Curriculum vitae
Valentina Ciriani
[aggiornato al 13.04.2019]

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://homes.di.unimi.it/ciriani

2 Formazione e stato di servizio

2.1 Formazione universitaria

Gennaio 2003 – dicembre 2004. Svolge attività di ricerca presso il Dipartimento di Informatica dell'Università di Pisa. In gennaio e 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. Nel Periodo marzo 2003 - dicembre 2004 è stata titolare di un *assegno di ricerca* presso il Dipartimento di Informatica dell'Università di Pisa sul tema "Informatica".

Novembre 1998 – novembre 2002. Frequenta il Corso di Dottorato di Ricerca in Informatica (XIV ciclo), presso il Dipartimento Informatica dell'Università di Pisa Nel marzo 2003 consegue il titolo di *Dottore di Ricerca in Informatica* discutendo la tesi "Three-Level Logic Synthesis: Algebraic Approach and Minimization Algorithms", relatore: Prof. Fabrizio Luccio.

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

2.2 Stato di servizio

Il primo marzo 2015 ha preso servizio come Professore Associato S.S.D. INF01 – Informatica e attualmente è afferente al Dipartimento di Informatica dell'Università degli Studi di Milano.
Il 3 gennaio 2005 ha preso servizio come Ricercatore S.S.D. INF01 – Informatica (confermata dal 3 gennaio 2008) presso il Dipaerimento di Tecnologie dell'Informazione dell'Università degli Studi di Milano.

3 Attività di ricerca e pubblicazioni scientifiche

3.1 Interessi di ricerca

I suoi principali interessi di ricerca sono le *architetture degli elaboratori* e gli *algoritmi e strutture dati*, con particolare riferimento ai seguenti temi:

- Sintesi di circuiti e Computer Aided Design (CAD);
- Algoritmi per la gestione di grandi quantità di dati;
- Protezione di informazioni sensibili.

3.2 Attività di organizzazione e valutazione

Organizzazione di conferenze scientifiche

- È stata program co-chair per il topic "Logic Synthesis and Timing Analysis" della conferenza *Design, Automation and Test in Europe DATE 2014*.
- È stata program co-chair della Special Section "Emerging technologies and circuit synthesis (ETCS)" della conferenza *Euromicro Conference on Digital System Design DSD 2014*.
- È program co-chair della Special Section "Emerging technologies and circuit synthesis (ETCS)" della conferenza *Euromicro Conference on Digital System Design DSD 2015*.
- È stata program co-chair delle *Giornate Nazionali di Sintesi Logica*, GNSL (2005-2014):
    - 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 gugno 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

Membro di comitati di programma

- 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, Barcelona Spagna.
- È stata membro del comitato di revisione del libro "Advances in Artificial Intelligence for Privacy Protection and Security", A. Solanas and , Martínez-Ballesté (eds), World Scientific Publishing Company.
- 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.
- È stata membro del comitato di programma della conferenza *Workshop on Data Privacy Management (DPM)*, 24 settembre 2009, Saint Malo, Francia.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 8-12 marzo 2010, Dresden, Germania.
- 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.
- È stata membro del comitato di programma della conferenza *Data Privacy Management (DPM)*, 23 settembre 2010, Atene, Grecia.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 14-18 marzo 2011, Grenoble, Francia.
- 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.
- È stata membro del comitato di programma della conferenza *Data Privacy Management (DPM)*, 15-16 settembre 2011, Leuven, Belgio.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE*), 12-16 marzo 2012, Dresden, Germania.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 18-22 marzo 2013, Grenoble, Francia.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 24-28 marzo 2014, Dresden, Germania.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 9-13 marzo 2015, Grenoble, Francia.
- È stata membro del comitato di programma della conferenza *Design, Automation and Test in Europe (DATE)*, 14-18 marzo 2016, Dresden, Germania.
- È stata membro del comitato di programma della conferenza *International Workshop on Boolean Problems (IWSBP)*, 19-21 settembre 2018, Bremen, Germania.
- 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.
- È stata membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 20-22 giugno 2018, Barcelona, Spagna.

- È stata membro del comitato di programma della conferenza *Reed-Muller 2019 Workshop (RM2019)*, 23-24 maggio 2019, Bremen, Germania.
- 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.
- È stata membro del comitato di programma della conferenza *International Conference on Microelectronic Devices and Technologies (MicDAT)*, 22-24 maggio 2019, Amsterdam, Olanda.

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)
- Proceeding IEEE
- Theory of Computing Systems
- 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
- International Workshop on Boolean Problems (IWSBP)
- IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)

Attività di valutazione

Nel 2014 è stata valutatore del progetto PISCOPIA Fellowship Programme cofinanziato da Marie Curie Actions.

3.3 Seminari e partecipazione a conferenze

Seminari su invito

È stata invitata a tenere alcuni seminari presso Università italiane ed estere:

- 15/04/1999, presso il Politecnico di Torino, dal titolo "Aspetti pratici del Data Mining"
- 07/04/2003, presso l'Università degli studi di Roma, La Sapienza, dal titolo "Exploiting Regularities for Boolean Function Synthesis", seminario della serie SIA: Seminario Interdipartimentale di Algoritmica
- 10/06/2005, presso University of Bremen (Germania), dal titolo: "2SPP networks: syntesis and testing"
- 11/11/2005, presso l'Università di Pisa, dal titolo: "Synthesis of a new class of regular functions"
- 11/07/2006, presso University of Bremen (Germania), dal titolo: "Projection based synthesis techniques"
- 19/02/2012, presso l'Accademia Giuseppe Aliprandi Firenze, dal titolo: "Cloud Teaching"
- 18/01/2012 presso l'Università di Pisa, dal titolo: "Boolean relations and logic synthesis"

Invited talk

È stata invitata a tenere seminari in conferenze internazionali:

- 10-11/12/2015 EPFL Workshop on Logic Synthesis & Verification (organization by Giovanni De Micheli), dal titolo: "Logic Synthesis via Boolean Relations".
- 29/03/2019 DATE 2019 Friday Workshop: Quo Vadis, Logic Synthesis? Dal titolo: "XOR Gates in Emerging Technologies".

3.4 Progetti di ricerca

È coinvolta, in qualità di responsabile per l'unità di ricerca dell'Università degli Studi di Milano per il segunete progetti approvato e finanziato:

- Progetto di ricerca H2020-MSCA-RISE-2015: "NANOxCOMP: Synthesis and Performance Optimization of a Switching Nano-crossbar Computer". Finaziamento per l'unità di ricerca dell'Università degli Studi di Milano: 99.000 EUR.

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

- Progetto di ricerca PRIN: "AMANDA: Algorithmics for MAssive and Networked DAta".
- Progetto di ricerca PRIN: "Cryptographic databases".
- Progetto Europeo FP7-ICT: "PrimeLife - Privacy and Identity Management in Europe for Life".
- Progetto di ricerca FIRB: "Enabling Platforms for High-Performance Computational Grids Oriented to Scalable Virtual Organizations".
- Progetto di ricerca MIUR: "ALINWEB: Algorithmics for Internet and the Web".
- Progetto di ricerca MIUR: "Enhanced Content Delivery".
- Progetto di ricerca MIUR: "High-Performance Distributed Platform".
- Progetto di ricerca MURST: "Algoritmi per grandi insiemi di dati: scienza e ingegneria".
- Progetto di ricerca Vigoni/DAAD: "Sintesi di circuiti logici non ridondanti e con un numero limitato di livelli", responsabile della parte italiana Prof. Fabrizio Luccio, Università di Pisa, e responsabile della parte tedesca Prof. Rolf Drechsler, University of Bremen.

3.5 Coordinamento di gruppi di ricerca

Dal 2009 al 2015 è responsabile e coordinatore del Laboratorio ALOS (Algorithms and Logic Synthesis Lab.) presso il Dipartimento di Informatica, sede di Crema (alos.di.unimi.it). 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, sede di Crema. 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). Per affrontare la complessità di progettazione di tali sistemi è indispensabile disporre di metodi formali per la modellazione, di algoritmi per la decomposizione e la sintesi da modelli logici, di tecniche per la validazione di requisiti e la verifica di proprietà.

3.6 Collaborazioni scientifiche

Principali collaborazioni di ricerca in ambito accademico:

- R. K. Brayton (UC Berkeley, US)
- R. Drechsler, G. Fey (University of Bremen, Germania)
- P. Fiser (Czech Technical University in Prague, Repubblica Ceca)
- J. Cortadella (Universitat Politècnica de Catalunya, Spagna)
- S. Muthukrishnan (Rutgers, The State University of New Jersey, US)
- Mustafa Altun, ECC Group, Istanbul Technical University GR
- Lorena Anghel, TIMA Lab., France
- Mehdi B. Tahoori, Dependable Nano-Computing Group, Karlsruhe Institute of Technology, Germany
- S. Jajodia (George Mason University, US)
- A. Bernasconi, P. Ferragina, F. Luccio, L. Pagli, N. Pisanti (Università di Pisa, Italia)
- T. Villa (Università degli Studi di Verona, Italia)
- S. Cimato, R. Cordone, S. De Capitani di Vimercati, S. Foresti, V. Liberali, G. Livraga, P. Samarati, G. Trucco (Università degli Studi di Milano, 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 "Synthesis of multi level hard functions".
- Dr. Dan Alexandrescu, IROC Techonogies, France collaborazione sul tema "Synthesis and Performance Optimization of a Switching Nano-Crossbar Computer ".

3.7 Soggiorni presso centri di ricerca esteri

- Nel giugno 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.
- Nel luglio 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).

3.8 Breve descrizione dell'attività di ricerca

I suoi interessi nelle aree delle *architetture degli elaboratori* e degli *algoritmi e strutture dati* sono descritti e classificati nei seguenti paragrafi. La maggior parte dei risultati sono stati ottenuti, oltre che nell'ambito puramente teorico, anche tramite la progettazione e la realizzazione di sistemi software.

3.8.1 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
I metodi classici di sintesi logica si basano sulla minimizzazione a due livelli, il cui scopo è ottenere un circuito logico costituito da un primo livello di porte AND e da un secondo livello composto da un'unica porta OR. La minimizzazione a due livelli presenta due grossi vantaggi: gli algoritmi di ottimizzazione sono piuttosto veloci e i circuiti risultanti - grazie alla profondità fissata e limitata a due - hanno tempi di calcolo brevi e facilmente stimabili. D'altra parte, la minimizzazione a due livelli presenta anche un grosso svantaggio: la rappresentazione di diverse funzioni risulta estremamente inefficiente, nel senso che la dimensione dei circuiti ottenuti arriva ad essere esponenziale nel numero delle variabili di ingresso, rendendone impossibile la realizzazione pratica. Per ovviare a questo problema sono stati introdotti e studiati circuiti logici a tre livelli (circuiti SPP), costituiti da un primo livello di porte EXOR, un secondo livello di porte AND e un terzo livello composto da un'unica porta OR.

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, 36, 40, 42]. 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, 36, 40, 42].
L'attività di ricerca ha avuto quindi come obiettivo la progettazione e l'implementazione di procedure di sintesi che producano, con tempi di elaborazione accettabili, circuiti logici con un numero costante di livelli. 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, 48, 53, 55, 59, 61, 74]. In particolare per alcuni modelli, nonostante l'elevata complessità dei problemi di minimizzazione corrispondenti (che risultano essere anche più difficili di NP-hard) è stato possibile progettare algoritmi di approssimazione polinomiali, caratterizzati da rapporti di approssimazione costanti [10, 29, 45, 49, 50, 51, 63, 91]. Sono state inoltre proposte delle soluzioni euristiche efficienti per la sintesi di forme DSOP (Disjoint Sum of Product) [17, 52] e tecniche di sintesi di celle resistenti alle radiazioni [76]. In fine alcuni studi hanno utilizzato le tecniche tipiche della sintesi logica in altri contesti, quali l'allineamento di sequenze [43], la sicurezza informatica [75] e il data mining [59].

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 introdotto 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, 19, 38, 42, 62, 90]. 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. La teoria dell'autosimmetria è stata applicata anche alla sintesi a due livelli standard (forme SOP) ed è stata proposta una nuova forma a tre livelli, denominata ORAX [8].
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, 46, 60, 65, 68].
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 e lo studio di due particolari tipi di regolarità utilizzate a tale scopo.

3. Collaudabilità di reti logiche
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*. Questo approccio si è dimostrato più efficiente rispetto ai metodi tradizionali che separano nettamente lo studio della collaudabilità dal processo di sintesi.

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. La collaudabilità di tali circuiti è stata analizzata, in riferimento a diversi modelli di errore, con tecniche di analisi sia statiche che dinamiche [6, 9, 26, 41, 44, 48]. Grazie ad un dettagliato studio teorico si è ottenuta una classificazione del comportamento di questi circuiti rispetto alla loro collaudabilità; ovvero è stato possibile affermare sotto quali condizioni i circuiti sono completamente collaudabili e quando possono invece contenere delle ridondanze.

Il principale contributo in questo settore è lo studio della collaudabilità nei circuiti a più livelli e la descrizione di circuiti collaudabili in alcuni modelli statici di errore.

4. 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, 29, 32, 45, 49, 50, 51, 71] o con lo scopo di spostare segnali critici verso l'uscita [15, 18, 33, 54, 55, 63, 66, 69, 70, 92, 93]. 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. A differenza di algoritmi di fattorizzazione sviluppati solo per la minimizzazione dell'area, le decomposizioni studiate considerano delle specifiche variabili critiche (per esempio quelle con attività di commutazione più alta). La decomposizione e la relativa proiezione sono ottenute da alcune generalizzazioni della decomposizione di Shannon rispetto alle variabili critiche.

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.

3.8.2 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, 39]. È stata infatti descritta una struttura dati per la manipolazione efficiente di stringhe su disco. L'approccio utilizza una nuova e concettualmente semplice struttura dati auto-organizzante (SASL) che si basa sulla struttura dati randomizzata skip list e che può essere utilizzata anche in memoria interna.

In presenza di grandi quantità di dati, sono spesso utilizzati supporti di memoria interna di grandi dimensioni e di basso costo, che hanno quindi una maggiore probabilità di guasti fisici in porzioni di memoria. 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 [67, 68, 72, 73]. Le ridondanze nella rappresentazione e le proprietà strutturali dei BDD e ZDD sono state utilizzare per definire nuove strutture canoniche e resilienti agli errori.

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. Le istanze polinomiali di un problema difficile sono particolari istanze per cui è possibile descrivere un algoritmo di risoluzione polinomiale ad hoc. In questo ambito è stato studiato il Quadratic Assignment Problem (QAP) (un problema difficile di programmazione lineare intera). L'attività di ricerca ha pro-

dotto alcuni risultati nell'ambito della progettazione di algoritmi per istanze polinomiali di tale problema [4, 37].

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 la descrizione di versioni resilienti agli errori di alcuni classici diagrammi di decisione binari.

3.8.3 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 delle tecniche più usate e studiate. 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, la data di nascita, 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 (corrispondente ad un 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, 27, 28, 30, 31, 47, 56, 57, 58]. Sono state inoltre utilizzate strutture dati compatte come le BDD per la descrizione e la manipolazione di funzioni booleane [16, 64]

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

3.9 Descrizione delle pubblicazioni

Classificazione delle pubblicazioni

L'attività di ricerca ha dato luogo a 88 pubblicazioni, tra le quali:

- *25 pubblicazioni referate su riviste internazionali e 1 articolo accettato per la pubblicazione.* Tra queste appaiono: IEEE Transactions on Computer (TC), Theoretical Computer Science, ACM Transactions on Algorithms (TALG), IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), Theory of Computing Systems, ACM Transactions on Information and System Security (TISSEC), Journal of Computer Security.
- *10 capitoli invitati su libri a livello internazionale e soggetti a revisione, e 1 capitolo accettato per la pubblicazione.*
- *53 pubblicazioni referate in atti di conferenze internazionali.* 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).

Articoli invitati in special issue con revisione

Gli articoli [2, 4, 26, 29, 11, 12, 14, 16, 15, 18, 19, 33, 34] sono stati selezionati tra i migliori articoli presentati alle conferenze [38, 37, 41, 45, 48, 47, 58, 64, 63, 66, 62, 69, 75] e invitati, come versione estesa, in special issue di riviste internazionali o capitoli di libri; dove sono stati soggetti ad ulteriore revisione.

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 [43].
- "Exploiting Flexibility in Circuit Optimization Using Boolean Relations (Abstract)", invitato alla conferenza *EURO XXVI*, 2013 [92].

3.10 Elenco 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] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. 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] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. 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*, 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*, 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] D. Alexandrescu, M. Altun, L. Anghel, A. Bernasconi, V. Ciriani, L. Frontini, M. 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.

Capitoli invitati in libri internazionali

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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: 9781441975171.

[33] 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.

[34] 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.

[35] 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

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

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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'08)*, 2009, ISBN: 978-3-540-95947-2.

[54] 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.

[55] 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.

[56] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. 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.

[57] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Keep a Few: Outsourcing Data while Maintaining Confidentiality. *14th European Symposium On Research In Computer Security (ESORICS)*, 2009, ISBN: 9783642044434.

[58] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. 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.

[59] 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.

[60] 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.

[61] 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.

[62] Anna Bernasconi and Valentina Ciriani, Autosymmetric Multiple-Valued Functions: Theory and Spectral Characterization. *IEEE 41st International Symposium on Multiple-Valued Logic (ISMVL)*, 2011, ISBN: 9781457701122.

[63] 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.

[64] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. 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: 9783642223471.

[65] 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: 9783800733330.

[66] Anna Bernasconi, Valentina Ciriani, Gabriella Trucco, and Tiziano Villa, Projected don't cares. *15th Euromicro Conference on digital system design (DSD)*, 2012, ISBN: 9780769547985.

[67] 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: 9783902457332.

[68] Anna Bernasconi, Valentina Ciriani, and Lorenzo Lago, Compact OBDDs for 2D-Reducible Functions. *10th International workshop on Boolean problems*, 2012, ISBN: 9783860124383.

[69] Anna Bernasconi, Valentina Ciriani, Petr Fiser, and Gabriella Trucco, Weighted don't cares. *10th International workshop on Boolean problems*, 2012, ISBN: 9783860124383.

[70] 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: 9783981537000.

[71] 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: 9781479905225.

[72] Anna Bernasconi, Valentina Ciriani, Lorenzo Lago, Error Resilient OBDDs. *IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, 2013, ISBN: 9781467361354.

[73] Anna Bernasconi and Valentina Ciriani. Zero-Suppressed Binary Decision Diagrams Resilient to Index Faults. *Theoretical Computer Science (TCS2014)*, 2014, ISBN: 9783662446010.

[74] 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: 9781479957934.

[75] Stelvio Cimato, Valentina Ciriani, and Matteo Moroni. ESOP Synthesis for Secure Computation. *10th International Workshop on Boolean Problems (IWSBP14)*, 2014.

[76] 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.

[77] 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.

[78] 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.

[79] 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: 9781509035618.

[80] D. Alexandrescu, M. Altun, L. Anghel, A. Bernasconi, V. Ciriani, L. Frontini, M. Tahoor. Synthesis and Performance Optimization of a Switching Nano-Crossbar Computer. *Digital System Design (DSD), 2016 Euromicro Conference on*, 2016, ISBN: 9781509028177.

[81] Anna Bernasconi, Valentina Ciriani, Luca Frontini, Valentino Liberali, Gabriella Trucco, and Tiziano Villa. Logic Synthesis for Switching Lattices by Decomposition with P-Circuits. *Digital System Design (DSD), 2016 Euromicro Conference on*, 2016, ISBN: 9781509028177.

[82] Morgul, M. Ceylan, Alexandrescu, Dan, Tunali, Onur, Altun, Mustafa, Frontini, Luca, Ciriani, Valentina, Vatajelu, E. Ioana, Anghel, Lorena, Moritz, Csaba Andras, Stan, Mircea R. Integrated Synthesis Methodology for Crossbar Arrays. *NANOARCH*, 2018, ISBN: 9781450358156

[83] Anna Bernasconi, Robert Brayton, Valentina Ciriani, Robert Brayton, Gabriella Trucco, and Tiziano Villa. Complemented circuits. *International Workshop on Boolean Problems*, 2016, ISBN: 9783860125403.

[84] S. Cimato, V. Ciriani, E. Damiani, M. 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: 9781538628805.

[85] A. Bernasconi, V. Ciriani, L. Frontini, G. Trucco (2017). Composition of Switching Lattices and Autosymmetric Boolean Function Synthesis. *Digital System Design (DSD), 2017 Euromicro Conference on*, 2017, ISBN: 9781538621462.

[86] M. Altun, V. Ciriani, and M. Tahoori. Computing with nano-crossbar arrays: Logic synthesis and fault tolerance. *Design, Automation & Test in Europe Conference (DATE)*. 2017, ISBN: 9783981537086.

[87] M. Ehsanpour, S. Cimato, V. Ciriani, E. Damiani. Exploiting Quantum Gates in Secure Computation. *Digital System Design (DSD), 2017 Euromicro Conference on*, 2017, ISBN: 9781538621462.

[88] M. C. Morgul,D. Alexandrescu,O. Tunali, M. Altun, L. Frontini, V. Ciriani, E I. Vatajelu, L. Anghel, C.A. Moritz, M. R. Stan (2018). Integrated Synthesis Methodology for Crossbar Arrays.*NANOARCH '18 : Proceedings.* p. 91-97, ACM, ISBN: 9781450358156, Athens, 2018.

[89] A. Bernasconi,C V. Ciriani, L. Frontini, (2019). Testability of Switching Lattices in the Stuck at Fault Model. *IEEE/IFIP International Conference on VLSI and System-on-Chip, VLSI-SoC* vol. 2018-, p. 213-218, IEEE Computer Society, ISBN: 978153864756

Altre pubblicazioni

[90] 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.

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

[92] 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.

[93] 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.

[94] 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 *11th IEEE/ACM International Workshop on Logic & Synthesis (IWLS15)*, 2015.

4 Attività di didattica, di didattica integrativa e di servizio agli studenti

4.1 Attività didattica

È stata docente dei seguenti insegnamenti presso l'Università degli Studi di Milano, sede di Crema:

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

16. A.A. 14/15 – *Logica* (6 cfu), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica (a cui mutua Logica Matematica, insegnamento obbligatorio del I anno della laurea Triennale in Informatica).
17. A.A. 14/15 – *Mathematical Logic* (in Inglese)(6 cfu), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
18. A.A. 15/16 – *Logica* (6 cfu), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica (a cui mutua Logica Matematica, insegnamento obbligatorio del I anno della laurea Triennale in Informatica).
19. A.A. 15/16 – *Mathematical Logic* (in Inglese)(6 cfu), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
20. A.A. 15/16 – *Laboratorio di Ingegneria del Software* (3 cfu), insegnamento obbligatorio del II anno della laurea Triennale in Informatica.
21. A.A. 16/17 – *Logica* (6 cfu), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica (a cui mutua Logica Matematica, insegnamento obbligatorio del I anno della laurea Triennale in Informatica).
22. A.A. 16/17 – *Mathematical Logic* (in Inglese)(6 cfu), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
23. A.A. 16/17 – *Laboratorio di Ingegneria del Software* (3 cfu), insegnamento obbligatorio del II anno della laurea Triennale in Informatica.
24. A.A. 16/17 – *Circuit modeling and applications to security and new technologies*, PhD informatica.
25. A.A. 17/18 – *Logica* (6 cfu), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica (a cui mutua Logica Matematica, insegnamento obbligatorio del I anno della laurea Triennale in Informatica).
26. A.A. 17/18 – *Logica Matematica*(6 cfu), insegnamento obbligatorio de I anno della laurea Triennale in Informatica.
27. A.A. 17/18 – *Laboratorio di Ingegneria del Software* (3 cfu), insegnamento obbligatorio del II anno della laurea Triennale in Informatica.
28. A.A. 18/19 – *Logica* (6 cfu), insegnamento obbligatorio del I anno della laurea Magistrale in Sicurezza Informatica (a cui mutua Logica Matematica, insegnamento obbligatorio del I anno della laurea Triennale in Informatica).
29. A.A. 18/19 – *Mathematical Logic* (in Inglese)(6 cfu), insegnamento a scelta del I anno della laurea Magistrale in Informatica.
30. A.A. 18/19 – *Laboratorio di Ingegneria del Software* (3 cfu), insegnamento obbligatorio del II anno della laurea Triennale in Informatica.
31. A.A. 18/19 – *Circuit modeling and applications to biology, security and new technologies* , PhD informatica.

4.2 Attività di supporto alla didattica

È stata titolare dei seguenti contratti per il supporto alla didattica dei seguenti insegnamenti presso l'Università di Pisa:

- A.A. 00/01 – Titolare di 2 contratti per il supporto alla didattica ai corsi di *Algoritmi e Strutture Dati 1* e *Algoritmi e Strutture Dati, primo modulo* presso l'Università di Pisa.

- A.A. 01/02 – Titolare di 2 contratti per il supporto alla didattica ai corsi di *Laboratorio di introduzione alla programmazione* e *Algoritmi e Strutture Dati* presso l'Università di Pisa.
- A.A. 02/03 – Titolare di 2 contratti per il supporto alla didattica ai corsi di *Algoritmi e Strutture Dati* e *Laboratorio di programmazione di strutture dati* presso l'Università di Pisa.
- A.A. 03/04 – Titolare di 2 contratti per il supporto alla didattica ai corsi di *Algoritmica* e *Laboratorio di programmazione di strutture dati* presso l'Università di Pisa.

4.3 Attività didattiche integrative e di servizio agli studenti

Relatore di tesi

Ha seguito, in qualità di relatore o correlatore, 17 tesi triennali ed 10 tesi magistrali su tematiche relative alla sintesi di circuiti logici, agli algoritmi ed alle strutture dati.

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 l'A.A. 14/15 e 15/16. È stata supervisore di una Erasmus internship della durata di 3 mesi (giugno 2014 - settembre 2014).

5 Attività istituzionali, organizzative e di servizio

5.1 Attività istituzionali

- Dal 2012 al 2015 è membro eletto della *Giunta del Dipartimento di Informatica* dell'Università degli Studi di Milano.
- Dal 2012 al 2015è membro del *Comitato di Direzione della Facoltà di Scienze e Tecnologie* dell'Università degli Studi di Milano.
- Dal 2011 è membro del *Collegio dei Docenti di Dottorato in Informatica* dell'Università degli Studi di Milano.

5.2 Attività di servizio

- Dal 2017 è referente AQ per i corsi di laurea triennale in "Sicurezza dei Sistemi e delle Reti Informatiche" e "Sicurezza dei Sistemi e delle Reti Informatiche, on-line".
- Dal 2012 è membro della *Commissione Orientamento* del Dipartimento di Informatica, Università degli studi di Milano (per maggiori dettagli si veda la Sezione 5.2.1).

- Dal 2005 al 2016 è stata membro delle *Commissione Orario*, responsabile per il coordinamento e la preparazione dell'orario delle lezioni tenute presso la sede di Crema del 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.
- 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 2008 al 2010 è stata membro della *Commissione Orientamento* del Consiglio di Coordinamento Didattico di Crema, Università degli studi di Milano.
- 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 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.

5.2.1 Attività per la commissione orientamento

Per la commissione orientamento, oltre ad aver tenuto *numerosi seminari di orientamento* alle lauree informatiche presso gli istituti scolastici, ha organizzato, coordinato e insegnato i seguenti stage rivolti agli studenti delle scuole superiori:

- Dal 2010, allenamenti per le *Olimpiadi dell'Informatica* presso Università degli studi di Milano - sede di Crema. In particolare:
    - dal 2010 allenamenti per le olimpiadi territoriali (circa 20 ore ogni anno)
    - dal 2011 allenamenti per le olimpiadi scolastiche (circa 16 ore ogni anno)
    - nel 2011 giornata di allenamento per le olimpiadi nazionali (circa 8 ore)
- Nel 2010/2011, allenamenti della Squadra Nazionale Italiana per le *Olimpiadi Internazionali dell'Informatica*.
- 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, *stage* estivo "Apps e programmazione per piattaforma Android" (15 ore ogni anno).
- Dal 2013, *stage* estivo "Apps e programmazione per piattaforma Android 2: Java" (15 ore ogni anno).
- Nel 2014, *learning week* presso l'istituto Volta di Lodi "APP- LINCHIAMOCI: un ambiente visuale per la promozione culturale" (25 ore).