LUCA ODDONE BREVEGLIERI

Breve Curriculum Vitae et Studiorum – maggio 2016

UFFICIO: Dipartimento di Elettronica, Informazione e Bioingegneria
Via Ponzio 34 / 5
Politecnico di Milano
Piazza Leonardo da Vinci n. 32
20133 Milano
tel 02 2399 3653
fax 02 2399 3411
e-mail luca.breveglieri@polimi.it
home page http://www.deib.polimi.it

1. Informazioni generali

- Nato in Italia, 4 aprile 1962
- Maturità scientifica, 1980
- Laurea in ingegneria elettronica, 1986
- Dottorato di ricerca in ingegneria elettronica dell'informazione e dei sistemi (IEIS), 1991
- Collaboratore tecnico (7° livello), dal 1991 al 1998
- Professore associato (II^{a} fascia) dal 1998, raggruppamento disciplinare ING-INF-05 (ex K05A) "sistemi per l'elaborazione delle informazioni"

2. Attività didattica

- dal 2004: "Architettura del Calcolatore e Sistemi Operativi" (fondamenti di architettura del calcolatore e di sistemi operativi), laurea in ingegneria informatica, secondo anno – vedi beep.metid.polimi.it
- dal 2005: "Formal Languages and Compilers" (fondamenti di teoria dei linguaggi artificiali, sintassi e progetto di compilatori), laurea magistrale in ingegneria informatica, primo anno – vedi beep.metid.polimi.it
- dal 2004 al 2008 "Fondamenti di Crittografia" (fondamenti di crittografia, algoritmi e architetture), laurea magistrale in ingegneria informatica, primo anno – vedi beep.metid.polimi.it

3. Attività di ricerca

A partire dalla laurea ha effettuato attività di ricerca principalmente nel campo delle architetture VLSI dedicate e della crittografia applicata, e in parte nel campo dei linguaggi artificiali. Gli argomenti specifici sono i seguenti:

- progetto di architetture dedicate per aritmetica del calcolatore, elaborazione di segnale e di immagine, e più recentemente per sistemi crittografici
- automi, grammatiche e linguaggi formali, per modellare sistemi concorrenti

La ricerca nel campo dell'aritmetica dei calcolatori ed elaborazione di segnale e immagine ha compreso: studio di architetture VLSI per moltiplicazione veloce e per convoluzione discreta.

La ricerca in campo crittografico comprende:

- architetture VLSI efficienti per algoritmi crittografici innovativi e computazionalmente intensivi come i sistemi basati su curve ellittiche e su funzioni di pairing
- metodi di attacco a sistemi crittografici hardware e software basati su potenza (DPA) e tramite iniezione di guasto (DFA)
- metodi di protezione di sistemi crittografici hardware contro attacchi basati su iniezione di guasto tramite tecniche di tolleranza ai guasti

La ricerca nel campo dei linguaggi artificiali comprende: studio di grammatiche e linguaggi formali per modellare sistemi di calcolo concorrenti, e problemi di analisi sintattica (parsing).

A partire dal 2004 è stato co-fondatore e co-chair del workshop “Fault Diagnosis and Tolerance in Cryptography”, FDTC, vedi:

http://www.fdtc-workshop.eu

in collaborazione con la University of Massachusetts at Amherst, MA, USA.

A partire dal 20015 è stato co-fondatore e co-chair del workshop “Mobile Systems Technology”, MST, vedi:

http://www.mstworkshop.eu

in collaborazione con Micron, Inc.

Ha svolto un progetto europeo di ricerca industriale (MEDEA+ CRYPTOSOC A 304; progetto triennale: 2002 - 2004) relativo alle metodologie e architetture per la realizzazione di crittografia in server di rete di alta potenza, insieme a partner di ricerca e industriali italiani e stranieri: Politecnico di Torino, ST Microelectronics Italia, BULL Francia, SAGEM Francia, AMTEC Italia, I2E Francia, CEA Francia.

Ha svolto un progetto europeo di ricerca industriale (JU ENIAC “TOISE”); progetto triennale: 2011 - 2014) relativo alla realizzazione di sicurezza in smart grid elettriche, per applicazioni di smart metering a multimedia gateway, insieme a partner di ricerca e industriali italiani e stranieri: Università di Milano Bicocca, Università della Cantabria, ST Microelectronics Italia, AZCOM Italia, Thales Francia, CEA-LETI Francia, PWI Belgio, HAI Grecia, e altri

Ha in corso una collaborazione di ricerca con ST Microelectronics Italia, relativa al progetto di architetture VLSI efficienti per calcoli crittografici (in particolare per crittografia a chiave pubblica) e allo studio di metodi di attacco e contromisure basati su potenza (DPA) e iniezione di guasti (DFA).

4. Pubblicazioni

È co-autore di 28 articoli su rivista scientifica internazionale con comitato di revisione, di 7 contributi a volume pubblicato da editore internazionale, e di 83 articoli a congresso internazionale con comitato di revisione, nei settori di ricerca sopra indicati. Ha inoltre circa altre 20 pubblicazioni, di vario genere, tra cui la curatela e la traduzione di vari libri e manuali universitari. L’elenco completo della pubblicazioni è visibile sul sistema IRIS, e in gran parte sul sistema IEEExplore.

Ha pubblicato il testo seguente (in inglese):

S. Crespi Reghizzi; L. Breveglieri; A. Morzenti, Formal Languages and Compilation (2nd edition), Springer-Verlag, DOI:10.1007/978-1-4471-5514-0, ISBN:9781447155133, pp. 1-397, 2013.

e la traduzione in italiano:

S. Crespi Reghizzi; L. Breveglieri; A. Morzenti, Linguaggi formali e compilazione (2a edizione), Società Editrice Esculapio, Bologna, Italia, DOI:10.15651/978-88-748-8875-7, ISBN:978-88-7488-875-7, pp.1-488, 2015.

5. Altre attività

È stato consigliere scientifico presso ASI (Area Servizi Informatici) del Politecnico di Milano e delegato del rettore presso CILEA (Consorzio Interuniversitario Lombardo per l'Elaborazione Automatica – ora CINECA), e ora supervisiona le attività di calcolo scientifico intensivo (supercalcolo) per conto del Politecnico di Milano. Dal 2010 è membro del Comitato di Iniziativa e Monitoraggio per il programma co-finanziato LISA (Laboratorio Informatico di Simulazione Avanzata – edizioni I, II e III), Politecnico di Milano-Regione Lombardia.

Nel corso di vari anni, a partire dal 1987 fino a oggi, ha svolto attività di traduzione in italiano di testi scientifici nei settori dei sistemi operativi, delle strutture di calcolatore e delle reti telematiche, editi in inglese da McGraw-Hill e Morgan Kaufmann, poi pubblicati o in via di pubblicazione in italiano da parte di McGraw-Hill Libri Italia e Zanichelli Italia.