Alessandro Barenghi

Name
Date of birth
Citizenship
Email
Web page

Position and Education

Record of Employment

2nd November 2016 – now

Assistant Professor (tenure-track path, full-time job, according to the Italian Law n. 240/2010 - art.24, paragraph 3, letter B - Senior) at the Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Italy. Academic Discipline: ING-INF/05 - Information Processing Systems. Academic recruitment field for the Italian University Research and Teaching Regulation: 09/H1 - Information Processing Systems.

2nd May 2015 – 1st November 2016

Assistant Professor (non tenure-track path, full-time job, according to the Italian Law n.240/2010 - art.24, paragraph 3, letter A) at the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Italy. Academic field for the Italian University Research and Teaching Regulation: ING-INF/05 Information Processing Systems, Academic Discipline: 09/H1 Information Processing Systems.

1st April 2013 – 30th April 2015

Post-Doctoral Research Assistant (according to the Italian law n.240/2010 - art.22) at the Department of Electronics and Computer Science of the Politecnico di Milano working on *Analysis and evaluation of methodologies and techniques for the design and securing of digital devices*.

1st April 2011 – 31st March 2013

Post-Doctoral Research Assistant (according to the Italian law n.449/1997 - art.51) at the Department of Electronics, Information and Bioengineering (DEIB) of the Politecnico di Milano working on *Study and evaluation of the design of efficient, reliable and secure digital cryptographic devices*.

1st January 2008 – 17th February 2011

Ph.D. student at the Department of Electronics and Computer Science of the Politecnico di Milano working on *Developments in side channel attacks to digital cryptographic devices: differential power and fault analysis*.

Education

- Ph.D. in Information Technology at Politecnico di Milano. Title obtained on 17 February 2011.
  Title: *Developments in side channel attacks to digital cryptographic devices: differential power and fault analysis*
  Advisor: Prof. *Luca Breveglieri*
  Reviewers: Prof. *D. Naccache*, Prof. *J.P. Seifert*, Prof. *I. Verbauwhede*,

  Minor Research Title: *Techniques for the optimization of the transfer of learning in reinforcement learning algorithms* (January 2008 - September 2009).
  Advisor: Prof. *Andrea Bonarini*.

- Italian engineering licence (Professional practice examination), 1st session 2008, Politecnico di Milano.
- M.Sc. in Computer Science Engineering. April 2007.
  Thesis title: *Innovative and complex cryptographic functions: how to efficiently compute a Tate pairing in hardware (algorithm, design methodology, architecture and evaluation)*, Advisor Prof. *Luca Breveglieri*
- Cambridge *Certificate of Proficiency in English (CPE)* - Pass Grade B, Average mark 3.9/5

VISITING EXPERIENCES

- Visiting researcher at ST Microelectronics Rousset, France (September 2009 - November 2009).
- Visiting researcher at Ruhr Universität Bochum, Bochum, Germany (February 2010 - April 2010).

SCHOLARSHIPS

- Scholarship from STMicroelectronics (January 2008 - January 2010) for Ph.D. studies at Politecnico di Milano, Italy.
- Funding for External ECRYPT II Visitor (February 2010 - April 2010) for leading research on Differential Power Analysis at EMSEC group in Ruhr Universität Bochum.

Awards

AW.8. Selection as Top Picks in Hardware and Embedded Security.

"A Code Morphing Methodology to Automate Power Analysis Countermeasures", in *Proceedings of the 49th Design Automation Conference (DAC 2012)*, San Francisco, California, USA, 3-7 June 2012, ACM, ISBN 978-1-4503-1199-1 [doi: http://dx.doi.org/10.1145/2228360.2228376]

The top picks were selected from conference papers that have appeared in leading hardware security conferences including DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, Usenix Security, ASIA CCS, NDSS, ISCA, HASP, MICRO, ASPLOS, HPCA, ACSAC and ACM CCS during the six-year period: 1/1/2012- 12/31/2017.

AW.7. HiPEAC Paper Award - 2018
"Side-channel security of superscalar CPUs: Evaluating the Impact of Microarchitectural Features" in *Proceedings of the 55th Annual Design Automation Conference, DAC'18*, San Francisco, CA, USA, June 24–29, 2018, 6 pages, New York, NY, USA, June 2018. ACM. ISBN: 978-1-4503-5700-5/18/06. (DOI: https://doi.org/10.1145/3195970.3196112

AW.6. HiPEAC Paper Award - 2015
"Information Leakage Chaff: Feeding Red Herrings to Side Channel Attackers", in *Procceedings of the 52nd Design Automation Conference (DAC 2015)*, ACM, 2015, pp. 210:1210:6 (ISBN: 978-1-4503-2730-5). [doi: http://dx.doi.org/10.1145/2593069.2593073]

AW.5. SIN 2014 Best Paper Award
"Differential Fault Analysis for Block Ciphers: an Automated Conservative Analysis" in In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN 14)*. ACM 2014, pp. 171:1-171:8, (ISBN: 978-1-4503-3033-6/14/09). [doi: http://doi.acm.org/10.1145/2659651.2659709]

AW.4. HiPEAC Paper Award - 2014
"A Multiple Equivalent Execution Trace Approach to Secure Cryptographic Embedded Software", in *Proceedings of the 51st Design Automation Conference (DAC 2014)*, ACM, 2014, pp. 210:1210:6 (ISBN: 978-1-4503-2730-5). [doi: http://dx.doi.org/10.1145/2593069.2593073]

AW.3. HiPEAC Paper Award - 2013
"Compiler-based Side Channel Vulnerability Analysis and Optimized Countermeasures Application", in *Proceedings of the 50th Design Automation Conference (DAC 2013)*, June 2-6, 2013. Austin, Texas, USA. ACM 2013.ISBN 978-1-4503-2071-9. [doi: http://dx.doi.org/10.1145/2463209.2488833]

AW.2. HiPEAC Paper Award - 2012
"A Code Morphing Methodology to Automate Power Analysis Countermeasures", in *Proceedings of the 49th Design Automation Conference (DAC 2012)*, San Francisco, California, USA, 3-7 June 2012, ACM, ISBN 978-1-4503-1199-1 [doi: http://dx.doi.org/10.1145/2228360.2228376]

AW.1. HOST 2011 Best Paper Award
"A Novel Fault Attack Against ECDSA", in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2011)*, June 5-6, 2011, San Diego, California, USA. (ISBN: 978-1-4577-1059-9). [doi: http://dx.doi.org/10.1109/HST.2011.5955015].

Teaching activity

2018-2019

Informatica ed elementi di informatica medica (39 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Biomedical Engineering - BSc-IT , Politecnico di Milano.

Algorithms and Principles of Computer Science (Theoretical Computer Science) (30 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Information Technology - Online Study Programme, Politecnico di Milano - Polo di Como.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

2017-2018

Informatica ed elementi di informatica medica (39 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Biomedical Engineering - BSc-IT , Politecnico di Milano.

Algorithms and Principles of Computer Science (Theoretical Computer Science) (30 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Information Technology - Online Study Programme, Politecnico di Milano - Polo di Como.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

2016-2017

Algorithms and Principles of Computer Science (Theoretical Computer Science) (30 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Information Technology - BSc-IT , Politecnico di Milano.

Algorithms and Principles of Computer Science (Algorithms and Data Structures) (30 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Information Technology - BSc-IT , Politecnico di Milano.

Algorithms and Principles of Computer Science (Theoretical Computer Science) (30 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Information Technology - Online Study Programme, Politecnico di Milano - Polo di Como.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (20 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. W. Fornaciari.

2015-2016

Informatica (42 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Civil Engineering - BSc-IT , Politecnico di Milano.

Lecturer for the PhD course "Energy Aware Design of Computing Systems and Applications." - Topic: Power Analysis Based Side Channel Attacks and Countermeasures (4 hours). - PhD Course in Information Technology (IT), Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (20 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. W. Fornaciari.

2014-2015

Informatica (44 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Civil Engineering - BSc-IT , Politecnico di Milano.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (20 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. W. Fornaciari.

2013-2014

Informatica (42 hours, **Lecturer**) - Undergraduate level - Bachelor of Science in Civil Engineering - BSc-IT , Politecnico di Milano.

Lecturer for the PhD course "Energy Aware Design of Computing Systems and Applications." - Topic: A Security Application of Fine Grain Power Measurement and Compiler-based Power Profile Manipulation (4 hours). - PhD Course in Information Technology (IT), Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano.

Formal Languages and Compilers (18 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (16 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. W. Fornaciari.

2012-2013

Algorithms and Principles of Computer Science - Theoretical Computer Science (20 hours, Teaching Assistant) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. M. Pradella.

Algorithms and Principles of Computer Science - Algorithms and Data Structures (20 hours, Teaching Assistant) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. M. Pradella.

Formal Languages and Compilers (14 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (16 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. W. Fornaciari.

2011-2012

Algorithms and Principles of Computer Science - Theoretical Computer Science (20 hours, Teaching Assistant) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. M. Pradella.

Algorithms and Principles of Computer Science - Algorithms and Data Structures (20 hours, Teaching Assistant) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. M. Pradella.

Formal Languages and Compilers (10 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Cryptography and Security of Digital Devices (16 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, at Politecnico di Milano, 2nd semester. Lecturer: Prof G. Pelosi

Software Platforms for Networking (16 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. G. Agosta.

2010-2011

Computer Architecture and Operating Systems (40 hours, Teaching Assistant) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. L. Breveglieri.

Software Platforms for Networking (20 hours, Teaching Assistant) - Undergraduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. G. Agosta.

Formal Languages and Compilers (10 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

2009-2010

Formal Languages and Compilers (10 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Fundamentals of Cryptography (18 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano (Campus Como), 1st semester. Lecturer:s Prof. A. Cherubini, Prof. L. Breveglieri.

2008-2009

Formal Languages and Compilers (10 hours, Teaching assistant) Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Fundamentals of Cryptography (18 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano (Campus Como), 1st semester. Lecturer:s Prof. A. Cherubini, Prof. L. Breveglieri.

Laboratory of Operating Systems and Software Design (12 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. G. Agosta.

2007-2008

Formal Languages and Compilers (10 hours, Teaching assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. L. Breveglieri.

Fundamentals of Cryptography (18 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano (Campus Como), 1st semester. Lecturer:s Prof. A. Cherubini, Prof. L. Breveglieri.

Computer Science II (48 hours, Lab Supervisor) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. L. Breveglieri.

2006-2007

Algorithms and Architectures for Cryptographic Systems (8 hours, Teaching Assistant) - Graduate level - Master of Science in Information Technology, MSc-IT, Politecnico di Milano, 1st semester. Lecturer: Prof. G. M. Bertoni.

Computer Science II (48 hours, Lab Tutor) - Undergraduate level - Bachelor of Science in Information Technology, BSc-IT, Politecnico di Milano, 2nd semester. Lecturer: Prof. L. Breveglieri.

STUDENTS SUPERVISION

Graduate Students Supervision/Co-Advisor

- *Alain Carlucci*, 2017-2018, "Achieving low-cost side channel attacks via quantitative information analysis". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Andrea Grazioso*, 2017-2018, "Enabling robust keyservers for OpenPGP: key reconciliation reengineering for the Peaks keyserver". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Mattia Pini*, 2016-2017, "PEAKS: Adding Proactive Security to OpenPGP keyservers". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Michele Madaschi*, 2016-2017, "Evaluating OpenCL Programming Practices for FPGAs: a case study on symmetric block ciphers". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Niccolò Izzo*, 2016-2017, "Reliably achieving and efficiently preventing Rowhammer attacks". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Davide Botti*, 2015-2016, "Architectural characterization of passive side channel leakage: the case of ARM Cortex-A7". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.
- *Stefano Sanfilippo*, 2015-2016, "A compiler-based technique for automated analysis and protection against side-channel attacks.". Master of Science in Engineering of Computing Systems, MScIT, Politecnico di Milano, Milano, Italy. Advisors: Prof. Gerardo Pelosi. Prof. Alessandro Barenghi.

- *Nicholas Mainardi*, 2015-2016, (in Italian) "A predicated grammar for X.509 certificates and its parser: systematically checking for syntactic soundness of digital certificates". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Alessandro Barenghi.
- *Emanuele Dedonatis*, 2015-2016, "Differential power analysis on embedded multicore platforms: experimenting with contactless power measurements". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Alessandro Barenghi.
- *Davide Macocchi*, 2014-2015, (in Italian) "Progettazione e validazione di circuiti aritmetico-logici resistenti a crittanalisi di tipo side-channel". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Alessandro Barenghi.
- *Dario Navoni*, 2013-2014, "Security in Building Automation Systems: a Study on Multi-party Key-agreement Protocols". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Alessandro Barenghi.
- *Francesco Fiduccia*, 2013-2014, "Fine-tuning of a Toolchain for the Automated Application of Side-channel Software Countermeasures". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Giovanni Agosta. Co-advisors: Dr. Gerardo Pelosi, Dr. Alessandro Barenghi
- *Michele Beretta, Alessandro Di Federico*, 2012-2013, "Security and Privacy in Social Networks". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Alessandro Barenghi.
- *Massimo Maggi, 2012-2013*, "Compiler-based Techniques to Assess the Side-channel Vulnerability of Cryptographic Implementations". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Dr. Giovanni Agosta, Alessandro Barenghi.
- *Francesco Fiduccia*, 2012-2013, "Implementation of a Toochain for the Automated Application of Side-channel Software Countermeasures". Master of Science in Information Technology, MSc-IT, Politecnico di Milano, Milano, Italy. Advisor: Prof. Gerardo Pelosi. Co-advisor: Prof. Giovanni Agosta, Alessandro Barenghi.
- *Fabio Pozzi*, 2010-2011, (in Italian) "Analisi, Progettazione e Sviluppo di Contromisure per Vulnerabilità basate su Alterazioni del Flusso di Controllo LibDefender: una libreria dinamica per garantire l'integrità del flusso di esecuzione". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Gerardo Pelosi. Co-advisor: Alessandro Barenghi.
- *Valerio Ponte, Ermes Viviani*, 2010-2011, "Parallel Scalable Parsing With Floyd Grammars". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Stefano Crespi Reghizzi. Co-advisor: Alessandro Barenghi.
- *Paolo Bottoglia*, 2010-2011, (in Italian) "Aspetti di sicurezza informatica in centri servizi di grandi dimensioni: il caso di Lombardia Informatica". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Luca Breveglieri. Co-advisor: Alessandro Barenghi.
- *Andrea Palomba*, 2009-2010, (in Italian) "Novel Differential Fault Attack to Integer Multiplication in Elliptic Curve Digital Signature Algorithm based on Special Case Discrete Logarithm". Master of Science

in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
Advisor: Prof. Luca Breveglieri. Co-advisor: Alessandro Barenghi.

- *Mauro Pellicioli*, 2008-2009, (in Italian) "Fault Attacks Against the AES Cryptographic System". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Luca Breveglieri. Co-advisor: Alessandro Barenghi.
- *Emanuele Parrinello*, 2008-2009, (in Italian) "Fault Attacks Against RSA". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Luca Breveglieri. Co-advisor: Alessandro Barenghi.
- *Antonio Parata*, 2008-2009, (in Italian) "Individuazione automatica di vulnerabilità in applicazioni PHP mediante Static Taint Analysis". Master of Science in Information Technology, MSc–IT, Politecnico di Milano, Milano, Italy.
  Advisor: Prof. Giovanni Agosta. Co-advisor: Gerardo Pelosi. Co-advisor: Alessandro Barenghi.

Professional Activities

National and International Research Projects

I contributed actively in the following research projects:

- *WorkingAge - Smart Working environments for all Ages*
  HORIZON 2020 Programme
  call: H2020-SC1-DTH-2018-1, Research and Innovation Actions (RIA)
  Grant Agreement Number: 826232
  Local project leader: Prof. Gerardo Pelosi.
- *SafeCOP - Safe Cooperating Cyber-Physical Systems using Wireless Communication*
  ECSEL Joint Undertaking Project
  Workpackage leader of "T6.1 Dissemination and Communication activities"
  call: H2020-ECSEL-2015-1-RIA, Two stage Research and Innovation Actions (RIA)
  Grant Agreement Number: 692529
  Local project leader: Prof. William Fornaciari.
- *MANGO - exploring Manycore Architectures for Next-GeneratiOn HPC systems*
  ECSEL Joint Undertaking Project
  Workpackage leader of "T2.1 Programming Models"
  call: H2020-FETHPC-2014, FET Proactive
  Grant Agreement Number: 671668
  Local project leader: Prof. William Fornaciari.
- *M^2DC - Modular Microserver DataCentre*
  HORIZON 2020 Programme
  Research and Innovation Actions (RIA) call: H2020-ICT-2015 - topic : ICT-04-2015
  Grant Agreement Number: 688201
  Local project leader: Prof. William Fornaciari.
- *TOISE - Trusted Computing for European Embedded Systems*,
  ENIAC Joint Undertaking Project
  JTI-CP-ENIAC - Joint Technology Initiatives - Collaborative Project (ENIAC)

Grant Agreement Number282557 Local project leader: prof. Luca Breveglieri

Conference and Workshop Organization

Program Chair and Organization Committees

- Co-chair and Co-Organizer of the 5th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Valencia, Spain, 24th January 2019. Proc. ACM.
- Co-chair and Co-Organizer of the 5th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Manchester, UK, 24th January 2018. Proc. ACM. (ISBN: 978-1-4503-6374-7)
- Co-chair and Co-Organizer of the 4th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Stockholm, Sweden, 24 January 2017. Proc. ACM. (ISBN: 978-1-4503-4065-6)
- Co-chair and Co-Organizer of the 3rd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Prague, Czech Republic, 19th January 2016. Proc. ACM. (ISBN: 978-1-4503-4065-6)
- Registration Chair for the ACM International Conference on Computing Frontiers 2016 Como, Italy, 16th - 18th May 2016. Proc. ACM.
- Co-chair and Co-Organizer of the 2nd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Amsterdam, The Netherlands, 19th January 2015. Proc. ACM. (ISBN: 978-1-4503-3187-6)
- Co-Organizer of the 1st HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2), Vienna, Austria, 20th January 2014. Proc. ACM. (ISBN: 978-1-4503-2484-7)

Program Committee Membership

I am a member of the Program Committee of the following conferences:

- International Conference on Information Systems Security and Privacy - ICISSP - (2015-2019). Proc. INSTCC.
- Workshop on Security Proofs for Embedded Systems - PROOFS - (2012 to 2017), Proc. Springer.
- ACM Conference on Computing Frontiers (2017)
- 7th International Conference on Security of Information and Networks - SIN - (2014-2016). Proc. ACM.
- Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2012). Proc IEEE-CPS.

Referee and Chair services

I acted as a reviewer for the following conferences/journals:

- ACM Transactions on Design Automation of Electronic Systems (TODAES)
- IEEE Transactions on Computers (TC)
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
- IEEE Transactions on VLSI Systems (TVLSI)
- IEEE Transactions on Information Forensics and Security (TIFS)

- IEEE Transactions on Parallel and Distributed Systems (TPDS)
- IEEE Transactions on Emerging Topics in Computing (TETC)
- IEEE Systems Journal - Special Issue on Security and Privacy in Complex Systems
- Journal VLSI Integration - Elsevier
- Journal of Systems and Software - Elsevier
- ACM/IEEE Design Automation Conference (DAC 2012 to 2016 as external reviewer, 2015 as expert reviewer)
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2015 as external reviewer)
- IEEE/ACM International Conference on Design Automation and Test in Europe (DATE 2011-2013-2014) (external reviewer)
- International Smart Card Research and Advanced Application Conference (CARDIS 2017-2018)
- International Conference on Security and Cryptography (SECRYPT 2011-2012-2014) (external reviewer)
- IEEE International Symposium on Computer Arithmetic (ARITH 2013)
- IEEE Symposium on Hardware-Oriented Security and Trust (HOST 2011-2012)

My Erdős Number is 2 : (Alessandro Barenghi $\rightarrow$ Israel Koren $\rightarrow$ Paul Erdős).

Talks and Tutorials

INVITED TALKS

- Panel session: "Does the Internet of Things need hardware security?" at the Workshop on Malicious Software and Hardware in Internet of Things, (MAL-IoT 2016) Como, Italy, 16th May 2016.
- Keynote speech: "Turning security from a feature into a design guideline" at Workshop on Practical Hardware Innovations in Security Implementation and Characterization (PHISIC 2013), 13-14 June 2013, held at the Centre Microélectronique de Provence, Gardanne
- "GPGPU Acceleration of Cryptographic Applications", at the IEEE/ACM Workshop on Designing for Embedded Parallel Computing Platforms: Architectures, Design Tools, and Applications. Design Automation and Test in Europe, March 12, 2010, DATE 2010, Poster Session (w/o Proceedings).
- "Fault attacks to AES with every key length" March 16, 2010, held at UCL Crypto Group, Université catholique de Louvain, Louvain-la-neuve Belgium.
- "Attacking AES 256 Through Low Voltage Faults" April 15, 2010, held at Horst Görtz Institut für IT-Sichereit, Ruhr Universität Bochum, Bochum, Germany.

POSTER (PEER-REVIEWED) – INTERACTIVE PRESENTATIONS

- Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi and Michele Scandale. 2016. "Encasing Block Ciphers to Foil Key Recovery Attempts via Side Channel", Work-in-Progress session at the 2016 Design Automation Conference (DAC'16), June 5, 2016, Austin, TX, USA.
- Giovanni Agosta, Alessandro Barenghi, Massimo Maggi and Gerardo Pelosi. 2014. "Extending the Design Space for Secure Embedded System Design", Work-in-Progress session at the 2014 Design Automation Conference (DAC'14), June 5, 2014, San Francisco, CA, USA.
- Gerardo Pelosi in collaboration with Giovanni Agosta, Alessandro Barenghi, and Massimo Maggi. 2014. "Compiler-based Side Channel Analysis". Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures and Design Tools and Architectures for Multicore Embedded Computing Platform - PARMA-DITAM 2014 (Poster Submission Session), January 20, 2014, Vienna, Austria.

SUMMER SCHOOLS

- ECRYPT II Winter School: Mathematical Foundations in Cryptography at EPFL, Lausanne, Switzerland.

Complete publication list

The research activity concerning publications involving multiple authors took place in a tightly knit collaboration among them, thus the contribution of each one of them to the publication itself is to be considered equal.

PUBLICATION LIST

Bibliometry: Google Scholar (All - 2014): Citations 1453 - 1121, h-index 20 - 16, i10-index 30 - 26; Scopus: Citations 902, h-index: 15

REFEREED INTERNATIONAL JOURNALS

IJ.16. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Reactive Side-channel Countermeasures: Applicability and Quantitative Security Evaluation". *Microprocessors and Microsystems Journal*, Volume 62 (October 2018), pages 50-60. ISSN: 0141-9331 (print). Elsevier 2018.
(DOI: https://doi.org/10.1016/j.micpro.2018.07.001)

IJ.15. Davide Zoni, Alessandro Barenghi, Gerardo Pelosi, and William Fornaciari. "A Comprehensive Side-Channel Information Leakage Analysis of an In-Order RISC CPU Microarchitecture". *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 23, issue 5, Article 57 (August 2018), 30 pages.
ISSN: 1084-4309, EISSN:1557-7309 (DOI: https://doi.org/10.1145/3212719)

IJ.14. Alessandro Barenghi, Nicholas Mainardi, Gerardo Pelosi. "Systematic Parsing of X.509: Eradicating Security Issues with a Parse Tree". *Journal of Computer Security (JCS)*, vol. 26, no. 6, pp. 817–849. October 30th, 2018. ISSN: 0926-227X (Print), 1875-8924 (Online). (DOI: http://dx.doi.org/10.3233/JCS-171110)

IJ.13. A. Oleksiaka, M. Kierzynkaa, G. Agosta, A. Barenghi, C. Brandolese, W. Fornaciari, Gerardo Pelosi *et. al.*
"M2DC – Modular Microserver DataCentre with Heterogeneous Hardware", *Microprocessors and Microsystems Journal*, Volume 52, pages 117–130, July 2017. ISSN: 0141-9331 (print). Elsevier 2017.
(DOI: https://doi.org/10.1016/j.micpro.2017.05.019)

IJ.12. Alessandro Barenghi, Michele Beretta, Alessandro Di Federico, and Gerardo Pelosi, "A privacy-preserving encrypted OSN with stateless server interaction: the Snake design". In *Computers & Security Journal (CoSe)*, Volume 63, pages 67–84, November 2016. ISSN: 0167-4048 (print). Elsevier 2016.
(DOI: http://dx.doi.org/10.1016/j.cose.2016.09.005)

IJ.11. Alessandro Barenghi, Stefano Crespi Reghizzi, Dino Mandrioli, Federica Panella, and Matteo Pradella, "Parallel Parsing Made Practical", *Science of Computer Programming*, vol.112, no. 3, pp. 195-226, 2015, Elsevier, ISSN: 0167-6423.
(DOI: http://dx.doi.org/doi:10.1016/j.scico.2015.09.002)

IJ.10. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Gerardo Pelosi, Stefano Sanfilippo, Ruggero Susella.
"A Fault-based Secret Key Retrieval Method for ECDSA: Analysis and Countermeasure". *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, Vol. 13, No. 1, Article 8, pages: 1–26, April 2016. ISSN: 1550-4832 (Print), 1550-4840 (Online). (DOI: http://dx.doi.org/10.1145/2767132)

IJ.9. Giovanni Agosta, Alessandro Barenghi, and Alessandro Di Federico, and **Gerardo Pelosi**. "OpenCL Performance Portability for General-purpose Computation on Graphics Processor Units: an Exploration on Cryptographic Primitives". *Concurrency and Computation: Practice and Experience (CCPE)*, Volume 27, Issue 14, pages 3633–3660, ISSN: 1532-0634 (Print). September 2015. (DOI: http://dx.doi.org/10.1002/cpe.3358)

IJ.8. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "The MEET Approach: Securing Cryptographic Embedded Software against Side Channel Attacks". *IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 34(8):1320 - 1333, August 2015. IEEE. ISSN: 0278-0070 (Print).
(DOI: http://dx.doi.org/10.1109/TCAD.2015.2430320)

IJ.7. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Trace-based Schedulability Analysis to Enhance Passive Side-Channel Attack Resilience of Embedded Software". *Information Processing Letters (IPL)*,

115(2):292–297, February 2015. Elsevier. ISSN: 0020-0190 (Print).
(DOI: http://dx.doi.org/10.1016/j.ipl.2014.09.030)

IJ.6. Giovanni Agosta, Alessandro Barenghi, Massimo Maggi, and **Gerardo Pelosi**. "Design Space Extension for Secure Implementation of Block Ciphers". *IET Computers & Digital Techniques – Special issue: Hardware Security*, Vol. 8, Issue 6, pp. 256–263, November 2014. ISSN: 1751-8601 (Print), 1751-861X (Online).
(DOI: http://dx.doi.org/10.1049/iet-cdt.2014.0037)

IJ.5. Alessandro Barenghi, Cédric Hocquet, David Bol, François-Xavier Standaert, Francesco Regazzoni, and Israel Koren, " A Combined Design-Time/Test-Time Study of the Vulnerability of Sub-Threshold Devices to Low Voltage Fault Attacks", *IEEE Transactions on Emerging Topics in Computing*, vol. 2 , no. 2, pp 107-118, IEEE, 2014. ISSN: 2168-6750. (DOI: http://dx.doi.org/10.1109/tetc.2014.2316509)

IJ.4. Alessandro Barenghi, Gerardo Pelosi, and Federico Terraneo. "Secure and Efficient Design of Block Cipher Implementations on Microcontrollers". *International Journal of Grid and Utility Computing (JGUC)*, 4(2/3):110–118, September 2013. ISSN: 1741-847X (Print), 1741-8488 (Online). (DOI: http://dx.doi.org/10.1504/IJGUC.2013.056246)

IJ.3. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, and **Gerardo Pelosi**. "A Fault Induction Technique Based on Voltage Underfeeding with Application to Attacks against AES and RSA". *Journal of Systems and Software (JSS)*, 86(7):1864–1878, July 2013. ISSN: 0164-1212. (DOI: http://dx.doi.org/10.1016/j.jss.2013.02.021)

IJ.2. Alessandro Barenghi, Stefano Crespi Reghizzi, Dino Mandrioli, and Matteo Pradella, "Parallel Parsing of Operator Precedence Grammars" *Information Processing Letters*, vol. 113, no.7, pp. 245-249, Elsevier 2013, ISSN 0020-0190 (DOI: http://dx.doi.org/10.1016/j.ipl.2013.01.008)

IJ.1. Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice and Countermeasures" *Proceedings of the IEEE*,vol. 100, no. 11, pp. 3056-3076, IEEE, 2012, ISSN: 0018-9219 (DOI: http://dx.doi.org/10.1109/JPROC.2012.2188769)

EDITORIAL CONTRIBUTIONS

ED.5. Giovanni Agosta, Alessandro Barenghi, Israel Koren, Karine Heydemann, and Gerardo Pelosi (Editors). Proceedings of the 6th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2 '19). Valencia, Spain, 21 January 2019 ACM New York, NY, USA. 2019.
ISBN: 978-1-4503-6182-8. (URL: http://dl.acm.org/)

ED.4. Giovanni Agosta, Alessandro Barenghi Gerardo Pelosi (Editors). Proceedings of the 5th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2 '18). Manchester, United Kingdom, 24 January 2018 ACM New York, NY, USA. 2018.
ISBN: 978-1-4503-6374-7. (URL: https://dl.acm.org/citation.cfm?id=3178291)

ED.3. Giovanni Agosta, Alessandro Barenghi, Israel Koren, Gerardo Pelosi (Editors). Proceedings of the 4th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2 '17). Stockholm, Sweden, 24 January 2017 ACM New York, NY, USA. 2017.
ISBN: 978-1-4503-4869-0. (URL: http://dl.acm.org/citation.cfm?id=3031836)

ED.2. Giovanni Agosta, Alessandro Barenghi, Israel Koren, Gerardo Pelosi (Editors). Proceedings of the 3rd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2 '16). Prague, Czech Republic, 20th January 2016. ACM New York, NY, USA. 2016.
ISBN: 978-1-4503-4065-6.(URL: http://dl.acm.org/citation.cfm?id=2858930)

ED.1. Gerardo Pelosi, Israel Koren, Alessandro Barenghi, Giovanni Agosta. (Editors). Proceedings of the 2nd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS2'15). Amsterdam, The Netherlands, 19th January, 2015. ACM New York, NY, USA. 2015.
ISBN: 978-1-4503-3187-6 (DOI: http://dl.acm.org/citation.cfm?id=2694805)

REFEREED CHAPTERS IN INTERNATIONAL BOOKS

IB.7. Ariel Oleksiak, Giovanni Agosta, Alessandro Barenghi, Carlo Brandolese, William Fornaciari, Gerardo Pelosi, *et.al.* "M2DC - A Novel Heterogeneous Hyperscale Microserver Platform". In Christoforos Kachris, Babak Falsafi, Dimitrios Soudris, editors, *Hardware Accelerators in Data Centers*, pages 155–174. Springer International Publishing, Switzerland, August 2017. ISBN: xxx-x-xxx-xxxxx-x (Print) xxx-x-xxx-xxxxx-x (Online).
(DOI: http://dx.doi.org/101007/xxx-x-xxx-xxxxx-x_x) [to appear]

IB.6. Alessandro Barenghi, Luca Breveglieri, Andrea Palomba, and Gerardo Pelosi. "Fault Sensitivity Analysis at Design Time". In Bernard Candaele, Dimitrios Soudris, Iraklis Anagnostopoulos, editors, *Trusted Computing for Embedded*

Systems, pages 175-186. Springer International Publishing, Switzerland, January 2015. ISBN: 978-3-319-09419-9 (Print) 978-3-319-09420-5 (Online). (DOI: http://dx.doi.org/101007/978-3-319-09420-5_9)

IB.5. Alessandro Barenghi, Luca Breveglieri, Mariagrazia Fugini, and Gerardo Pelosi. "Computer Security Anchors in Smart Grids: The Smart Metering Scenario and Challenges". In Bernard Candaele, Dimitrios Soudris, Iraklis Anagnostopoulos, editors, *Trusted Computing for Embedded Systems*, pages 175-186. Springer International Publishing, Switzerland, January 2015. ISBN: 978-3-319-09419-9 (Print) 978-3-319-09420-5 (Online). (DOI: http://dx.doi.org/101007/978-3-319-09420-5_9)

IB.4. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Symmetric Key Encryption Acceleration on Heterogeneous Many- Core Architectures", In Saiful Azad and Al-Sakib Khan Pathan, editors, *Practical Cryptography: Algorithms and Implementations using C++*, pages 251-297. CRC Press, Taylor & Francis Group, Boca Raton, Florida, USA, December 2014. ISBN: 978-1-4-822-28892 (Print).

IB.3. Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, Fabrizio De Santis, Filippo Melzani, Andrea Palomba, Gerardo Pelosi, "Design Time Engineering of Side Channel Resistant Cipher Implementations", in Atilla Elçi et al. editors, *Theory and Practice of Cryptography Solutions for Secure Information Systems*. Advances in Information Security, Privacy, and Ethics (AISPE) Book Series. IGI Global. Editors: Atilla Eli et al., May 2013. ISBN: 978-1-466-64030-6, e-ISBN: 978-1-466-64031-3. (DOI: http://dx.doi.org/10.4018/978-1-4666-4030-6]

IB.2. Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, Mauro Pellicioli, Gerardo Pelosi, "Injection Technologies for Fault Attacks on Microprocessors" in In Marc Joye and Michael Tunstall, editors, *Fault Analysis in Cryptography, Information Security and Cryptography*, pages 275-293. Springer, Berlin, Heidelberg, November 2012. ISBN: 978-3-642-29655-0 (Print), 978-3-642-29656-7 (Online), ISSN: 1619-7100. (DOI: http://dx.doi.org/10.1007/978-3-642-29656-7_16]

IB.1. Alessandro Barenghi, Elena Trichina, "Fault Attacks on Stream Ciphers" in In Marc Joye and Michael Tunstall, editors, *Fault Analysis in Cryptography, Information Security and Cryptography*, pages 239-255. Springer, Berlin, Heidelberg, November 2012. ISBN: 978-3-642-29655-0 (Print), 978-3-642-29656-7 (Online), ISSN: 1619-7100. (DOI: http://dx.doi.org/10.1007/978-3-642-29656-7_16]

REFEREED INTERNATIONAL CONFERENCES

IC.49. Alessandro Barenghi, Nicholas Mainardi and Gerardo Pelosi, "Comparison-Based Attacks Against Noise-free Fully Homomorphic Encryption Schemes". In *Proceedings of the 20th International Conference on Information and Communications Security, ICICS 2018, October 29-31, 2018. Lille, France*, David Naccache and Shouhuai Xu and Sihan Qing and Pierangela Samarati and Gregory Blanc and Rongxing Lu (editors), Volume 11149 of Lecture Notes in Computer Science, pages 117–191, Springer, Cham 2018. ISBN: 978-3-030-01949-5 (Print) 978-3-030-01950-1 (Online). Copyright: Springer Nature Switzerland AG 2018. Also part of the Security and Cryptology book sub series,
Print ISSN: 0302-9743. Series Online ISSN: 1611-3349
(DOI: https://doi.org/10.1007/978-3-030-01950-1_11)

IC.48. Alessandro Barenghi, Luca Breveglieri, Niccolò Izzo, Gerardo Pelosi, "Software-only Reverse Engineering of Physical DRAM Mappings for Rowhammer Attacks". In Magdy S. Abadir, Ilia Polian, Sohrab Aftabjahani, and Yier Jin (editors), *Proceedings of the 2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, July 2-4, 2018, Platja d'Aro, Costa Brava, Spain, pages 19-24, New York, NY, USA, October 2018. IEEE.
Electronic ISBN: 978-1-5386-6544-2. Print on Demand(PoD) ISBN: 978-1-5386-6545-9. IEEE Part Number: CFP18G73-ART. (DOI: http://dx.doi.org/10.1109/IVSW.2018.8494868)

IC.47. Alessandro Barenghi, Michele Madaschi, Nicholas Mainardi and Gerardo Pelosi, "OpenCL HLS Based Design of FPGA Accelerators for Cryptographic Primitives". In Stephen Jarvis, Bahman Javadi, and Song Guo (editors), *Proceedings of the International Conference on High Performance Computing & Simulation (HPCS 2018)*. July 16–20, 2018. Orléans, France, pp. 634-641. IEEE 2018. ISBN: 978-1-5386-7879-4 (Electronic). ISBN: 978-1-5386-7878-7 (Print). ISBN: 978-1-5386-7880-0 (Print on Demand(PoD)). (DOI: https://doi.org/10.1109/HPCS.2018.00105)

IC.46. Alessandro Barenghi and Gerardo Pelosi, "Side-channel security of superscalar CPUs: Evaluating the Impact of Microarchitectural Features". In Sharon Hu, Rob Aitken and Anand Raghunathan (editors), *Proceedings of the 55th Annual Design Automation Conference, DAC'18*, San Francisco, CA, USA, June 24–29, 2018, 6 pages, New York, NY, USA, June 2018. ACM. ISBN: 978-1-4503-5700-5/18/06. (DOI: https://doi.org/10.1145/3195970.3196112)

IC.45. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, and Paolo Santini, "LEDAkem: A Post-quantum Key Encapsulation Mechanism Based on QC-LDPC Codes". In Tanja Lange and Rainer Steinwandt (editors), Proceedings of *The Ninth International Conference on Post-Quantum Cryptography (PQCrypto 2018)*, Fort Lauderdale, Florida, April 9-11, 2018. Proceedings. Lecture Notes in Computer Science volume 10786, also part of the Security and Cryptology subseries, pages: 1–22, Springer International Publishing AG, part of Springer Nature 2018. Springer, Cham

2018. Print ISBN 978-3-319-79062-6, Online ISBN 978-3-319-79063-3. Series Print ISSN 0302-9743. Series Online ISSN 1611-3349. (DOI: https://doi.org/10.1007/978-3-319-79063-3_1)

IC.44. Alessandro Barenghi, Nicholas Mainardi, and Gerardo Pelosi, "A Security Audit of the OpenPGP Format". In S. Jarvis, L. Liu, B. Javadi, S. Guo (editors), Proceedings of the *11th International Conference on Frontier of Computer Science and Technology (FCST-2017)*, Exeter, England, UK, 21-23 June 2017, pages 336-343. IEEE 2017. eISBN: 978-1-5386-0840-1. Print on Demand(PoD) ISBN: 978-1-5386-0841-8. eISSN: 2375-527X.
(DOI: http://dx.doi.org/10.1109/ISPAN-FCST-ISCC.2017.35)

IC.43. Alessandro Barenghi, Nicholas Mainardi and Gerardo Pelosi. "A Novel Regular Format for X.509 Digital Certificates". In Shahram Latifi (editor) *Information Technology: New Generations*. Proceedings of the *14th International Conference on Information Technology (ITNG 2017), April 10-12, 2017, Las Vegas, Nevada, USA*. Series in Advances in Intelligent Systems and Computing, volume 558, pages: 133–139, Springer International Publishing 2018.
First Online: 18 July, 2017. ISBN 978-3-319-54977-4 (Print), ISBN 978-3-319-54978-1 (eBook). series ISSN 2194-5357, ISSN 2194-5365 (electronic). (DOI: http://dx.doi.org/10.1007/978-3-319-54978-1_18)

IC.42. Alessandro Barenghi and Gerardo Pelosi. "An Enhanced Dataflow Analysis to Automatically Tailor Side Channel Attack Countermeasures to Software Block Ciphers". In A. Armando, R. Baldoni, R. Focardi (editors), Proceedings of the *Italian Conference on Cyber Security (ITA-SEC 2017), 17-20 January 2017, Venice, Italy*, pages: 8–18, CEUR Workshop Proceedings 2017, Vol-1816, ISSN 1613-0073. 2017. (http://ceur-ws.org/Vol-1816/paper-02.pdf)

IC.41. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Encasing Block Ciphers to Foil Key Recovery Attempts via Side Channel". In Sri Parameswaran and Frank Liu (editors), *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2016), Austin, TX, USA, November 07-10, 2016, Austin, TX, USA*, pages 1–8. New York, NY, USA, November 2016. ACM. ISBN: 978-1-4503-4466-1/16/11.
(DOI: http://dx.doi.org/10.1145/2966986.2967033)

IC.40. Alessandro Barenghi and Gerardo Pelosi, "A Note on Fault Attacks against Deterministic Signature Schemes". In *Proceedings of the 11th International Workshop on Security - Advances in Information and Computer Security (IWSEC 2016), Akihabara-Ochanomizu District, Tokyo, Japan, September 12–14, 2016*, Kazuto Ogawa and Katsunari Yoshioka (editors), Volume 9836 of Lecture Notes in Computer Science, pages 182–192, Springer 2016.
ISBN: 978-3–319-44523-6 (Print) 978-3-319-44524-3 (Online), ISSN: 0302-9743.
(DOI: http://dx.doi.org/10.1007/978-3-319-44524-3_11)

IC.39. Giovanni Agosta, Alessandro Barenghi, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Stefano Delucchi, Massimo Massa, Maurizio Mongelli, Enrico Ferrari, Leonardo Napoletani, Luciano Bozzi, Carlo Tieri, Dajana Cassioli and Luigi Pomante, "V2I Cooperation for Traffic Management with SafeCOP". In Proceedings of the *19th Euromicro Conference on Digital System Design (DSD 2016)*, Special Session on Architectures & Systems for Automotive & Intelligent Transportations, August 31 - September 2, 2016. Limassol, Cyprus, pages 621–627, New York, NY, USA, IEEE 2016. ISBN: 978-1-5090-2818-4 (Print) 978-1-5090-2817-7 (Online) (DOI: http://dx.doi.org/10.1109/DSD.2016.18)

IC.38. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, "Automated Instantiation of Side-Channel Attacks Countermeasures for Software Cipher Implementations". In Gianluca Palermo and John Feo (editors), *Proceedings of the 13th ACM International Conference on Computing Frontiers (CF'16), Como, Italy, May 16-19, 2016*, pages 455–460, New York, NY, USA, May 2016. ACM. ISBN: 978-1-4503-4128-8/16/05.
(DOI: http://dx.doi.org/10.1145/2903150.2911707)

IC.37. Alessandro Barenghi, Alessandro Di Federico, Gerardo Pelosi, and Stefano Sanfilippo. "Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-proof?" In Pernul G. and Peter Y. A. Ryan and Edgar Weipp (editors), In *Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS '15)*, Vienna, Austria, September 23-25, 2015, volume 9326 of Lecture Notes in Computer Science, pages 1-18, Springer International Publishing. ISBN: 978-3-319-24173-9 (Print) 978-3-319-24174-6 (Online), ISSN: 0302-9743. (DOI: http://dx.doi.org/10.1007/978-3-319-24174-6_22)

IC.36. Giovanni Agosta, Alessio Antonini, Alessandro Barenghi, Dario Galeri, and Gerardo Pelosi. Cyber-Security Analysis and Evaluation for Smart Home Management Solutions. In Jing Yang Jou, Yen Hsyang Chu, Yin-Yi Lin, and Yen-Wen Chen (editors) *Proceedings of the 49th IEEE International Conference on Security Technology (ICCST 2015)*, Taipei, Taiwan, R.O.C., 21-24 September, 2015, pages 1-6, IEEE. ISBN: 978-1-4799-8690-3 (Print). (DOI: http://dx.doi.org/10.1109/CCST.2015.7389663)

IC.35. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Information Leakage Chaff: Feeding Red Herrings to Side Channel Attackers". In Sharon Hu and Rob Aitken (editors), *Proceedings of the 52nd Annual Design Automation Conference, DAC'15*, San Francisco, CA, USA, June 7-11, 2015, pages 1-6, New York, NY, USA, June 2015. ACM. ISBN: 978-1-4503-3520-1/15/06. (DOI: http://dx.doi.org/10.1145/2744769.2744859)

IC.34. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Towards Transparently Tackling Functionality and Performance Issues Across Different OpenCL Platforms". In *Proceedings of the International Symposium*

on Computing and Networking - Across Practical Development and Theoretical Research - (CANDAR 2014) Mt. Fuji, Shizuoka, Japan - December 10-12, 2014, pages 130-136, Piscataway, NJ, USA,December 2014. IEEE. ISBN: 978-1-4799-4152-0/14 (Print). (DOI: http://dx.doi.org/10.1109/CANDAR.2014.53)

IC.33. Alessio Antonini, Alessandro Barenghi, Gerardo Pelosi, and Saman Zonouz, "Security Challenges in Building Automation and SCADA", *Proceedings of the 48th IEEE International Conference on Security Technology (ICCST 2014)*, Rome, Italy, 13-16 October, 2014, pages 176-181, IEEE. ISBN: 978-1-4799-3530-7 (Print). (DOI http://dx.doi.org/10.1109/CCST.2014.6986996)

IC.32. Giovanni Agosta, Alessandro Barenghi, and Gerardo Pelosi, "Securing Software Cryptographic Primitives for Embedded Systems against Side Channel Attacks", *Proceedings of the 48th IEEE International Conference on Security Technology (ICCST 2014)*, Rome, Italy, 13-16 October, 2014, pages 382-387, IEEE. ISBN: 978-1-4799-3530-7 (Print). (DOI http://dx.doi.org/10.1109/CCST.2014.6986996)

IC.31. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. "Differential Fault Analysis for Block Ciphers: an Automated Conservative Analysis". In Ron Poet, Atilla Elçi, Manoj Singh Gaur, Mehmet A. Orgun, and Oleg B. Makarevich, editors, in Proceedings of the *7th International Conference on Security of Information and Networks*, SIN '14, Glasgow, Scotland UK September, 9-11, 2014, pages 171:1-171:8, New York, NY, USA, September 2014. ACM. ISBN: 978-1-4503-3033-6/14/09. **Best Paper Award**. (DOI: http://dx.doi.org/10.1145/2659651.2659709]

IC.30. Alessandro Barenghi and Gerardo Pelosi. "On the Security of Partially Masked Software Implementations". In Pierangela Samarati, editor, SECRYPT 2014 - Proceedings of the *11th International Conference on Security and Cryptography*, Vienna, Austria, 28-30 August, 2014, pages 492-499. SciTePress, August 2014. ISBN: 978-989-758-045-1 (Print) /http://dx.doi.org/10.1145/2744769.2744859).

IC.29. Alessandro Barenghi, Michele Beretta, Alessandro Di Federico, and Gerardo Pelosi, "Snake: an End-to-End Encrypted Online Social Network". In Julien Bourgeois and Frédéric Magoulès, editors, in *Proceedings of the 6th International Symposium on Cyberspace Safety and Security (CSS 2014)*, Paris, France, 20-22 August, 2014, pages 775-782, Piscataway, NJ, USA, August 2014. IEEE Computer Society. ISBN: 978-1-4799-6123-8/14 (Print). (DOI: http://dx.doi.org/10.1109/HPCC.2014.128)

IC.28. Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. *A Multiple Equivalent Execution Trace Approach to Secure Cryptographic Embedded Software*, in Soha Hassoun, Charles Alpert, and Sharon Hu, editors, *Proceedings of the 51th Annual Design Automation Conference, DAC '14*, San Francisco, CA, USA, June 1-5, 2014, pages 1-6, New York, NY, USA, May 2014. ACM. ISBN: 978-1-4503-2730-5/14/06 (Print). (DOI: http://dx.doi.org/10.1145/2593069.2593073)

IC.27. Alessandro Barenghi, Stefano Crespi Reghizzi, Dino Mandrioli, Federica Panella, Matteo Pradella, "The PAPAGENO parallel-parser generator", in *Proceedings of the 23rd International Conference on Compiler Construction*, April 7th, 2014, In Albert Cohen, editor, Volume 8409 of Lecture Notes in Computer Science, pages 192-196, Springer, Heidelberg, ISBN: 978-3-642-54806-2, (DOI: http://dx.doi.org/10.1007/978-3-642-54807-9_11)

IC.26. Alessio Antonini, Alessandro Barenghi, Gerardo Pelosi, "Security Analysis of Building Automation Networks: Threat Model and Viable Mitigation Techniques", in *Proceedings of the 18th Nordic Conference on Secure IT Systems* (NordSec 2013), October 18-21, 2013, Ilulissat, Greenland. Volume 8208 of Lecture Notes in Computer Science, pages 199-214, Berlin, Heidelberg, October 2013. Springer Berlin Heidelberg. ISBN: 978-3-642-41487-9 (Print) 978-3-642-41488-6 (Online), ISSN: 0302-9743. (DOI: http://dx.doi.org/10.1007/978-3-642-41488-6_14)

IC.25. Giovanni Agosta, Alessandro Barenghi, Massimo Maggi, Gerardo Pelosi, "Compiler-based Side Channel Vulnerability Analysis and Optimized Countermeasures Application", *Proceedings of the 50th Design Automation Conference (DAC 2013)*, Austin, TX, USA, May 29-June 7, 2013, pages 81:1-81:6, New York, NY, USA, May 2013. ACM. ISBN: 978-1-4503-2071-9 (DOI: http://dx.doi.org/10.1145/2463209.2488833)

IC.24. Giovanni Agosta, Alessandro Barenghi, Michele Scandale, Gerardo Pelosi, "Enhancing Passive Side-Channel Attack Resilience through Schedulability Analysis of Data-Dependency Graphs", in Proceedings of the 7th International Conference on Network and System Security (NSS 2013). June 3-4, 2013. Madrid, Spain. Springer- LNCS 7873, Lopez, Javier; Huang, Xinyi; Sandhu, Ravi (Eds.) 2013. ISBN: 978-3-642-38630-5, ISSN 0302-9743. (DOI: http://dx.doi.org/10.1007/978-3-642-38631-2_58)

IC.23. Alessandro Barenghi, Gerardo Pelosi and Fabio Pozzi, "Drop-In Control Flow Hijacking Prevention through Dynamic Library Interception", in Proceedings of the 10th International Conference on Information Technology - Software Security Track, April 15-17, 2013, Las Vegas, Nevada, USA. IEEE-CS 2013. pp. 640-647. ISBN: 978-0-7695-4967-5. (DOI: http://dx.doi.org/10.1109/ITNG.2013.99)

IC.22. Alessandro Barenghi, Gerardo Pelosi and Francesco Regazzoni "Simulation-Time Security Margin Assessment against Power-Based Side Channel Attacks",in *Proceedings of the 7th Workshop on Embedded Systems Security (WESS 2012)*, October 12, 2012, Tampere, Finland, ACM 2012. ISBN: 978-1-4503-1286-8/12/10.

IC.21. Alessandro Barenghi, Ermes Viviani, Stefano Crespi Reghizzi, Dino Mandrioli and Matteo Pradella. "PAPAGENO: a parallel parser generator for operator precedence grammars", in Proceedings of the 5th International Conference on Software Language Engineering, Dresden, Germany, September 25-28, 2012, Lecture Notes in Computer Science, volume 7745, pp 264-274, Springer, ISBN: 978-3-642-36088-6. (DOI: http://dx.doi.org/10.1007/978-3-642-36089-3_15)

IC.20. Giovanni Agosta, Alessandro Barenghi and Gerardo Pelosi "A Code Morphing Methodology to Automate Power Analysis Countermeasures", in Proceedings of the 49th Design Automation Conference (DAC), San Francisco, California, USA, 3-7 June 2012, ACM, ISBN 978-1-4503-1199-1. (DOI: http://dx.doi.org/10.1145/2228360.2228376)

IC.19. Giovanni Agosta, Alessandro Barenghi and Gerardo Pelosi "Exploiting Bit-level Parallelism in GPGPUs: a Case Study on KEELOQ Exhaustive Key Search Attack", in Proceedings of PARMA 2012 - 3rd Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures. 28-29 February 2012, Munich, Germany, GI Edition - Lecture Notes in Informatics (LNI) series. Society for Computer Science, Volume P-200, pp. 385-396. Editors: Gero Mühl, Jan Richling, and Andreas Herkersdorf. ISBN 978-3-88579-294-9, ISSN 1617-5468.

IC.18. Giovanni Agosta, Alessandro Barenghi, Antonio Parata and Gerardo Pelosi "Automated Security Analysis of Dynamic Web Applications through Symbolic Code Execution", in Proceedings of the 9th International Conference on Information Technology: New Generations (ITNG 2012), Las Vegas, Nevada, USA, April 16-18, 2012. IEEE Computer Society. ISBN 978-0-7695-4654-4. (DOI: http://dx.doi.org/10.1109/ITNG.2012.167)

IC.17. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Andrea Palomba and Gerardo Pelosi "Fault Attack to the Elliptic Curve Digital Signature Algorithm with Multiple Bit Faults", in *Proceedings of the 4th International Conference on Security of Information and Networks (SIN 2011)*, November 14–19, 2011, Sydney, Australia. Proc. ACM 2011, pp. 63-72, ISBN: 978-1-4503-1020-8. (DOI: http://dx.doi.org/10.1145/2070425.2070438)

IC.16. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Maria Grazia Fugini, and Gerardo Pelosi "Smart Metering in Power Grids: Application Scenarios and Security", *Proceedings of the IEEE PES Innovative Smart Grid Technology Conference (ISGT2011 Asia)*, November 13–16, 2011, Perth, Australia. IEEE 2011, ISBN: 978-1-4577-0875-6/11.

IC.15. Amir Moradi, Alessandro Barenghi, Timo Kasper and Christof Paar, "On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks - Extracting Keys from Xilinx Virtex-II FPGAs", in *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011)*, ACM 2011, October 17-21, 2011, Chicago, IL, USA. ISBN 978-1-4503-0948-6. (DOI: http://doi.acm.org/10.1145/2046707.2046722)

IC.14. Alessandro Barenghi, Gerardo Pelosi, "Security and Privacy in Smart Grid Infrastructures", in Proceedings of the 22nd Database and Expert Systems Applications (DEXA) International Workshops - 6th Workshop on Flexible Database and Information System Technology (FlexDBIST-2011), Toulouse, France, Aug. 29-Sep. 2, 2011, IEEE Computer Society, ISBN: 978-0-7695-4486-1, ISSN: 1529-4188. (DOI: http://dx.doi.org/10.1109/DEXA.2011.74)

IC.13. Alessandro Barenghi, Guido M. Bertoni, Fabrizio De Santis,Filippo Melzani, "On the efficiency of design time evaluation of the resistance to power attacks", in *Proceedings of 14th Euromicro Conference on Digital System Design (DSD 2011)*, August 31- September 2, 2011, Oulu, Finland, IEEE Computer Society, ISBN-978-0-7695-4494-6. (DOI: http://dx.doi.org/10.1109/DSD.2011.103)

IC.12. Alessandro Barenghi, Cédric Hocquet, David Bol, Franois-Xavier Standaert, Francesco Regazzoni, Israel Koren, "Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-Threshold Devices through an example of a 65nm AES implementation", in *Proceedings of 7th Workshop on RFID Security and Privacy (RFIDSec 2011)*, June 26-28, 2011, Amherst, Massachussets, USA, Lecture Notes in Computer Science, Springer. (ISBN 978-3-642-25285-3).

IC.11. Alessandro Barenghi, Guido M. Bertoni, Andrea Palomba, Ruggero Susella, "A Novel Fault Attack Against ECDSA", **Best Paper Award** in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2011)*, June 5-6, 2011, San Diego, California, USA. (ISBN: 978-1-4577-1059-9). (DOI: http://dx.doi.org/10.1109/HST.2011.5955015).

IC.10. Alessandro Barenghi, Gerardo Pelosi, Yannick Teglia, "Information Leakage Discovery Techniques to Enhance Secure Chip Design", in *Proceedings of the 5th Workshop in Information Security Theory and Practice (WISTP 2011) - Security and Privacy of Mobile Devices in Wireless Communication* (Proc. Springer-LNCS), June 1-3, 2011, (ISBN: 978-3-642-21039-6). (DOI: http://dx.doi.org/10.1007/978-3-642-21040-2_9).

IC.9. Alessandro Barenghi, Luca Breveglieri, Israel Koren, Gerardo Pelosi, Francesco Regazzoni,"Low Cost Software Countermeasures Against Fault Attacks: Implementation and Performances Trade Offs", in *Proceedings of the 5th Workshop on Embedded Systems Security (WESS 2010)*, October 24, 2010, Scottsdale, Arizona, USA, ACM Press and Digital Library 2010 (ISBN: 978-1-4503-0078-0). (DOI: http://dx.doi.org/10.1145/1873548.1873555).

IC.8. Alessandro Barenghi, Guido M. Bertoni, Mauro Pellicioli, Gerardo Pelosi "Fault Attack on AES with Single-Bit Induced Faults", in *Proceedings of the 6th International Conference on Information Assurance and Security (IAS 2010)*, 23–25

August 2010, Atlanta, Georgia, USA, IEEE 2010, pp. 167-172, (ISBN:978-1-4244-7408-0). (DOI: http://dx.doi.org/10.1109/ISIAS.2010.5604061).

IC.7. Alessandro Barenghi, Gerardo Pelosi, Yannick Teglia, "Improving First Order Differential Power Attack Through Filtering", in *Proceedings of The 3rd International Conference on Security of Information and Networks (SIN 2010)*, ACM-SIGSAC, 7–11 September 2010, Taganrog, Rostov region, Russia, ACM 2010, pp. 124-133, (ISBN: 978-1-4503-0234-0). (DOI: http://doi.acm.org/10.1145/1854099.1854126).

IC.6. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Mauro Pellicioli, Gerardo Pelosi "Low Voltage Fault Attacks to AES", in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2010)*, June 13–14, 2010, Anaheim, California, USA, IEEE Computer Society 2010, pp. 7-12, (ISBN: 978-1-4244-7810-1). (DOI: http://dx.doi.org/10.1109/HST.2010.5513121).

IC.5. Giovanni Agosta, Alessandro Barenghi, Fabrizio De Santis, Gerardo Pelosi "Record Setting Software Implementation of DES Using CUDA", *In Proceedings of the International Symposium on Information Security and Privacy (ISISP 2010)*, Las Vegas, Nevada, USA, 12–14 April 2010, IEEE Computer Society 2010, pp. 748-755, (ISBN: 978-0-7695-3984-3). (DOI: http://doi.ieeecomputersociety.org/10.1109/ITNG.2010.43).

IC.4. Giovanni Agosta, Alessandro Barenghi, Fabrizio De Santis, Andrea Di Biagio, Gerardo Pelosi "Fast Disk Encryption Through GPGPU Acceleration", in *Proceedings of the 10-th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2009)*, Hiroshima, Japan, 8–11 December 2009, IEEE Computer Society 2009, pp. 102-109. (ISBN: 978-0-7695-3914-0).
(DOI: http://dx.doi.org/10.1109/PDCAT.2009.72).

IC.3. Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello, Gerardo Pelosi "Low Voltage Fault Attacks on the RSA Cryptosystem", in *Proceedings of the 6-th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2009)*, Lausanne, Switzerland, September 6, 2009, IEEE Computer Society 2009, pp. 23-31. (ISBN: 978-0-7695-3824-2). (DOI: http://dx.doi.org/10.1109/FDTC.2009.30).

IC.2. Andrea di Biagio, Alessandro Barenghi, Giovanni Agosta, Gerardo Pelosi "Design of a Parallel AES for Graphics Hardware using the CUDA framework", in *Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS 2009)*, Rome, Italy, May 29, 2009, IEEE Computer Society 2009, pp. 1-8, (ISBN: 978-1-4244-3751-1). (DOI: http://doi.ieeecomputersociety.org/10.1109/IPDPS.2009.5161242).

IC.1. Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, Gerardo Pelosi "A FPGA Coprocessor for the Cryptographic Tate Pairing over $\mathbb{F}_p$", in *Proceedings of the 5th International Conference on Information Technology: New Generations (ITNG 08)*, Las Vegas, USA, 7–9 April 2008, IEEE Computer Society 2008, pp. 112-119 (ISBN: 978-0-7695-3099-4). (DOI: http://doi.ieeecomputersociety.org/10.1109/ITNG.2008.260).

Technical Reports and Thesis

TR.7. Alessandro Barenghi, Francesco Regazzoni, Gerardo Pelosi "Simulation-Time Security Margin Assessment against Power-Based Side Channel Attacks". International Association for Cryptologic Research (IACR) - Cryptology ePrint Archive, Report 2014/307, 2014. http://eprint.iacr.org/2014/307

TR.6. "The PAPAGENO parallel parser generator", HiPEAC Info Newsletter 3, January 2013, published by the HiPEAC Network of Excellence, http://www.hipeac.net/publications.

TR.5. Amir Moradi, Alessandro Barenghi, Timo Kasper, Christof Paar, "On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks - Extracting Keys from Xilinx Virtex-II FPGAs", International Association for Cryptologic Research (IACR) - Cryptology ePrint Archive, Report 2011/390, (July 2011). Available online at http://eprint.iacr.org/2011/390.pdf

TR.4. "Parallel Parsing on Multicore and Handheld devices Hipeac", HiPEAC Info Newsletter 26, April 2011, published by the HiPEAC Network of Excellence, http://www.hipeac.net/publications.

TR.3. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Mauro Pellicioli, Gerardo Pelosi, "Low Voltage Fault Attacks to AES and RSA on General Purpose Processors", International Association for Cryptologic Research (IACR) - Cryptology ePrint Archive, Report 2010/130, (April 2010). Available online at http://eprint.iacr.org/2010/130.pdf

TR.2. Alessandro Barenghi, "Transfer from Multiple Transformed Source Tasks in Batch Reinforcement Learning". Technical Report n. 2009.07, February 2009, Politecnico di Milano

TR.1. Alessandro Barenghi, "Innovative and complex cryptographic functions: How to efficiently compute a Tate pairing in hardware". MSc. Thesis, Politecnico di Milano, April 2007

PATENT

PT.1. Giovanni Agosta, Alessandro Barenghi, Guido Marco Bertoni, and Gerardo Pelosi. “Method and system for protecting electronic devices, related computer program product”. European Patent Application with search Report: ITTO20111 229 (A1), June 2013. Proprietor(s): Politecnico di Milano, ST Microelectronics Srl (IT). Application and Priority number: IT2011TO01229 20111229. Priority date: 2011-12-29.

Milan, March 12, 2019

Signature

Alessandro Barenghi

I agree to the treatment of personal data in accordance with privacy regulations