi, Valentina Ciriani, Luca Frontini, Mehdi B. Tahoori. "Synthesis and Performance Optimization of a Switching Nano-Crossbar Computer". *Euromicro Conf. on Digital System Design (DSD)*, 2016, ISBN: 978-1-5090-2817-7.

[85] Anna Bernasconi, Valentina Ciriani, Luca Frontini, Valentino Liberali, Gabriella Trucco, and Tiziano Villa. "Logic Synthesis for Switching Lattices by Decomposition with P-Circuits". *Euromicro Conference on Digital System Design (DSD)*, 2016, ISBN:978-1-5090-2817-7.

[86] Anna Bernasconi, Robert Brayton, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa. "Complemented circuits". *Int. Workshop on Boolean Problems*, 2016, ISBN: 978-3-86012-540-3.

[87] Mustafa Altun, Valentina Ciriani, and Mehdi B. Tahoori. "Computing with nano-crossbar arrays: Logic synthesis and fault tolerance". *Design, Automation & Test in Europe Conference (DATE)*. 2017, ISBN: 978-3-9815-3708-6.

[88] Stelvio Cimato, Valentina Ciriani, Ernesto Damiani, Maryam Ehsanpour. "A multiple valued logic approach for the synthesis of garbled circuits". *IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, 2017, ISBN: 978-1-5386-2880-5.

[89] Anna Bernasconi, Valentina Ciriani, Luca Frontini, Gabriella Trucco (2017). "Composition of Switching Lattices and Autosymmetric Boolean Function Synthesis". *Digital System Design (DSD), Euromicro Conference on*, 2017, ISBN: 978-1-5386-2146-2.

[90] Maryam Ehsanpour, Stelvio Cimato, Valentina. Ciriani, Ernesto Damiani. "Exploiting Quantum Gates in Secure Computation". *Digital System Design (DSD), 2017 Euromicro Conference on*, 2017, ISBN: 978-1-5386-2146-2.

[91] M. Ceylan Morgul, Onur Tunali, Mustafa Altun, Luca Frontini, Valentina Ciriani, E. Ioana Vatajelu, Lorena Anghel, Csaba Andras Moritz, Mircea R. Stan, and Dan Alexandrescu. "Integrated Synthesis Methodology for Crossbar Arrays". *NANOARCH* p. 91-97, ACM, 2018, ISBN: 978-1-4503-5-8156.

[92] Anna Bernasconi, Valentina Ciriani, Luca Frontini. "Testability of Switching Lattices in the Stuck at Fault Model". *IEEE/IFIP International Conference on VLSI and System-on-Chip, VLSI-SoC*, p. 213-218, IEEE Computer Society, 2018, ISBN: 978-1-5386-4756-1.

[93] Anna Bernasconi, Valentina Ciriani, Tiziano Villa. "Approximate Logic Synthesis by Symmetrization". *Design, Automation and Test in Europe (DATE)*, 1655-1660, 2019, ISBN: 978-3-9819263-2-3.

[94] Lorena Anghel, Anna Bernasconi, Valentina Ciriani, Luca Frontini, Gabriella Trucco, Ioana I. Vatajelu. "Fault Mitigation of Switching Lattices under the Stuck-At-Fault Model". 1–6, *IEEE Latin American Test Symposium (LATS)*, 2019, ISBN: 978-1-7281-1756-0.

[95] Stelvio Cimato, Valentina Ciriani, Ernesto Damiani, Maryam Ehsanpour. "An OBDD-Based Technique for the Efficient Synthesis of Garbled Circuits". 158-167, *International Workshop on Security and Trust Management (STM)*, 2019, ISBN 978-3-030-31510-8.

[96] Anna Bernasconi, Valentina Ciriani, and Luca Frontini. "Testability of Switching Lattices in the Cellular Fault Model". *Euromicro Conference on Digital System Design (DSD)*, 2019, ISBN 978-1-7281-2862-7.

[97] Anna Bernasconi, Valentina Ciriani, Jordi Cortadella, and Tiziano Villa. "Computing the Full Quotient in Bi-Decomposition by Approximation". *Design, Automation and Test in Europe (DATE)*, 2020, ISBN 978-3-9819263-4-7.

[98] Anna Bernasconi, Valentina Ciriani, Stelvio Cimato, and Maria Chiara Molteni. "Multiplicative Complexity of Autosymmetric Functions: Theory and Applications to Security". *57th Design Automation Conference (DAC)*, 2020, ISBN 978-1-7281-1085-1.

[99] Padmanabhan Balasubramanian, Anna Bernasconi, Valentina Ciriani and Tiziano Villa, "A Boolean Heuristic for Disjoint SOP Synthesis," *24th Euromicro Conference on Digital System Design (DSD)*, 2021, ISBN 978-1-6654-2703-6.

[100] Anna Bernasconi, Valentina Ciriani. "Autosymmetry of Incompletely Specified Functions". *Design, Automation and Test in Europe (DATE)*, 2021, ISBN 978-3-9819263-5-4.

[101] Maria Chiara Molteni, Vittorio Zaccaria and Valentina Ciriani . " ADD-based Spectral Analysis of Probing Security". *Design, Automation and Test in Europe (DATE)*, 2022, accettato per la pubblicazione.

[102] Anna Bernasconi, Valentina Ciriani. "On the Optimal OBDD Representation of 2-XOR Boolean Affine Spaces ". *Design, Automation and Test in Europe (DATE)*, 2022, accettato per la pubblicazione.

Articoli in atti informali e abstract

[103] Anna Bernasconi, Valentina Ciriani, Fabrizio Luccio, and Linda Pagli. "Implicit Test of Regularity for Incompletely Specified Boolean Functions". Atti informali *11th IEEE/ACM International Workshop on Logic & Synthesis (IWLS)*, 345-350, 2002.

[104] Anna Bernasconi, Valentina Ciriani, and Roberto Cordone. "EXOR Projected Sum of Products (Abstract)". *AIRO*, 2006, ISBN: 8860550742.

[105] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa. "Exploiting Flexibility in Circuit Optimization Using Boolean Relations (Abstract)", presentazione su invito. *EURO XXVI*, 2013, ISBN: 9789077171417.

[106] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa. "Compact representation of logic functions using Boolean relations (Abstract)". Atti informali *Computability in Europe (CiE)*, 2013.

[107] Anna Bernasconi, Robert Brayton, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa. "Minimization of Incompletely Specified Functions as Three-Level Logic via Boolean Relations". Atti informali *International Workshop on Logic & Synthesis (IWLS)*, 2015.

5 Attività di didattica e di servizio agli studenti

5.1 Attività didattica per i corsi di laurea triennali e magistrali

È stata titolare di 41 insegnamenti presso l'Università degli Studi di Milano. Inoltre è stata titolare di 7 edizioni di un insegnamento on-line di Laurea Triennale dell'Università degli Studi di Milano.

Insegnamenti in presenza:

1. A.A. 04/05 – Titolare dell'insegnamento *Logica Matematica* (MAT/01, 5 cfu, 40 ore), insegnamento complementare del III anno della laurea Triennale in Informatica.
2. A.A. 05/06 – Titolare dell'insegnamento *Laboratorio di Programmazione* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
3. A.A. 06/07 – Titolare dell'insegnamento *Fondamenti di Logica Matematica* (MAT/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Scienze e Tecnologie dell'Informazione.
4. A.A. 06/07 – Titolare dell'insegnamento *Laboratorio di Programmazione* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
5. A.A. 07/08 – Titolare dell'insegnamento *Fondamenti di Logica Matematica* (MAT/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Scienze e Tecnologie dell'Informazione.
6. A.A. 07/08 – Titolare dell'insegnamento *Laboratorio di Programmazione* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
7. A.A. 08/09 – Titolare dell'insegnamento *Fondamenti di Logica Matematica* (MAT/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Scienze e Tecnologie dell'Informazione.
8. A.A. 08/09 – Titolare dell'insegnamento *Laboratorio di Programmazione* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
9. A.A. 09/10 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
10. A.A. 10/11 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
11. A.A. 11/12 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
12. A.A. 12/13 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
13. A.A. 12/13 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese)(MAT/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Informatica.
14. A.A. 13/14 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
15. A.A. 13/14 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese)(MAT/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Informatica.
16. A.A. 14/15 – Titolare dell'insegnamento *Logica* (INF/01, 5 cfu, 40 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.

17. A.A. 14/15 – Titolare dell'insegnamento *Logica-Laboratorio* (INF/01, 1 cfu, 16 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
18. A.A. 14/15 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese)(MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
19. A.A. 15/16 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
20. A.A. 15/16 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese)(MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
21. A.A. 15/16 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del II anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
22. A.A. 15/16 – Titolare dell'insegnamento *Progettazione model driven del software-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento facoltativo del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
23. A.A. 16/17 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
24. A.A. 16/17 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese) (MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
25. A.A. 16/17 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del II anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
26. A.A. 16/17 – Titolare dell'insegnamento *Progettazione model driven del software-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento facoltativo del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
27. A.A. 17/18 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
28. A.A. 17/18 – Titolare dell'insegnamento *Logica Matematica* (INF/01, 5 cfu, 40 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
29. A.A. 17/18 – Titolare dell'insegnamento *Logica Matematica-Laboratorio* (INF/01, 1 cfu, 16 ore), insegnamento obbligatorio del I anno della laurea Triennale in Informatica.
30. A.A. 17/18 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del II anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
31. A.A. 18/19 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
32. A.A. 18/19 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese) (MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
33. A.A. 18/19 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
34. A.A. 19/20 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
35. A.A. 19/20 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.

36. A.A. 19/20 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese) (MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
37. A.A. 20/21 – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
38. A.A. 20/21 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.
39. A.A. 20/21 – Titolare dell'insegnamento *Mathematical Logic* (in Inglese) (MAT/01, 6 cfu, 48 ore), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
40. A.A. 21/22 (primo semestre) – Titolare dell'insegnamento *Logica* (INF/01, 6 cfu, 48 ore), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica.
41. A.A. 21/22 (primo semestre) – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 cfu, 24 ore), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche.

Insegnamenti per la laurea on-line:

1. A.A. 15/16 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
2. A.A. 16/17 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
3. A.A. 17/18 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
4. A.A. 18/19 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
5. A.A. 19/20 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
6. A.A. 20/21 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.
7. A.A. 21/22 – Titolare dell'insegnamento *Progettazione di Software sicuro-Laboratorio* (INF/01, 1,5 CFU, edizione on-line), insegnamento obbligatorio del III anno della laurea Triennale in Sicurezza dei sistemi e delle reti informatiche on-line, erogato dall'Università degli Studi di Milano.

5.2 Attività didattica per il dottorato di ricerca

È stata titolare di 2 insegnamenti per il Dottorato di Ricerca in Informatica presso l'Università degli Studi di Milano.

1. A.A. 16/17 – Titolare dell'insegnamento *Circuit modeling and applications to security and new technologies*, (2 cfu, 10 ore) insegnamento del Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.
2. A.A. 18/19 – Titolare dell'insegnamento *Circuit modeling and applications to biology, security and new technologies*, (2 cfu, 10 ore) insegnamento del Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.

5.3 Attività didattiche integrative e di servizio agli studenti

Relatore di tesi di laurea

Ha seguito, in qualità di relatore o correlatore, più di 20 tesi triennali e più di 10 tesi magistrali principalmente su tematiche relative alla sintesi di circuiti logici e alla sicurezza e privatezza informatica.

Relatore di tesi di dottorato

1. Supervisore della dottoranda Asma Taheri Monfared (XXXVII ciclo), Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.
   - Argomento della tesi: Synthesis of quantum circuits.
2. Co-supervisore della dottoranda Maryam Ehsanpour (XXX ciclo), Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.
   - Titolo della tesi: Toward Lower Communication Garbled Circuit Evaluation.
   - Esame finale: 28 febbraio 2018
3. Co-supervisore del dottorando Luca Frontini (XXXI ciclo), Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.
   - Titolo della tesi: Synthesis and Design of High Density Integrated Circuits.
   - Esame finale: 1 febbraio 2019.
4. Co-supervisore della dottoranda Maria Chiara Molteni (XXXIV ciclo), Dottorato di Ricerca in Informatica dell'Università degli Studi di Milano.
   - Argomento della tesi: On the security of cryptographic circuits: protection against probing attacks and performance improvement of garbled circuits.

Partecipazione a commissione di esami finali di PhD

Nel 2018 ha partecipato alla commissione di revisione di tesi di dottorato per il PhD program del Department of Computer Science, Universitat Politecnica de Catalunya (UPC), Barcelona, Spain.

Seminari per studenti universitari

Nell'A.A. 12/13 ha organizzato ed è stata docente di un ciclo di 6 seminari (di 2 ore ciascuno) con attività di laboratorio sul tema "Programmazione di App per Android" presso la sede di Crema dell'Università degli Studi di Milano.

Attività di tutorato

- È stata tutor per la *Laurea Triennale in Informatica* negli anni accademici: 09/10, 10/11, 11/12, 12/13, 13/14.
- È tutor per la *Laurea Magistrale in Sicurezza Informatica* per gli anni accademici 14/15, 15/16, 16/17, 17/18, 18/19, 19/20, 20/21 e 21/22.

Programma Erasmus

- È stata supervisore di una Erasmus internship della durata di 3 mesi (giugno 2014 - settembre 2014), dello studente Yusuf Miletli (Dumlupinar University, Turchia).
- È stata referente per l'Università degli Studi di Milano per tre Lecturer exchange (Erasmus+): Prof. Chris Koliopanos (Tech. Educational Institute of Epirus, Grecia), 2014; Prof. Antonis Mairgiotis (Technological Educational Institute of Epirus, Grecia), 2014; Prof. Rafael Martinez Torres (Universidad Complutense de Madrid, Spagna), 2018.

6 Attività istituzionali, di servizio e terza missione

6.1 Attività istituzionali e di servizio

- Dal 2017 è *referente AQ* (nell'ambito del sistema di Assicurazione della Qualità della didattica) per il corso di laurea triennale in "Sicurezza dei Sistemi e delle Reti Informatiche, erogazione on-line" del Consiglio di Coordinamento Didattico di Informatica, Università degli Studi di Milano.
- Dal 2021 è *referente*, per il Dipartimento di Informatica, della *Rete di referenti sulle politiche di genere* dell'Università degli Studi di Milano.
- Dal 2021 è *coordinatrice* del *Gruppo di lavoro sulle politiche di genere per le discipline STEM* dell'Università degli Studi di Milano.
- Dal 2020 è membro della *Commissione Orario* per il Consiglio di Coordinamento Didattico di Informatica dell'Università degli Studi di Milano.
- Dal 2011 è membro del *Collegio dei Docenti di Dottorato in Informatica* dell'Università degli Studi di Milano.
- Dal 2017 al 2020 è stata *referente AQ* (nell'ambito del sistema di Assicurazione della Qualità della didattica) per il corso di laurea triennale in "Sicurezza dei Sistemi e delle Reti Informatiche" del Consiglio di Coordinamento Didattico di Informatica, Università degli Studi di Milano.
- Dal 2012 al 2015 è stata membro eletto della *Giunta del Dipartimento di Informatica* dell'Università degli Studi di Milano.

- Dal 2012 al 2015 è stata membro eletto del *Comitato di Direzione della Facoltà di Scienze e Tecnologie* dell'Università degli Studi di Milano.
- Dal 2011 al 2016 è stata la *responsabile* per l'Università degli Studi di Milano della convenzione per gli allenamenti delle *Olimpiadi dell'Informatica* per gli studenti della scuola secondaria.
- Nel 2009, 2010 e 2012 è stata membro della *Commissione per la prova di ammissione alla Laurea Magistrale in Sicurezza* del Consiglio di Coordinamento Didattico di Crema, Università degli Studi di Milano.
- Dal 2008 al 2019 è stata membro della *Commissione Orientamento* del Dipartimento di Informatica, Università degli Studi di Milano.
- Dal 2006 al 2008 è stata membro della *Commissione Tesi, Stage e Tirocini* del Consiglio di Coordinamento Didattico di Crema, Università degli Studi di Milano.
- Dal 2005 al 2016 è stata membro delle *Commissione Orario*, con il ruolo di responsabile per il coordinamento e la preparazione dell'orario delle lezioni tenute presso la sede di Crema dell'Università degli Studi di Milano.
- Dal 2005 al 2008 è stata membro della *Commissione per la prova di ammissione degli studenti stranieri* del Consiglio di Facoltà di Scienze Matematiche Fisiche e Naturali, Università degli Studi di Milano.

6.2 Partecipazione a commissioni giudicatrici

- Il 03/09/2021 è nominata membro della *commissione giudicatrice* della selezione pubblica per la stipula di un contratto triennale di ricercatore a tempo determinato (RTDB) ai sensi dell'art. 24, comma 3, lettera b) della legge n.240/2010 per il settore concorsuale 01/B1-Informatica presso l'Università degli studi di Catania.
- Il 26/09/2021 è nominata membro della *commissione giudicatrice* della selezione pubblica per l'ammissione nell'anno accademico 2021/2022 (XXXVII ciclo) al corso di dottorato di ricerca in Informatica (borse aggiuntive PON), presso l'Università degli studi di Milano.
- Il 19/11/2021 è nominata membro della *commissione giudicatrice* della selezione pubblica per la stipula di un contratto triennale di ricercatore a tempo determinato (RTDA) ai sensi dell'art. 24, comma 3, lettera a) della legge n.240/2010, a valere sul PON "Ricerca e Innovazione" di cui al D.M. 1062/2021, per il settore concorsuale 01/B1-Informatica presso l'Università per Stranieri "Dante Alighieri" di Reggio Calabria.

6.3 Terza missione

Per contribuire alla terza missione e in particolare alle attività di public engagement dell'Ateneo, ha organizzato e coordinato i seguenti **stage** *rivolti agli studenti delle scuole superiori*, di cui è anche stata docente:

- Dal 2010 al 2017, allenamenti per le *Olimpiadi dell'Informatica*. In particolare:
  - dal 2010 al 2017 allenamenti per le olimpiadi territoriali presso l'Università degli Studi di Milano - sede di Crema (circa 20 ore ogni anno)
  - dal 2011 al 2013 allenamenti per le olimpiadi scolastiche presso l'Università degli Studi di Milano - sede di Crema (circa 16 ore ogni anno)
  - nel 2011 giornata di allenamento per le olimpiadi territoriali presso l'Università di Pisa (circa 6 ore)

  - nel 2011 giornata di allenamento per le olimpiadi nazionali presso l'Università degli Studi di Milano - sede di Crema (circa 8 ore)
- Nel 2010/2011, allenamenti della Squadra Nazionale Italiana per le *Olimpiadi Internazionali dell'Informatica* (due allenamenti a Sirmione, BS, e un allenamento a Volterra, PI).
- Nel 2012, nel 2013 e nel 2015, *stage* di "Problem Solving" presso la sede dell'Istituto Superiore Pacioli di Crema (12 ore ogni anno)
- Dal 2012 al 2015 e nel 2018, *stage* estivo "Apps e programmazione per la piattaforma Android" (15 ore ogni anno).
- Dal 2013 al 2015, *stage* estivo "Apps e programmazione per la piattaforma Android 2: Java" (15 ore ogni anno).
- Nel 2014, *learning week* presso l'istituto Volta di Lodi "APP-LICHIAMOCI: un ambiente visuale per la promozione culturale" (25 ore).
- Nel 2017 e nel 2019, *stage* di logica e problem solving (nell'ambito del progetto di alternanza scuola lavoro) rivolto agli studenti del Liceo Scientifico Leonardo Da Vinci di Crema presso l'Università degli Studi di Milano - sede di Crema (circa 5 ore ogni anno).

Inoltre:

- Dal 2008 al 2019 ha tenuto decine di seminari, su temi di ricerca in Informatica e Sicurezza Informatica, rivolti a studenti degli istituti superiori della Lombardia.
- Nel 2011 ha tenuto uno stage, rivolto ai docenti delle scuole superiori, per la preparazione alle *Olimpiadi dell'Informatica* a Sirmione, BS (circa 10 ore);
- Il 19/02/2012 ha tenuto un seminario su invito presso l'Accademia Giuseppe Aliprandi di Firenze, dal titolo: "Cloud Teaching";
- Nel 2015 ha tenuto uno stage sul Coding rivolto a bambini tra i 7 e gli 11 anni, nell'ambito dell'Universtà dei Bambini presso l'Università degli Studi di Milano - sede di Crema (circa 5 ore).
- Nel gennaio 2020 ha tenuto un laboratorio di Coding e Robotica Educativa rivolto a bambini in età prescolare, presso la Scuola dell'Infanzia Santa Maria della Croce, Crema (circa 4 ore).
- Dal 2012 al 2016 è stata membro della CEPIS Women in ICT Task Force, il cui scopo principale è quello di incoraggiare e stimolare l'interesse dei giovani, in particolare delle donne, a intraprendere gli studi e le carriere lavorative nell'ambito dell'ICT.

Milano, 29/11/2021