LUCA BREVEGLIERI

Curriculum Vitae et Studiorum – June 2008

OFFICE: Dipartimento di Elettronica e Informazione
(Dept. of Electronic Engineering and Information Science)
Via Ponzio 34 / 5
Politecnico di Milano
Piazza Leonardo da Vinci n. 32
I - 20133 Milano
ITALY
tel +39 (0)2 2399 3653
fax +39 (0)2 2399 3411
e-mail luca.breveglieri@polimi.it
homepage http://www.dei.polimi.it/

1. General information

- born in Italy, 4 april 1962
- master in electronic engineering, 1986
- Ph.D. in electronic engineering of information and systems, 1991
- associate professor from 1998 to day (in engineering of information and systems)

2. Teaching activity

Since his enrolment as an associate professor, prof. L. Breveglieri has taught or is currently teaching the following bachelor and master courses.

- from 1998 to 2001: “Fondamenti di Informatica II” – in italian
  eng. “Foundamentals of Informatics II”
  basics of operating systems and computer architecture, bachelor, 2rd year (Politecnico di Milano)
- from 1998 to 2001: “Calcolatori Elettronici” – in italian
  eng. “Digital Circuits”
  basics of switching theory, bachelor, 2nd year (Politecnico di Milano)
- from 2001 to 2005: “Informatica I” – in italian
  eng. “Computer Programming”
  basics of computer programming in C language, bachelor, 1st year (Politecnico di Milano)
- from 2001 to day: “Informatica II” – in Italian
  eng. “Computer Architecture and Operating System”
  basics of operating systems and computer architecture, bachelor, 1st year (Politecnico di Milano)
- from 2005 to day: “Formal Languages and Compilers” – in english
  basics of artificial languages theory and compiler design, master, 1st year (Politecnico di Milano)
- from 2004 to day: “Fondamenti di Crittografia” – in italian
  basics of cryptographic algorithms and architectures, master, 2nd year (Politecnico di Milano)
- in 2004: “Algebra dei Campi Finiti e Crittografia” – in italian
  basics of cryptographic algebra and algorithms, Ph.D, (Politecnico di Milano)

Prof. L. Breveglieri is involved in the faculty of ALaRI (Advanced Learning and Research Institute, Lugano, Switzerland); see http://www.alari.ch. He has taught for a few years at ALaRI an elective course (in english) on the foundations of cryptography (20 hours), in collaboration with prof. Christof Paar (University of Ruhr at Bochum, Germany).

Since 2000 prof. L. Breveglieri has been advising 4 Ph.D. candidates (3 finished), on various themes related to the research in the applied cryptography field.

3. Research activity

Since the master degree (in electronic engineering) prof. Breveglieri has been working mainly in the field of dedicated VLSI architectures and applied cryptography, and partly in that of formal languages for modeling complex systems. In these broad fields he has 11 journal publications and 60 conference publications, and has been the editor of 2 conference proceedings. Here is a detailed list of research topics:

- Design of dedicated architectures for computer arithmetic; see journals [1, 6] and conferences [1, 6, 17, 19, 22, 23]. This research is targeted to the identification and optimized design of digital circuits for the efficient computation of basic arithmetic operations, like integer multiplication and discrete convolution.
- Design of dedicated architectures signal and image processing, see journals [2, 7] and conferences [2, 4, 9, 12, 14, 21, 25, 30], and in particular for high energy physics (namely calorimetry measurements at the Large Hadron Collider of CERN, Geneva, Switzerland), see journals [3, 4] and conferences [8, 10,11, 13, 15, 16, 20]. This research is targeted to identification and optimized design of VLSI architectures for signal and image processing, like FFT and similar transforms. The work related to LHC measurements deals in particular with high precision integer arithmetic for the detection of particle position and energy.
- Design of dedicated architectures for cryptographic systems, see journals [11] and conferences [26, 27, 32, 35, 36, 38, 42, 46, 47, 48, 50, 51, 52, 53, 55, 59, 60]. This research is targeted to the design of efficient software routines and optimized VLSI coprocessors for the computation of innovative and complex cryptographic algorithms and protocols, like for instance elliptic curve cryptosystems (ECC), pairing-based cryptosystems, and other ones.
- Side channel attack methodologies to cryptographic architectures, see journals [8, 9, 10] and conferences [28, 29 33, 34, 37, 39, 40, 41,43, 44, 45, 49, 54, 56, 57, 58]; moreover he has been guest editor of the journal special section [1] and editor of the books [2, 3]. This research focuses on the very novel topic of side channel attacks to cryptographic systems, both software and hardware. In particular, the extremely recent filed of the so-called fault-injection-based attacks and differential fault analysis (DFA) to cryptographic systems is considered.
- Automata, grammars and formal languages, and modeling of concurrent systems, see journals [5] and conferences [3, 5, 18, 24]. This research is targeted to the study of some theoretical properties of innovative automata, grammar and language families, for application to modeling concurrent systems of various types.

In particular, the research in the cryptography field (the most recent and currently most active one) includes: efficient VLSI architectures for innovative and computing-intensive cryptographic algorithms like elliptic curves and pairing systems; power attacks, fault-injection-based attacks and differential fault analysis to cryptographic systems; and protection methods (countermeasures) to fault-injection-based attacks by means of classical and innovative fault diagnosis and tolerance techniques.

From 1992 to 1995 he has been involved in the FERMI Project (RD-16) at CERN, Geneva, Switzerland, aimed at the design of a fully digital readout system for high energy physics experiments planned at the Large Hadron Collider (namely the ATLAS and CMS experiments).Since 2000 he has been having a collaboration with ST Microelectronics (Italy) on various topics related to the research in applied cryptography. The company supports part of the research and has funded 4 Ph.D. grants (3 years each).

From 2002 to 2004 he has been involved in the EU MEDEA+ project A304 “Cryptosoc”, with Politecnico di Torino, ST Microelectronics, AMTEC, BULL, CEA, Sagem, E2, and others. This project is dedicated to the modeling and designing of efficient IP HW blocks for cryptographic computations. See: http://www.medeaplus.org.

Since 2004 he is co-founder and co-chair (with prof. I. Koren, university of Massachusetts at Amherst, MA, USA) of the workshop:

“*Fault Diagnosis and Tolerance in Cryptography*”, FDTC

see http://conferenze.dei.polimi.it/FDTC08 (and 07, 06, 05, 04). Since 2006 the FDTC workshop has published proceedings (by Springer-Verlag and IEEE).

He has taken invited part to some scientific events. Here is a recent excerpt:

- reviewer of the project “Hardware Acceleration of Cryptosystems based on Elliptic Curves”, 05/IN/I856, 2005, Irish Science Foundation (SF), Ireland
- invited lecture on "Parallel Hardware Architectures for the Computation of the Tate Pairing", at the IPAM Workshop on Special Purpose Hardware for Cryptography: Attacks and Applications, December 4 - 8, 2006, Institute of Pure and Applied Mathematics (IPAM), University of California at Los Angeles (UCLA), Los Angeles, USA, see http://www.ipam.ucla.edu
- reviewer of the project “SECHIP” of the programme on "Sécurité et Sûreté Informatique" SESUR – edition 2007, Agence Nationale de la Recherche (ANR), France

Since 2008 to day he is in the program committee of the Workshop on Arithmetic of Finite Fields (WAIFI).

Since 1998 to day he has served as reviewer of some international journals on computer science and engineering, to include Electronics Letters (IEE) and Transactions of Computers (IEEE).

Finally, since 2004 to day he has visited several times the University of Massachusetts at Amherst (UMASS), MA, USA.

4. Other activities

In 2001 he has acted as external evaluator of the project "Trasmissione Dati" (“Data Transmission”), of the Azienda Ospedaliera Cà Granda di Niguarda, Milano, Italy.

In 2002 he has been responsible of the research contract “Nuova Rete di Telecomunicazioni Tamoil” (“New Telecom Net of Tamoil Italy”), Tamoil Italia.

From 2004-2005 he has been responsible (with prof. M. G. Fugini of Politecnico di Milano) in the research project “Feasibility Study of a National Data Centre for the Recepiton, Elaboration and Storage of Space Telemetry Data”, Gavazzi Spazio Italy spa.

In 2004 and 2005 he has been elected and has acted as advisor for the promotion board to associate professor and assistant professor at the Politecnico di Bari and Università di Bergamo, Italy, respectively.

In 2005 he has acted as evaluator for project “Insubrinet” (an optical connection between the cities of Como, Italy, and Lugano, Switzerland), Administration of the Province of Como, Italy.

In 2007-08 he has been invited and has acted as external advisor for the promotion board to associate (full) professor, University College of Cork, Cork, Ireland.

5. Divulgation activity

Since the master degree, prof. L. Breveglieri has contributed to computer science divulgation and has made or directed several partial or full translations from english to italian of well known textbooks of computer programming and architecture. Here is a list thereof:

- R. Thompson, L. R. Rogers, J. L. Yates, *Advanced Programmes’s Guide to Unix SYSTEM V*, McGraw-Hill, USA, 1986

fully translated and published by McGraw-Hill Libri Italia in 1986 under the title "*Unix SYSTEM V: complementi di programmazione*"

- J. L. Hennessy, D. A. Patterson, *Computer Architecture: a Quantitative Approach*, Morgan Kaufmann Publishers, USA, 1990

  translated and published by Zanichelli Italia in 1993 under the title "*Architetture di calcolatori: metodi di valutazione e di progetto*"

- D. A. Patterson, J. L. Hennessy, *Computer Architecture and Design: the Hardware / Software Interface*, Morgan Kaufmann Publishers, USA, 1994

  translated and published by Zanichelli Italia in 1995 under the title "*Struttura e progetto dei calcolatori: l'interfaccia hardware e software*"

- L. L. Peterson, B. S. Davie, *Computer Networks: a Systems Approach*, Morgan Kaufmann Publishers, USA, 1996

  translated and published by Zanichelli Italia in 1999 under the title "*Reti di calcolatori: un approccio sistemico*"

- V. Hamacher, Z. Vranesic, S. Zacky, *Computer Organization*, McGraw-Hill, USA, 2004

  translated, directed and published by McGraw-Hill Libri Italia in 2007 under the title "*Introduzione all'architettura dei calcolatori*"

6. Publications

Journal and Book Editor

1. L. Breveglieri, I. Koren, Guest Editors, "*Special Section on Fault Diagnosis and Tolerance in Cryptography*", IEEE Transactions on Computers, volume 55, September, 2006
2. L. Breveglieri, I. Koren, D. Naccache, J-P. Seifert (eds.), "*Fault Diagnosis and Tolerance in Cryptography*", Proceedings of the 3rd International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2006, Yokohama, Japan, October 10, 2006, LNCS, volume 4236, (Sub-Library: Security and Cryptology), XIII, 253 pp.
3. L. Breveglieri, S. Gueron, I. Koren, D. Naccache, J-P. Seifert, (eds.), "*Fault Diagnosis and Tolerance in Cryptography*", Proceedings of the 4th International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2007, Vienna, Austria, September 10, 2007, IEEE Computer Society Press, 2007, 150 pp.

Journals

1. Fast Pipelined Complex Convolver; Breveglieri, L.; Piuri, V.; Electronics Letters, volume 28, issue 24, 19 Nov., 1992, Page(s): 2252 – 2254
2. Modular Design Methodologies for Image Processing Architectures; Antola, A.; Avai, A.; Breveglieri, L.; IEEE Transactions on Very Large Scale Integration (VLSI) Systems, volume 1, issue 4, Dec., 1993, Page(s): 408 – 414
3. A Digital Front-End Readout Microsystem for Calorimetry at LHC-The FERMI Project; Dell'Acqua, A.; Hansen, M.; Lofstedt, B.; Vanuxem, J.P.; Svensson, C.; Yuan, J.; Hentzell, H.; Alippi, C.; Breveglieri, L.; Dadda, L.; Piuri, V.; Salice, F.; Sami, M.; Stefanelli, R.; Cattaneo, P.; Fumagalli, G.; Goggi, V.G.; Brigati, S.; Gatti, U.; Maloberti, F.; Torelli, G.; Carlson, P.; Fuglesang, C.; Kerek, A.; Appelquist, G.; Berglund, S.; Bohm, C.; Yamdagni, N.; Sundblad, R.; IEEE Transactions on Nuclear Science, volume 40, issue 4, part 1-2, Aug., 1993, Page(s): 516 – 531
4. FERMI - A New Generation of Electronic Modules for Large Data Acquisition Arrays required by High Energy Physics; Dell'Acqua, A.; Alexanian, H.; Alippi, C.; Appelquist, G.; Bailly, P.; Benetta, R.; Berglund, S.; Bezamat, J.; Blouzon, F.; Bohm, C.; Breveglieri, L.; Brigati, S.; Carlson, P.; Cattaneo, P.; Dadda, L.; David, J.; Engstrom, M.; Fumagalli, G.; Gatti, U.; Genat, J.F.; Goggi, V.G.; Gong, S.F.; Hansen, M.; Hentzell, H.; Hoglund, I.; Inkinen, S.; Kerek, A.; LeDortz, O.; Lofstedt, B.; Maloberti, F.; Nayman, P.; Odmark, A.; Piuri, V.; Polesello, G.; Salice, F.; Sami, N.; Savoy-Navarro, A.; Stefanelli, R.; Sundblad, R.; Svensson, C.; Torelli, G.;

Vanuxem, J.P.; Yamdagni, N.; Yuan, J.; IEEE Transactions on Components Packaging and Manufacturing Technology, Part B: Advanced Packaging, volume 17, issue 3, Aug., 1994, Page(s): 302 – 309

5. Fair Expressions and Regular Languages over Lists; Breveglieri, L.; Informatique Théoretique et Applications / Theoretical Informatics and Applications – RAIRO, volume 31, number 1, 1997, Page(s): 15 – 66
6. A VLSI Inner Product Macrocell, Breveglieri; L.; Dadda, L.; IEEE Transactions on Very Large Scale Integration (VLSI) Systems, volume 6, issue 2, June, 1998, Page(s): 292 – 298
7. Dedicated Circuits for the Generation of Windows in Image Processing Architectures; Antola, A.; Breveglieri, L.; The Journal of VLSI Signal Processing, volume 25, issue 1, May, 2000, Page(s): 55 – 78
8. Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard; Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Piuri, V.; IEEE Transactions on Computers, volume 52, issue 4, April, 2003, Page(s): 492 – 505
9. Guest Editors' Introduction: Special Section on Fault Diagnosis and Tolerance in Cryptography; Breveglieri, L.; Koren, I.; IEEE Transactions on Computers, volume 55, issue 9, Sept., 2006, Page(s): 1073 – 1074
10. An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers; Breveglieri, L.; Koren, I.; Maistri, P.; IEEE Transactions on Computers, volume 56, issue 5, May, 2007, Page(s): 635 – 649
11. A Pairing SW Implementation for Smart-Cards; Bertoni, G.; Breveglieri, L.; Chen, L.; Fragneto, P.; Harrison, K.; et al.; The Journal of Systems & Software, volume 81, issue 7, July, 2008, Page(s): 1240 – 1247

Conferences

1. Fast Pipelined Multipliers for Bit-Serial Complex Numbers; Breveglieri, L.; Piuri, V.; Sciuto, D.; Proceedings of CompEuro '91, Advanced Computer Technology, Reliable Systems and Applications, 5th Annual European Computer Conference, 13 - 16 May, 1991, Page(s): 821–825
2. Window-Based Functional Blocks for Image Processing; Antola, A.; Breveglieri, L.; Proceedings of CompEuro '91, Advanced Computer Technology, Reliable Systems and Applications, 5th Annual European Computer Conference., 13 - 16 May, 1991, Page(s): 243 – 247
3. Deterministic Dequeue Automata and LL(1) Parsing of Breadth-Depth Grammars; Breveglieri. L.; Citrini, C.; Crespi Reghizzi, S.; Lecture Notes in Computer Science, Fundamentals of Computation Theory, volume 529, Springer-Verlag, 1991, Page(s): 146 – 156
4. Window-Based Dedicated Parallel Architectures for Image Processing; Antola, A.; Breveglieri, L.; Proceedings of the 11th IAPR International Conference on Pattern Recognition, 1992, volume IV, Conference D: Architectures for Vision and Pattern Recognition, 30 Aug. - 3 Sept., 1992, Page(s):199 – 203
5. A Fast Pipelined Complex Multiplier: the Fault Tolerance Issues; Breveglieri, L.; Piuri, V.; Sciuto, D.; Proceedings of the IEEE International Workshop on Defect and Fault Tolerance in VLSI Systems, 1992, 4 - 6 Nov., 1992, Page(s): 277 – 286
6. Bit Serial Fault Tolerant Architectures for Convolution and Polynomial Evaluation; Breveglieri, L.; Dadda, L.; Sciuto, D.; Proceedings of the 4th International Conference on Wafer Scale Integration, 1992, 22 - 24 Jan., 1992, Page(s): 310 – 319
7. Real-Time Scheduling by Queue Automata; Breveglieri. L.; Citrini, C.; Crespi Reghizzi, S.; Lecture Notes in Computer Science, Formal Techniques in Real-Time and Fault-Tolerant Systems, volume 571, Springer-Verlag, 1992, Page(s): 131 – 147
8. A Digital Front-End Readout Microsystem for Calorimetry at LHC-the FERMI Project; Alippi, C.; Appelquist, G.; Berglund, S.; Bohm, C.; Breveglieri, L.; Brigati, S.; Carlson, P.; Cattaneo, P.; Dadda, L.; Dell'Acqua, A.; Fuglesang, C.; Fumagalli, G.; Gatti, U.; Goggi, V.G.; Hansen, M.;

Hentzell, H.; Kerek, A.; Lofstedt, B.; Maloberti, F.; Piuri, V.; Salice, F.; Sami, M.; Stefanelli, R.; Sundblad, R.; SveNSSMICon, C.; Torelli, G.; Vanuxem, J.P.; Yamdagni, N.; Yuan, J.; Conference Record of the 1992 IEEE Nuclear Science Symposium and Medical Imaging Conference, volume 1, 1992, 25 - 31 Oct., 1992, Page(s): 424 – 426

9. Modular Design Methodologies For Image Processing Architectures; Antola, A.; Avai, A.; Breveglieri, L.; Paparella, A.; Proceedings of the Sixth International Conference on VLSI Design, 1993, January 3 - 6, 1993, Page(s): 260 – 263
10. A Digital Front-end Readout Mlcrosystem For Calorimeters At LHC; Dell'Acqua, A.; Alippi, C.; Appelquist, G.; Benetta, R.; Berglund, S.; Bezemat, J.; Blouzon, F.; Bohm, C.; Breveglieri, L.; Brigati, S.; Carlson, P.; Cattaneo, P.; Dadda, L.; David, J.; Engstrom, M.; Furnagalli, G.; Gatti, U.; Genat, J.F.; Goggi, G.; Hansen, M.; Hentzell, H.; Hoglund, I.; Inkinen, S.; Kerek, A.; LeDortz, O.; Lofstedt, B.; Maloberti, F.; Nayman, P.; Persson, S.T.; Piuri, V.; Salice, F.; Sami, M.; Savoy-Navarro, A.; Schwemling, P.; Stefanelli, R.; Sundblad, R.; Svensson, C.; Torelli, G.; Vanuxem, J.P.; Yamdagni, N.; Yuan, J.; Odmark, A.; IEEE Conference Record on Nuclear Science Symposium and Medical Imaging Conference, 31 Oct. - 6 Nov., 1993, Page(s): 773 – 776
11. System Level Policies for Fault Tolerance Issues in the FERMI Project; Dell'Acqua, A.; Hansen, M.; Ikinen, S.; Lofstedt, B.; Vanuxem, J.P.; Svensson, C.; Yuan, J.; Hentzell, H.; Del Buono, L.; David, J.; Genat, J.F.; Lebbolo, H.; LeDortz, O.; Nayman, P.; Savoy-Navarro, A.; Zitoun, R.; Alippi, C.; Breveglieri, L.; Dadda, L.; Piuri, V.; Salice, F.; Sami, M.; Stefanelli, R.; Cattaneo, P.; Fumagalli, G.; Goggi, G.; Brigati, S.; Gatti, U.; Maloberti, F.; Torelli, G.; Carlson, P.; Kerek, A.; Appelquist, G.; Berglund, S.; Bohm, C.; Engstrom, M.; Yamdagni, N.; Sundblad, R.; Hoglund, I.; Persson, S.T.; The IEEE International Workshop on Defect and Fault Tolerance in VLSI Systems, 1993, 27 - 29 Oct., 1993, Page(s): 1 –- 8
12. Pipelined Median Filters; Breveglieri, L.; Piuri, V.; Proceedings of the Instrumentation and Measurement Technology Conference, 1994, IMTC/94, 10th Anniversary. Advanced Technologies in I & M., 1994, IEEE, volume 3, 10- 1 2 May, 1994, Page(s): 1455 – 1458
13. A Modular Fault-Tolerant Approach to Design a Front-End Microsystem for Calorimetry at LHC; Breveglieri, L.; Piuri, V.; Proceedings of the Instrumentation and Measurement Technology Conference, 1994, IMTC/94, 10th Anniversary. Advanced Technologies in I & M., 1994, IEEE, volume 3, 10 -12 May, 1994, Page(s): 1136 – 1139
14. A Fast Pipelined FFT Unit; Breveglieri, L.; Piuri, V.; Proceedings of the International Conference on Application Specific Array Processors, 1994, 22 - 24 Aug., 1994, Page(s): 143 – 151
15. FERMI - A New Generation of Electronic Modules for Large Data Acquisition Arrays Required by High Energy Physics; Dell'Acqua, A.; Alippi, C.; Appelquist, G.; Berglund, S.; Bohm, C.; Breveglieri, L.; Brigati, S.; Del Buono, L.; Carlson, P.; Cattaneo, P.; Dadda, L.; David, J.; Engstrom, M.; Fumagalli, G.; Gatti, U.; Genat, J.F.; Goggi, G.; Hansen, M.; Hentzell, H.; Hoglund, I.; Inkinen, S.; Kerek, A.; Lebbolo, H.; LeDortz, O.; Lofstedt, B.; Maloberti, F.; Nayman, P.; Persson, S.T.; Piuri, V.; Salice, F.; Sami, M.; Savoy-Navarro, A.; Stefanelli, R.; Sundblad, R.; Svensson, C.; Torelli, G.; Vanuxem, J.P.; Yamdagni, N.; Yuan, J.; Zitoun, R.; Proceedings of the Sixth Annual IEEE International Conference on Wafer Scale Integration, 1994, 19 - 21 Jan., 1994, Page(s): 252 – 264
16. A Model for the Evaluation of Fault Tolerance in the FERMI System; Antola, A.; Breveglieri, L.; Proceedings of the 1995 IEEE International Workshop on Defect and Fault Tolerance in VLSI Systems, 1995, 13 - 15 Nov., 1995, Page(s): 72 – 80
17. Column Compression Pipelined Multipliers; Breveglieri, L.; Dadda, L.; Piuri, V.; Proceedings of the International Conference on Application Specific Array Processors, 1995, 24 - 26 July, 1995, Page(s): 93 – 103
18. Deterministic Parsing for Augmented Context-Free Grammars; Breveglieri, L.; Cherubini, A.; Crespi Reghizzi, S.; Lecture Notes in Computer Science, Mathematical Foundations of Computer Science, volume 969, Springer-Verlag, 1995, Page(s): 326 – 336

19. A VLSI Inner Product Macrocell; Breveglieri, L.; Dadda, L.; Proceedings of the Eighth Annual IEEE International Conference on Innovative Systems in Silicon, 1996, 9 - 11 Oct., 1996, Page(s): 26 – 35
20. Balancing of Fault Tolerance in the New Version of the FERMI Channel Chip: a Functional Evaluation; Antola, A.; Breveglieri, L.; Proceedings of the 1996 IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 1996, 6 - 8 Nov., 1996, Page(s): 249 – 257
21. Low-Latency Serial Architecture for the 1-D Discrete Wavelet Transform; Breveglieri, L.; Piuri, V.; Rona, M.; Swartzlander, E.E., Jr.; Proceedings of the Second Annual IEEE International Conference on Innovative Systems in Silicon, 1997, 8 - 10 Oct., 1997, Page(s): 300 – 309
22. Fast Arithmetic and Fault Tolerance in the FERMI System; Breveglieri, L.; Dadda, L.; Piuri, V.; Proceedings of the IEEE International Conference on Application-Specific Systems, Architectures and Processors, 1997, 14-16 July, 1997, Page(s): 374 – 383
23. A Serial-Input Serial-Output Bit-Sliced Convolver; Dadda, L.; Breveglieri, L.; Proceedings of the 1988 IEEE International Conference on Computer Design: VLSI in Computers and Processors, 1988, ICCD '88, 3 - 5 Oct., 1988, Page(s) : 490 – 495
24. Modeling Operating Systems Schedulers with Multi-Stack-Queue Grammars; Breveglieri, L.; Cherubini, A.; Crespi Reghizzi, S.; Lecture Notes in Computer Science, Fundamentals of Computation Theory, volume 1684, Springer-Verlag, 1999, Page(s): 161 – 172
25. Dedicated Circuits for the Generation of Windows in Image Processing Architectures; Antola, A.; Breveglieri, L.; The Journal of VLSI Signal Processing, volume 25, number 1, May, Springer-Verlag, 2000, Page(s): 55 – 78
26. Efficient Finite Field Digit-Serial Multiplier Architecture for Cryptography Applications; Bertoni, G.; Breveglieri, L.; Fragneto, P.; Proceedings of the Design, Automation and Test in Europe, 2001, Conference and Exhibition 2001, 13 - 16 March, 2001, Page(s): 812 –
27. A Comparative Cost/Performance Evaluation of Digit-Serial Multipliers for Finite Fields of Type GF(2n); Bertoni, G.; Breveglieri, L.; Fragneto, P.; Proceedings of the 14th Annual IEEE International ASIC / SOC Conference, 2001, 12 - 15 Sept., 2001, Page(s): 306 – 310
28. On the Propagation of Faults and their Detection in a Hardware Implementation of the Advanced Encryption Standard; Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Piuri, V.; Proceedings of the IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17 - 19 July, 2002, Page(s): 303 – 312
29. A Parity Code Based Fault Detection for an Implementation of the Advanced Encryption Standard; Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Piuri, V.; Proceedings of the 17th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, DFT 2002, 6 - 8 Nov., 2002, Page(s): 51 – 59
30. Digital Median Filters; Breveglieri, L,; Piuri, V.; The Journal The Journal of VLSI Signal Processing, volume 31, number 3, July, Springer-Verlag, 2002, Page(s): 191 – 206
31. About the Performances of the Advanced Encryption Standard in Embedded Systems with Cache Memory; Bertoni, G.; Bircan, A.; Breveglieri, L.; Fragneto, P.; Macchetti, M.; Zaccaria, V.; Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03, volume 5, 25 - 28 May, 2003, Page(s): V-145 – V-148
32. Parallel Architectures for Elliptic Curve Cryptoprocessors over Binary Extension Fields; Antola, A.; Bertoni, G.; Breveglieri, L.; Maistri, P.; Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, 2003, MWSCAS '03, volume 2, 27 - 30 Dec., 2003, Page(s): 802 – 805
33. Concurrent Fault Detection in a Hardware Implementation of the RC5 Encryption Algorithm; Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Piuri, V.; Proceedings of the IEEE International Conference on Application-Specific Systems, Architectures, and Processors, 2003., 24 - 26 June, 2003, Page(s): 423 – 432
34. Detecting and Locating Faults in VLSI Implementations of the Advanced Encryption Standard, Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Piuri, V.; Proceedings of the 18th IEEE

International Symposium on Defect and Fault Tolerance in VLSI Systems, 2003, 3 - 5 Nov., 2003, Page(s): 105 – 113

35. Efficient Software Implementation of AES on 32-Bit Platforms; Bertoni, G.; Breveglieri, L.; Fragneto, P.; Macchetti, M.; Marchesin, S.; Lecture Notes in Computer Science, Cryptographic Hardware and Embedded Systems - CHES 2002, volume 2523, Springer-Verlag, 2003, Page(s): 129 – 142
36. Finding Optimum Parallel Coprocessor Design for Genus 2 Hyperelliptic Curve Cryptosystems; Bertoni, G.; Breveglieri, L.; Wollinger, T.; Paar, C.; Proceedings of the International Conference on Information Technology: Coding and Computing, 2004, ITCC 2004, volume 2, 2004, Page(s): 538 – 544
37. Workshop on Fault Diagnosis and Tolerance in Cryptography; Breveglieri, L.; Koren, I.; 2004 International Conference on Dependable Systems and Networks, 28 June - 1 July, 2004, Page(s): 840 – 840
38. An Efficient Hardware-Based Fault Diagnosis Scheme for AES: Performances and Cost; Bertoni, G.; Breveglieri, L.; Koren, I.; Maistri, P.; Proceedings of the 19th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 2004, DFT 2004, 10 - 13 Oct., 2004, Page(s): 130 – 138
39. Detecting Faults in four Symmetric Key Block Ciphers; Breveglieri, L.; Koren, I.; Maistri, P.; Proceedings of the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2004, Page(s): 258 – 268
40. On the Generalized Linear Equivalence of Functions Over Finite Fields; Breveglieri, L.; Cherubini, A.; Macchetti, M.; Lecture Notes in Computer, Advances in Cryptology - ASIACRYPT 2004, volume 3329, Springer-Verlag, 2004, Page(s): 79 – 91
41. AES Power Attack Based on Induced Cache Miss and Countermeasure; Bertoni, G.; Zaccaria, V.; Breveglieri, L.; Monchiero, M.; Palermo, G.; International Conference on Information Technology: Coding and Computing, 2005, ITCC 2005, volume 1, 4 - 6 April, 2005, Page(s): 586 – 591
42. A Parallelized Design for an Elliptic Curve Cryptosystem Coprocessor; Sozzani, F.; Bertoni, G.; Turcato, S.; Breveglieri, L.; International Conference on Information Technology: Coding and Computing, 2005, ITCC 2005, volume 1, 4 - 6 April, 2005, Page(s): 626 – 630
43. On-line Testing for Secure Implementations: Design and Validation; Breveglieri, L.; Leveugle, R.; Nieuwland, A.; Rothbart, K.; Seifert, J.P.; 11th IEEE International On-Line Testing Symposium, 2005, IOLTS 2005, 6 - 8 July, 2005, Page(s): 211– 211
44. Incorporating Error Detection and Online Reconfiguration Into a Regular Architecture for the Advanced Encryption Standard; Breveglieri, L.; Koren, I.; Maistri, P.; 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 2005, DFT 2005, 3 - 5 Oct., 2005, Page(s): 72 – 80
45. A Complete Formulation of Generalized Affine Equivalence; Macchetti, M.; Caironi, M.; Breveglieri, L.; Cherubini, A.; Lecture Notes in Computer Science, Theoretical Computer Science, volume 3701, Springer-Verlag, 2005, Page(s): 338 – 347
46. Parallel Architectures for Elliptic Curve Cryptoprocessors over Binary Extension Fields; Antola, A.; Bertoni, G.; Breveglieri, L.; Maistri, P.; Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, 2003, MWSCAS '03, volume 2, 27 - 30 Dec., 2003, Page(s): 802 – 805
47. ECC Hardware Coprocessors for 8-bit Systems and Power Consumption Considerations; Bertoni, G.; Breveglieri, L.; Venturi, M.; Third International Conference on Information Technology: New Generations, 2006, ITNG 2006, 10 - 12 April, 2006, Page(s): 573 – 574
48. Parallel Hardware Architectures for the Cryptographic Tate Pairing; Bertoni, G.; Breveglieri, L.; Fragneto, P.; Pelosi, G.; Third International Conference on Information Technology: New Generations, 2006, ITNG 2006, 10 - 12 April, 2006, Page(s): 186 – 191

49. A Note on Error Detection in an RSA Architecture by Means of Residue Codes; Breveglieri, L.; Maistri, P.; Koren, I.; 12th IEEE International On-Line Testing Symposium, 2006, IOLTS 2006, 10 - 12 July, 2006 Page(s): 2 pp.
50. Software Implementation of Tate Pairing over GF(2/sup m/); Bertoni, G.; Breveglieri, L.; Fragneto, P.; Pelosi, G.; Sportiello, L.; Proceedings of Design, Automation and Test in Europe, 2006, DATE '06, volume 2, 6 - 10 March, 2006, Page(s): 5 pp.
51. Power Aware Design of an Elliptic Curve Coprocessor for 8 bit Platforms; Bertoni, G.; Breveglieri, L.; Venturi, M.; Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006, PerCom Workshops 2006, 13 - 17 March, 2006, Page(s): 5 pp.
52. Speeding Up AES By Extending a 32 bit Processor Instruction Set; Bertoni, G.; Breveglieri, L.; Roberto, F.; Regazzoni, F.; International Conference on Application-specific Systems, Architectures and Processors, 2006, ASAP '06, Sept., 2006, Page(s): 275 – 282
53. Performance of HECC Coprocessors Using Inversion-Free Formulae; Wollinger, T.; Bertoni, G.; Breveglieri, L.; Paar, C.; Lecture Notes in Computer Science, Computational Science and Its Applications - ICCSA 2006, volume 3982, Springer-Verlag, 2006, Page(s): 1004 – 1012
54. A Fault Attack Against the FOX Cipher Family; Breveglieri, L.; Koren, I.; Maistri, P.; Lecture Notes in Computer Science, Fault Diagnosis and Tolerance in Cryptography, volume 4236, Springer-Verlag, 2006, Page(s): 98 –105
55. Low-Power Architectures for Mobile Systems; Barretta, D.; Breveglieri, L.; Maistri, P.; Monchiero, M.; Negri, L.; Pagni, A.; Palermo, G.; Sami, M. G.; Silvano, C.; Villa, O.; Zafalon, R.; Mobile Information Systems, Springer-Verlag, 2006, Page(s): 177 – 206
56. Incorporating Error Detection in an RSA Architecture; Breveglieri, L.; Koren, I.; Maistri, P.; Ravasio, M.;Lecture Notes in Computer Science, Fault Diagnosis and Tolerance in Cryptography, volume 4236, Springer-Verlag, 2006, Page(s): 71 – 79
57. Power Attacks Resistance of Cryptographic S-boxes with Added Error Detection Circuits; Regazzoni, F.; Eisenbarth, T.; Grobschadl, J.; Breveglieri, L.; Ienne, P.; Koren, I.; Paar, C.; 22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems, 2007, DFT '07, 26 - 28 Sept., 2007, Page(s): 508 – 516
58. Countermeasures Against Branch Target Buffer Attacks; Agosta,G.; Breveglieri, L.; Pelosi,G.; Koren, I.; Workshop on Fault Diagnosis and Tolerance in Cryptography, 2007, FDTC 2007, 10 - 10 Sept., 2007, Page(s): 75 – 79
59. Programming Highly Parallel Reconfigurable Architectures for Public-Key Cryptographic Applications; Agosta, G.; Breveglieri, L.; Pelosi, G.; Sykora, M.; Fourth International Conference on Information Technology, 2007, ITNG '07, 2007, Page(s): 3 –10
60. A FPGA Coprocessor for the Cryptographic Tate Pairing over F_p; Barenghi, A.; Bertoni, G.; Breveglieri, L.; Pelosi, G.; Fifth International Conference on Information Technology: New Generations, 2008, ITNG 2008, 7 - 9 April, 2008, Page(s): 112 – 119

_____

(Luca Breveglieri)