

# FABIO PARESCHI

## CURRICULUM VITAE

Novembre 2011

### Informazioni Personali

Pareschi Fabio  
Via Giovanni Verga, 69  
44124 Ferrara (ITALY)  
Cittadinanza: Italiana  
Data di nascita: 14 gennaio 1976  
E-mail: fabio.pareschi@unife.it

### Formazione

**26 Marzo 2007:** Dottorato in Tecnologia dell'informazione, ricevuto dall'Università di Bologna nell'ambito del progetto di Dottorato Europeo (EDITH).

Titolo della tesi: "*Chaos-Based Random Number Generators: Monolithic Implementation, Testing and Applications*" (elaborato in lingua inglese). Relatori: Prof. Gianluca Setti e Prof. Riccardo Rovatti.

**19 Luglio 2001:** Laurea in ingegneria elettronica (vecchio ordinamento), ricevuta dall'Università di Ferrara. Valutazione: 110/110 con lode.

Titolo della tesi: "*Confronto teorico e sperimentale tra metodologie innovative per la riduzione delle EMI dovute a segnali di clock e PWM*". Relatore: Prof. Gianluca Setti.

### Esperienze tecniche e scientifiche

Da **Gennaio 2003 a oggi:** afferente al Dipartimento di Ingegneria (**ENDIF**) dell'**Università di Ferrara**, nel gruppo di ricerca di Elettronica ed Elaborazione dei Segnali in collaborazione con prof. Gianluca Setti.

- da **agosto 2011** come titolare dell'assegno di ricerca "*Progetto, realizzazione e misura di un prototipo di un convertitore analogico-informazione basato su compressing sensing*".
- da **dicembre 2006 a dicembre 2007** come titolare del fondo "*Progetto e realizzazione di un generatore di clock a 3 GHz a spettro espanso per la riduzione delle interferenze elettromagnetiche in dispositivi Serial-ATA*", progetto approvato e finanziato all'interno del bando per giovani ricercatori dell'Università di Ferrara nell'anno 2006.
- da **aprile 2003 ad aprile 2011** come titolare dell'assegno di ricerca "*Metodologie di analisi e progetto di circuiti caotici con assegnate proprietà statistiche: tecniche di implementazione robusta di circuiti tempodiscreti*".
- da **gennaio 2003 a marzo 2003** come collaboratore occasionale esterno per "*ottimizzazione, implementazione e verifica sperimentale di una metodologia di progetto di oscillatori a dinamica complessa*";

Da **Settembre 2003 a oggi:** afferente al centro di ricerca **ARCES** (*Advanced Research Center on Electronic Systems*) "*E. De Castro*" dell'**Università di Bologna**, nel gruppo di ricerca di Statistical Signal Processing.

- da **gennaio 2004 a dicembre 2006** partecipazione (in qualità di studente) al progetto di dottorato europeo in tecnologia dell'informazione (*European Doctorate in Information Technology, EDITH*), progetto coordinato dal centro di ricerca ARCES con la partecipazione di numerose istituzioni europee di alto livello, accademiche e non.
- da **ottobre 2005 a aprile 2006**, come previsto dal progetto di dottorato europeo, è stato trascorso un periodo di studio (come *visiting student*) presso una delle istituzioni europee partecipanti al progetto. La struttura scelta è stata il Dipartimento di Ingegneria Elettronica (**ESAT**) della **Università Cattolica di Leuven (Belgio)**, in cui si

è collaborato con il gruppo di lavoro di sicurezza informatica (*Computer Security and Industrial Cryptography*, COSIC) sotto la supervisione di prof. Bart Preneel e prof. Ingrid Verbauwhede.

Fin **dall'anno 2003** l'attività scientifica ha previsto inoltre la collaborazione come **revisore** volontario per alcune tra le più importanti conferenze internazionali (tra cui ISCAS, ESSCIRC, ECCTD, NOLTA) e riviste internazionali (in particolare TCAS-I, TCAS-II e JSSC) nell'ambito della microelettronica. Inoltre a partire da **Novembre 2009** tale attività ha compreso la collaborazione come **Editor Associato** alla rivista internazionale *Nonlinear Theory and Its Applications* (NOLTA) – IEICE e, da **Febbraio 2011** alla rivista *IEEE Transactions on Circuits and Systems Part II: Express Briefs* (TCAS2).

Da **Ottobre 2001 a Novembre 2002** – impiego presso la ditta *Kart s.a.s.*, Ferrara.

Lavoro consistente nella gestione di server internet (registrazione e manutenzione di domini internet, server DNS, server http, server di posta elettronica e server SQL), creazione e manutenzione di piccole rete per uffici e assistenza tecnica per i clienti.

## Attività didattica

L'attività didattica svolta dall'anno accademico 2003/2004 presso la facoltà di Ingegneria dell'**Università di Ferrara** ha incluso un supporto alla didattica consistente in saltuarie supplenze fatte per quanto riguarda i corsi "Teoria dei Circuiti" (laurea triennale), "Circuiti Analogici per l'Elaborazione dei Segnali" (laurea specialistica) e "Circuiti e algoritmi per l'elaborazione statistica dei segnali" (laurea specialistica) tenuti da prof. Gianluca Setti.

Inoltre, dall'anno accademico 2007/2008, tale attività comprende l'affiancamento ufficiale a prof. Gianluca Setti per il corso "Teoria dei Circuiti" come assistente. (titolare nell'anno accademico 2008/2009 in qualità di **professore a contratto** del corso "Elementi di Simulazione Circuitale ed Esempi di Applicazioni", corso integrativo dell'insegnamento di "Teoria dei Circuiti"). Tale affiancamento ha previsto il supporto per l'insegnamento teorico, congiuntamente all'organizzazione di lezioni di esercitazione (sia in aula sia in laboratorio di elettronica) per un totale di circa 20 ore di lezione per anno. L'affiancamento prevede anche la preparazione e la gestione degli esami, congiuntamente con prof. Setti.

L'attività didattica presso la facoltà di Ingegneria dell'**Università di Bologna** ha invece previsto, dall'anno accademico 2004/2005, la gestione di alcuni seminari in qualità di relatore. Sono state eseguite inoltre alcune supplenze per il corso di "Elaborazione Statistica dei Segnali Elettronici" (laurea specialistica, titolare prof. Riccardo Rovatti) e del corso di "Elettronica applicata" (laurea triennale, titolare prof. Riccardo Rovatti).

A partire dall'anno accademico 2003/2004 sono inoltre state seguite numerose tesi di laurea in qualità di correlatore, sia presso la facoltà di Ingegneria dell'**Università di Ferrara** sia presso la facoltà di Ingegneria dell'**Università di Bologna**.

## Breve descrizione dell'attività di ricerca

L'attività di ricerca svolta è stata per la maggior parte incentrata sull'elaborazione di segnali utilizzando tecniche avanzate di analisi statistica al fine di migliorare le prestazioni di circuiti esistenti. In particolare l'attività di ricerca ha incluso la progettazione e l'implementazione di circuiti elettronici analogici e mixed-mode, con particolare enfasi all'implementazione di circuiti non lineari dalla dinamica complessa (**circuiti caotici**) in tecnologia CMOS integrata. Più nel dettaglio, tra le applicazioni principali, si possono enumerare:

- lo studio della generazione di numeri casuali e pseudocasuali. In particolare si è studiato l'utilizzo di mappe caotiche per la generazione di numeri casuali e lo studio statistico dei numeri casuali generati per la validazione del generatore in esame.
- lo studio della riduzione delle interferenze elettromagnetiche dovute a segnali di clock. Si è studiato sia l'utilizzo di mappe caotiche, sia l'utilizzo di segnali deterministici con assegnate proprietà.
- la possibilità di effettuare auto diagnosi di un circuito inducendo il circuito stesso ad auto oscillare. La principale innovazione consiste nell'introdurre oscillazioni complesse in modo da poter misurare contemporaneamente più parametri del circuiti tramite analisi statistica.
- la possibilità di effettuare campionamenti di segnali ridondanti tramite un insieme di misure inferiori rispetto a quelle teoricamente necessarie (*compressing sensing*). Tale tecnica trova largo impiego

soprattutto su segnali biomedicali, notoriamente riconosciuti come segnali in cui il contenuto informativo è molto basso in rapporto alla banda del segnale.

#### ***Corsi frequentati (di elevata rilevanza):***

- “*Energy Efficient VLSI Design*”, Prof. Vojin G. Oklobdzija (Erik Jonsson School of Engineering and Computer Science, University of Texas, Dallas). ARCES – Università di Bologna, Bologna (Italy), May 24-27, 2010.
- “*Advanced on-chip interconnect*”, Prof. Eby G. Friedman (University of Rochester). DEIS – Università della Calabria, Rende (Italy), June 21-22, 2006.
- “Introduction course to Cadence-based full custom design”. IMEC vzw, Leuven (Belgium), October 24-27, 2005.
- “*CMOS Analog Integrated Circuit Design*”, Prof. Philip E. Allen (Georgia Institute of Technology), ITC-IRST, Trento (Italy), October 13–17, 2003.

#### ***Pubblicazioni recenti: (su rivista)***

[1] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “On Statistical Tests for Randomness included in the NIST SP800-22 test suite and based on the Binomial Distribution”, accepted for publication in *IEEE Transactions on Information Forensics and Security*.

[2] Mauro Mangia, Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “Spectral shaping of spreading sequences as a mean to address the trade-off between narrowband and multi-access interferences in UWB systems”, to appear in *Nonlinear Theory and Its Applications (NOLTA), IEICE*, Vol.E94-N, No.10. October 2011.

[3] Victor R. Gonzalez-Diaz, Fabio Pareschi, Gianluca Setti, and Franco Maloberti, “A Pseudorandom Number Generator Based on Time Variant Recursion of Accumulators”, in *IEEE Transactions on Circuits and Systems II - Express Briefs*, Vol. 58, No 9, pp. 580-584. September 2011.

[4] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti, “Implementation and Testing of High-speed CMOS True Random Number Generators based on Chaotic Systems”, in *IEEE Transactions on Circuits and Systems I - Regular Papers*, Vol. 57, No 12, pp. 3124-3137. December 2010.

[5] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti, “A 3 GHz Serial ATA Spread Spectrum Clock Generator Employing a Chaotic PAM Modulation”, in *IEEE Transactions on Circuits and Systems I - Regular Papers*, Vol. 57, No. 10, pp. 2577 - 2587. October 2010.

[6] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “Statistical Testing of a Chaos Based CMOS True-Random Number Generator”, in *Journal of Circuits, Systems, and Computers*, Vol. 19, No. 4, pp. 897-910. June 2010.

[7] Sergio Callegari, Fabio Pareschi, Gianluca Setti, and Mani Soma, “Complex Oscillation Based Test Framework and its Application to Analog Filters”, in *IEEE Transactions on Circuits and Systems I - Regular Papers*, Vol. 57, No. 5, pp. 956 - 969. May 2010.

[8] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “Periodicity as Condition to Noise Robustness for Chaotic Maps with Piecewise Constant Invariant Density”, in *International Journal on Bifurcation and Chaos*, Vol. 16, No. 11, pp. 3391-3400, November 2006.

#### ***Capitoli di libro***

[9] Fabio Pareschi, Gianluca Setti, Sergio Callegari, and Riccardo Rovatti, “Implementation of low EMI Spread Spectrum Clock Generator Exploiting a Chaos-based Jitter”, in *Intelligent Computing Based on Chaos*, L. Kocharev, Z. Galias, S. Lian (Eds.), pp. 145-171. Springer-Verlag, Berlin Heidelberg 2009.

[10] Fabio Pareschi, Sergio Callegari, Gianluca Setti, and Riccardo Rovatti, “Circuits and systems for the synthesis of chaotic signals in engineering applications”, in *Intelligent Computing Based on Chaos*, L. Kocharev, Z. Galias, S. Lian (Eds.), pp. 173-196. Springer-Verlag, Berlin Heidelberg 2009.

### **Pubblicazioni recenti: (conferenze internazionali con revisore)**

[11] Fabio Pareschi, Gianluca Setti, Riccardo Rovatti, and Giovanni Frattini, “A Spread Spectrum Clock Generator Based on a Short-Term Optimized Chaotic Map” in *Proceedings of 37th Solid-State Circuits Conference* (ESSCIRC2011), pp. 507-510. Helsinki (Finland), September 12-16, 2011.

[12] Sergio Callegari, Fabio Pareschi, Gianluca Setti, and Mani Soma, “Resonate and Fire Dynamics in Complex Oscillation Based Test of Analog Filters”, in *Proceedings of 2011 International Symposium on Circuits and Systems* (ISCAS2011), pp. 1331-1334. Rio de Janeiro (Brazil), May 15-18, 2011.

[13] Fabio Pareschi, Gianluca Setti, Riccardo Rovatti, and Giovanni Frattini, “Differences between Theoretical and Measured Spectrum in System Employing a Spread-Spectrum Clock for EMI Reduction Purposes”, in *Proceedings of 2010 International Symposium on Nonlinear Theory and its Applications* (NOLTA2010), pp. 63-66. Krakow (Poland), September 5-8, 2010.

[14] Fabio Pareschi, Giuseppe Scotti, Luca Giancane, Riccardo Rovatti, Gianluca Setti, and Alessandro Trifiletti, “Power Analysis of a Chaos-Based Random Number Generator for Cryptographic Security”, in *Proceedings of 2009 International Symposium on Circuits and Systems* (ISCAS2009), pp. 2858-2861. Taipei (Taiwan), May 24-27, 2009.

[15] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “On the Approximation Errors in the Frequency Test Included in the NIST SP800-22 Statistical Test Suite”, in *Proceedings of 2008 IEEE Asia Pacific Conference on Circuits and Systems* (APCCAS2008), pp. 1216-1219. Macao (China) November 30 - December 3, 2008.

[16] Fabio Pareschi, Gianluca Setti and Riccardo Rovatti, “A 3 GHz Spread Spectrum Clock Generator for SATA Applications Using Chaotic PAM Modulation”, in *Proceedings of 2008 Custom Integrated Circuits Conference* (CICC2008), pp. 451-454. San Jose (USA), September 21-24, 2008.

[17] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “Second Level NIST Randomness Test for Improving Test Reliability”, in *Proceedings of 2007 International Symposium on Circuits and Systems* (ISCAS2007), pp. 1437-1440. New Orleans (USA), May 27-30, 2007.

[18] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti, “A Fast Chaos-based True Random Number Generator for Cryptographic Applications”, in *Proceedings of 32th European Solid-State circuit Conference* (ESSCIRC2006), pp 130-133. Montreux (Switzerland), September 19-21, 2006.

[19] Luca Antonio De Michele, Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti, “Chaos-based High-EMC Spread-Spectrum Clock Generator”, in *Proceedings of 17th European Conference on Circuit Theory and Design* (ECCTD2005), pp 165-168. Cork (Ireland), August 29 - September 2, 2005. (**Winner of the best paper award**)

[20] Fabio Pareschi, Luca Antonio De Michele, Riccardo Rovatti, and Gianluca Setti, “A PLL-based clock generator with improved EMC”, in *Proceedings of 16th International Zurich symposium on Electromagnetic Compatibility* (EMCZurich2005), pp 367-372. Zurich (Switzerland), February 13-18, 2005. (**Winner of the best student paper award**)

### **Premi / Riconoscimenti internazionali**

- L'articolo “A PLL-based Clock Generator with Improved EMC” [20] presentato alla 16th International Zurich Symposium on Electromagnetic Compatibility, Zurich (Switzerland), February 13-18, 2005, è stato riconosciuto come miglior articolo presentato da studenti (**best student paper award**).
- L'articolo “Chaos-based High-EMC Spread-Spectrum Clock Generator” [19] presentato alla 17th European Conference on Circuit Theory and Design, Cork (Ireland), August 29 - September 2, 2005 è stato riconosciuto come miglior articolo presentato alla conferenza (**best paper award**).

Ferrara, 7/11/2011

Fabio Pareschi