Gerardo Pelosi: curriculum vitæ et studiorum

Cittadidanza [redacted]
Indirizzo [redacted]

Carriera

04 Maggio 2018 –

Professore Associato, presso il Politecnico di Milano – Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Milano.
Interessi di ricerca: Sicurezza informatica, crittografia applicata, hardware security.
Area concorsuale: 09 – Ingegneria industriale e dell'informazione.
Macro settore concorsuale: 09/H – Ingegneria Informatica.
Settore concorsuale: 09/H1 – Sistemi di elaborazione delle informazioni.
Settore scientifico disciplinare (SSD): ING-INF/05 - Sistemi di elaborazione delle informazioni.

04 Maggio 2015 – 03 Maggio 2018 (36 mesi)

Ricercatore univeritario a tempo determinato *Senior* (RTD-B), di cui all'art. 24, comma 3 lettera B, della Legge n. 240/2010 (*tenured position*, a tempo pieno), presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano.
Area concorsuale: 09 – Ingegneria industriale e dell'informazione.
Macro settore concorsuale: 09/H – Ingegneria Informatica.
Settore concorsuale: 09/H1 – Sistemi di elaborazione delle informazioni.
Settore scientifico disciplinare (SSD): ING-INF/05 - Sistemi di elaborazione delle informazioni.

01 Febbraio 2013 – 03 Maggio 2015 (27 mesi)

Ricercatore univeritario a tempo determinato *Junior* (RTD-A), di cui all'art. 24, comma 3 lettera A, della Legge n. 240/2010 (*non-tenured position*, a tempo pieno), presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano.
Area concorsuale: 09 – Ingegneria industriale e dell'informazione.
Macro settore concorsuale: 09/H – Ingegneria Informatica.
Settore concorsuale: 09/H1 – Sistemi di elaborazione delle informazioni.
Settore scientifico disciplinare (SSD): ING-INF/05 - Sistemi di elaborazione delle informazioni.

16 Giugno 2010 – 31 Gennaio 2013 (31 mesi e 15 giorni)

Ricercatore univeritario a tempo determinato (RTD), di cui all'art. 1, comma 14, della Legge n. 230/2005 (*non-tenured position*, a tempo pieno), presso il Dipartimento di Elettronica e Informazione (DEI) del Politecnico di Milano.
Settore scientifico disciplinare: ING-INF/05 - Sistemi di elaborazione delle informazioni.
In ottemperanza alla determinazione dei settori concorsuali (SC), raggruppati in macrosettori concorsuali (MC), di cui all'art. 15, Legge n. 240/2010, il decreto ministeriale del 29 Luglio 2011 ha definito le seguenti denominazioni per la classe di concorso in oggetto.
Area concorsuale: 09 – Ingegneria industriale e dell'informazione.
MC: 09/H - Ingegneria informatica. SC: 09/H1 – Sistemi di elaborazione delle informazioni.

01 Febbraio 2010 – 16 Giugno 2010 (4 mesi e 16 giorni)

Vincitore della selezione pubblica per il conferimento di un "Assegno di Ricerca", di cui all'art. 51, comma 6, della Legge del 27/12/1997, n. 449 e del decreto ministeriale del 11/2/1998, il Dipartimento di Ingegneria dell'Informazione e Metodi Matematici (DIMM) dell'Università degli Studi di Bergamo.
Titolo: Architetture per la protezione della sicurezza e dell'integrità nelle reti radio.

01 Febbraio 2009 – 31 Gennaio 2010 (12 mesi)

Vincitore della selezione pubblica per titoli e colloquio per il conferimento di un "Assegno di Ricerca" di cui all'art. 51, comma 6, della Legge del 27/12/1997, n. 449 e del decreto ministeriale del 11/2/1998, il Dipartimento di Ingegneria dell'Informazione e Metodi Matematici (DIMM) dell'Università degli Studi di Bergamo.
Titolo: Architetture per il controllo dell'accesso e per la protezione della sicurezza in reti *wireless*.

01 Agosto 2008 – 31 Gennaio 2009 (6 mesi)

Vincitore della selezione pubblica per titoli e colloquio per il conferimento di un "Assegno di Ricerca", di cui all'art. 51, comma 6, della Legge del 27/12/1997, n. 449 e del decreto ministeriale del 11/2/1998, presso il Dipartimento di Ingegneria dell'Informazione e Metodi Matematici (DIMM) dell'Università degli Studi di Bergamo.

Titolo: Modelli per la gestione di dati cifrati nell'ambito di basi di dati relazionali.

16 Giugno 2008 – 31 Luglio 2008 (2 mesi)

Incarico mediante contratto d'opera dal titolo: Progettazione di tecniche per la protezione di politiche in contesti di data outsourcing. Contratto stipulato nell'ambito del Progetto di Ricerca d'interesse nazionale (PRIN) anno 2006, presso il Dipartimento di Ingegneria dell'Informazione e Metodi Matematici (DIMM) dell'Università degli Studi di Bergamo (Determinazione del Direttore n. 130 del 18/06/2008).

16 Maggio 2007 – 15 Maggio 2008 (12 mesi)

Vincitore della selezione pubblica per titoli e colloquio per il conferimento di un "Assegno di Ricerca", id. 413174, di cui all'art. 51, comma 6, della Legge 27/12/1997, N. 449 e del decreto ministeriale del 11/2/1998, presso l'Università degli Studi di Bergamo, nell'ambito del Progetto Quadro FSE 2006, Id. 410978. Titolo: Principi, Metodologie e Tecniche per la modellistica e l'analisi di sistemi software critici e intelligenti.

01 March 2003 – 29 February 2004 (12 mesi)

Research Engineer presso i laboratori di ricerca e sviluppo denominati *Advanced System Technology (AST) Labs.* di STMicroelectronics, Agrate Brianza (MB), Italia.

Abilitazioni

30 Luglio 2020

Abilitazione scientifica nazionale alle funzioni di professore universitario di **prima fascia** in *Sistemi di Elaborazione delle Informazioni*. Conseguita ai sensi dell'art.16, com.1, Legge n.240/10.
Area: 09 - Ingegneria industriale e dell'informazione.
Macrosettore: 09/H - Ingegneria informatica.
Settore concorsuale (SC): 09/H1 – Sistemi di elaborazione delle informazioni.
Settore scientifico disciplinare (SSD): ING-INF/05 - Sistemi di elaborazione delle informazioni.

4 Aprile 2017

Abilitazione scientifica nazionale alle funzioni di professore universitario di **seconda fascia** in *Sistemi di Elaborazione delle Informazioni*. Conseguita ai sensi dell'art.16, com.1, Legge n.240/10.
Area: 09 - Ingegneria industriale e dell'informazione.
Macrosettore: 09/H - Ingegneria informatica.
Settore concorsuale (SC): 09/H1 – Sistemi di elaborazione delle informazioni.
Settore scientifico disciplinare (SSD): ING-INF/05 - Sistemi di elaborazione delle informazioni.

29 Gennaio 2014

Abilitazione scientifica nazionale alle funzioni di professore universitario di **seconda fascia** in *Informatica*. Conseguita ai sensi dell'art. 16, comma 1, Legge n. 240/10.
Area: 01 - Scienze matematiche e informatiche.
Macrosettore: 01/B - Informatica.
Settore concorsuale (SC): 01/B1 - Informatica.
Settore scientifico disciplinare (SSD): INF/01 - Informatica.

20 Dicembre 2003

Abilitazione nazionale per l'esercizio della professione di "Ingegnere delle Telecomunicazioni". Conseguita presso il Politecnico di Milano (1ma sessione).

Formazione

24 Maggio 2007

Dottorato in "Ingegneria dell'informazione" (Ph.D. in Information Technology), Politecnico di Milano.
Titolo Tesi: *Algorithms, Architectures and Protocols for Public-Key Cryptographic Systems with Innovative and Complex Functionalities: The Case of IBE and Compact Discrete Logarithm Systems.*

26 Gennaio 2006

Attività di ricerca minore dal titolo: *Gas Sensor Array Response Analysis by Means of Computational Intelligence Techniques*.

1 Marzo 2004 – 24 Maggio 2007

Studi di dottorato, presso il Politecnico di Milano - Piazza Leonardo da Vinci, 32 - Milano. Diparimento di Elettronica e Informazione – DEI.

20 Febbraio 2003

Laurea (Vecchio Ordinamento: 5 anni, ante D.M. 509/99 - D.M. 270/04) di Dottore in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano.

March 2002 – February 2003

Internship presso i laboratori R&D, Advanced System Technology (AST) – STMicroelectronics, Agrate Brianza (MB), Italy.

Finanziamenti

RICONOSCIMENTI FINANZIARI MINISTERIALI

5 Dicembre 2017

Beneficiario del "Finanziamento Annuale Individuale delle Attività Base di Ricerca" (Euro 3000/00), di cui all'art. 1, commi 295 e seguenti della Legge n. 232 dell'11 Dicembre 2016 (GU n. 297 del 21-12-2016 – Suppl. Ordinario n. 57). Finanziamento ottenuto sulla base della classifica stilata dall'Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca (ANVUR), considerando il valore *dell'indicatore della produzione scientifica* 2012–2016, in ottemperanza a quanto stabilito dalla suddetta Legge, favorendo del "Fondo per il finanziamento delle attivitÃ base di ricerca" (FFABR 2017) iscritto nello stato di previsione del MIUR 2017.

Premi e riconoscimenti

AW.9. Best Paper Award for the paper entitled "A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems"[IC.70], received at the *17th International Joint Conference on e-Business and Telecommunications (ICETE)*, held remotely (due to covid-19 pandemic) on July 8 - 10, 2020.

AW.8. 2018 Hardware and Embedded Security Top Picks paper Award.

The paper "A Code Morphing Methodology to Automate Power Analysis Countermeasures," [IC.29] appeared in *Proc. of the 49th Design Automation Conference* (DAC 2012), ACM, 2012. has been awarded for the most significant papers based on novelty and long-term impact from IEEE/ACM conferences and journals in the broad area of Hardware and Embedded Security during the six-year period: 2012 – 2017.

Presentations to the *2018 Top Picks in Hardware and Embedded Security Workshop*, co-located with IEEE/ACM ICCAD 2018 Conference, San Diego, CA, USA on November 8th, 2018.
https://wp.nyu.edu/toppicksinhardwaresecurity/top-pick-candidates/
were selected from papers appeared in leading hardware and embedded security conferences and journals including but not limited to DAC, DATE, ICCAD, HOST, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, Usenix Security, ASIA CCS, NDSS, ISCA, MICRO, ASPLOS, HPCA, ACSAC and ACM CCS during the six-year period: 2012 – 2017.

A peer-reviewed retrospective on the developments and impact of the work entitled "Compiler-based Techniques to Secure Cryptographic Embedded Software against Side Channel Attacks," will appear in the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD). IEEE 2019 [JR.23].

AW.7. HiPEAC Paper Award - 2018
Awarded by the Steering Committee of the European Network of Excellence on High Performance and Embedded Architecture and Compilation, for the paper entitled: "Side-channel security of superscalar CPUs: Evaluating the Impact of Microarchitectural Features,"[IC.60] in *Proc. of the 55th Design Automation Conference* (DAC 2018), ACM, 2018, 6 pages.
(ISBN: 978-1-4503-5700-5/18/06).

AW.6. HiPEAC Paper Award - 2015
Awarded by the Steering Committee of the European Network of Excellence on High Performance and Embedded Architecture and Compilation, for the paper entitled: "A Multiple Equivalent

Execution Trace Approach to Secure Cryptographic Embedded Software,"[IC.47] in *Proc. of the 52nd Design Automation Conference* (DAC 2015), ACM, 2015, pp. 33:1–33:6.
(ISBN: 978-1-4503-3520-1/15/06).

AW.5. SIN 2014 Best Paper Award: *Best Paper Overall*
"Differential Fault Analysis for Block Ciphers: an Automated Conservative Analysis"[IC.42], in *Proc. of the Int.l Conference on Security of Information and Networks* (SIN'14). ACM 2014, pp. 171:1-171:8. (ISBN: 978-1-4503-3033-6/14/09)

AW.4. SIN 2014 Best Paper Award: *Best Cryptographic Techniques Paper*
"Differential Fault Analysis for Block Ciphers: an Automated Conservative Analysis"[IC.42], in *Proc. of the Int.l Conference on Security of Information and Networks* (SIN'14). ACM 2014, pp. 171:1-171:8. (ISBN: 978-1-4503-3033-6/14/09)

AW.3. HiPEAC Paper Award - 2014
Awarded by the Steering Committee of the European Network of Excellence on High Performance and Embedded Architecture and Compilation, for the paper entitled: "A Multiple Equivalent Execution Trace Approach to Secure Cryptographic Embedded Software,"[IC.39] in *Proc. of the 51st Design Automation Conference* (DAC 2014), ACM, 2014, pp. 210:1–210:6.
(ISBN: 978-1-4503-2730-5).

AW.2. HiPEAC Paper Award - 2013
Awarded by the Steering Committee of the European Network of Excellence on High Performance and Embedded Architecture and Compilation, for the paper entitled: "Compiler-based Side Channel Vulnerability Analysis and Optimized Countermeasures Application,"[IC.34] in *Proc. of the 50th Design Automation Conference* (DAC 2013), ACM, 2013, pp. 81:1–81:6.
(ISBN: 978-1-4503-2071-9)

AW.1. HiPEAC Paper Award - 2012
Awarded by the Steering Committee of the European Network of Excellence on High Performance and Embedded Architecture and Compilation, for the paper entitled: "A Code Morphing Methodology to Automate Power Analysis Countermeasures,"[IC.29] in *Proc. of the 49th Design Automation Conference* (DAC 2012), ACM, 2012, pp. 77–82.
(ISBN: 978-1-4503-1199-1)

Incarichi per attività didattica presso Università

ATTIVITÀ DIDATTICA IN TITOLARITÀ

a.a. 2022-2023 (Titolarità: 27 *crediti formativi)*

Architetture dei Calcolatori e Sistemi Operativi – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Informatica (per Aerospaziali) – 6 Crediti formativi, 2°semestre.
Corso di Laurea Triennale in Ingegneria Aerospaziale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Big data management and Cybersecurity - 5 Crediti formativi, 1°semestre.
International Master in Fintech, MIP Politecnico di Milano Graduate School of Business.

Data Protection Officer (DPO) – 1 Credito formativo (Introduzione alla sicurezza informatica, elementi di sicurezza delle reti e protezione dei dati), Luglio 2022.
Master universitario di II livello, istituito per l'anno 2022/2023 presso il Dipartimento di Architettura e Studi Urbani del Politecnico di Milano.

a.a. 2021-2022 (Titolarità: 32 *crediti formativi)*

Introduction to Quantum Computing course - Ph.D. Level - 5 ECTS (European Credit Transfer System), Ph.D. Programme in Information Technology, Politecnico di Milano.

Architetture dei Calcolatori e Sistemi Operativi – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Informatica (per Aerospaziali) – 6 Crediti formativi, 2°semestre.
Corso di Laurea Triennale in Ingegneria Aerospaziale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Big data management and Cybersecurity - 5.0 Crediti formativi, 1°semestre.
International Master in Fintech, MIP Politecnico di Milano Graduate School of Business.

Data Protection Officer (DPO) – 1 Credito formativo (Introduzione alla sicurezza informatica, elementi di sicurezza delle reti e protezione dei dati), Luglio 2020.
Master universitario di II livello, istituito per l'anno 2021/2022 presso il Dipartimento di Architettura e Studi Urbani del Politecnico di Milano.

a.a. 2020-2021 (Titolarità: 34,5 *crediti formativi)*

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Architetture dei Calcolatori e Sistemi Operativi – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Informatica – 6 Crediti formativi, 2°semestre.
Corso di Laurea Triennale in Ingegneria Aerospaziale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Big data management and Cybersecurity – modulo di *Cybersecurity* – 2.5 Crediti formativi, 1°semestre.
International Master in Fintech, MIP Politecnico di Milano Graduate School of Business.

Data Protection Officer (DPO) – 1 Credito formativo (Introduzione alla sicurezza informatica, elementi di sicurezza delle reti e protezione dei dati), Luglio 2020.
Master universitario di II livello, istituito per l'anno 2020/2021 presso il Dipartimento di Architettura e Studi Urbani del Politecnico di Milano.

a.a. 2019-2020 (Titolarità: 24,5 crediti formativi)

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Big data management and Cybersecurity – modulo di *Cybersecurity* – 2.5 Crediti formativi, 1°semestre.
International Master in Fintech, MIP Politecnico di Milano Graduate School of Business.

Data Protection Officer (DPO) – 1 Credito formativo (Introduzione alla sicurezza informatica, elementi di sicurezza delle reti e protezione dei dati), Luglio 2020.
Master universitario di II livello, istituito per l'anno 2018/2019 presso il Dipartimento di Architettura e Studi Urbani del Politecnico di Milano.

Selected Topic in Cryptography - Ph.D. Level - 5 ECTS (European Credit Transfer System), Ph.D. Programme in Information Technology, Politecnico di Milano.

Co-lecturer for the **Introduction to Quantum Mechanics for ICT** course - Ph.D. Level - 1 ECTS (European Credit Transfer System) on *Quantum computing*, Ph.D. Programme in Information Technology, Politecnico di Milano.

a.a. 2018-2019 (Titolarità: 16 crediti formativi)

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Data Protection Officer (DPO) – 1 Credito formativo (Introduzione alla sicurezza informatica, elementi di sicurezza delle reti e protezione dei dati), Marzo 2019.
Master universitario di II livello, istituito per l'anno 2018/2019 presso il Dipartimento di Architettura e Studi Urbani del Politecnico di Milano.

a.a. 2017-2018 (Titolarità: 15 crediti formativi)

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2016-2017 (Titolarità: 15 crediti formativi)

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2015-2016 (Titolarità: 15 crediti formativi)

Informatica A – 10 Crediti formativi, 1°semestre.
Corso di Laurea Triennale in Ingegneria Gestionale, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2014-2015 (Titolarità: 5 crediti formativi)

Cryptography and Architectures for Computer Security – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2013-2014 (Titolarità: 5 crediti formativi)

Cryptography and Security of Digital Devices – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2012-2013 (Titolarità: 5 crediti formativi)

Cryptography and Security of Digital Devices – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2011-2012 (Titolarità: 5 crediti formativi)

Cryptography and Security of Digital Devices – 5 Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

a.a. 2010-2011 (Titolarità: 2,5 crediti formativi)

Algoritmi e Architetture per Sistemi Crittografici – $2,5$ Crediti formativi, 2°semestre.
Corso di Laurea Magistrale in Ingegneria Informatica, Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.

ATTIVITÀ DIDATTICA INTEGRATIVA

a.a. 2021-2022 (Esercitazioni: 10 ore. Tutoring: 6 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2020-2021 (Esercitazioni: 10 ore. Tutoring: 6 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2019-2020 (Esercitazioni: 74 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione Python) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Gestionale. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Patrizia Scandurra.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2018-2019 (Esercitazioni: 74 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione Python) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Gestionale. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Patrizia Scandurra.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2017-2018 (Esercitazioni: 74 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione Python) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Gestionale. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Patrizia Scandurra.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2016-2017 (Esercitazioni: 58 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Informatica (modulo di programmazione C/C++) – 16 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Gestionale. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Patrizia Scandurra.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2015-2016 (Esercitazioni: 58 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Informatica (modulo di programmazione C/C++) – 48 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2014-2015 (Esercitazioni: 138 ore. Tutoring: 18 ore)

Advanced Computer Architectures – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale in Ingegneria Informatica. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano. Titolare: Prof. Cristina Silvano.

Architettura dei Calcolatori e Sistemi Operativi – 40 ore di didattica frontale come *Esercitatore*. Laurea di 1mo Livello. Scuola di Ingegneria Industriale e dell' Informazione, Politecnico di Milano.
Titolare: Prof. Anna Antola.

Fondamenti di Informatica – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 48 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2013-2014 (Esercitazioni: 122 ore. Tutoring: 18 ore)

Architetture Avanzate dei Calcolatori – 10 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Cristina Silvano.

Architettura dei Calcolatori e Sistemi Operativi – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Anna Antola.

Fondamenti di Informatica – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 12 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2012-2013 (Esercitazioni: 80 ore. Tutoring: 6 ore)

Architettura dei Calcolatori e Sistemi Operativi – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Anna Antola.

Architettura dei Calcolatori e Sistemi Operativi – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Luca O. Breveglieri.

Fondamenti di Informatica – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale in qualità di *Tutor*. Corso di Laurea Specialistica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2011-2012 (Esercitazioni: 84 ore. Tutoring: 14 ore)

Architettura dei Calcolatori e Sistemi Operativi – 12 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Luca O. Breveglieri.

Fondamenti di Informatica – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea 1mo Livello. Scuola di Ingegneria Industriale e dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 8 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 6 ore di didattica frontale come *Tutor*. Corso di Laurea Specialistica, Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2010-2011 (Esercitazioni: 92 ore. Tutoring: 8 ore)

Algoritmi e Principi dell'Informatica (Mod 2 , Informatica 3) – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Giovanni Agosta.

Fondamenti di Informatica – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 8 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

a.a. 2009-2010 (Esercitazioni: 94 ore. Tutoring: 16 ore)

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica III – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Prof. Giovanni Agosta.

Fondamenti di Informatica – 34 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Informatica (modulo di programmazione C/C++) – 8 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Giuseppe Psaila.

Sicurezza dei Sistemi Informatici – 8 ore di didattica frontale come *Tutor*. Corso di Laurea Magistrale. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Stefano Paraboschi.

a.a. 2008-2009 (Esercitazioni: 94 ore. Tutoring: 8 ore)

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica III – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Giovanni Agosta.

Fondamenti di Informatica – 34 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano.
Titolare: Prof. Daniele M. Braga.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Vittorio Moriggia.

Informatica (modulo di programmazione C/C++) – 8 ore di didattica frontale come *Tutor*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Vittorio Moriggia.

a.a. 2007-2008 (Esercitazioni: 140 ore)

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica III – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Giovanni Agosta.

Informatica II – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Luca O. Breveglieri.

Informatica I – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Daniele M. Braga.

Applicazioni Internet A – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Alessandro Campi.

Informatica (modulo di programmazione C/C++) – 32 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello in Ingegneria Informatica. Facoltà di Ingegneria, Università degli Studi di Bergamo. Titolare: Prof. Vittorio Moriggia.

a.a. 2006-2007 (Esercitazioni: 98 ore)

Fondamenti di Crittografia – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano (Campus Como). Titolare: Prof. Alessandra Cherubini, Prof. Luca O. Breveglieri.

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica II – 40 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Luca O. Breveglieri.

Informatica I – 30 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Daniele M. Braga.

a.a. 2005-2006 (Esercitazioni: 68 ore)

Fondamenti di Crittografia – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano (Campus Como). Titolare: Prof. Alessandra Cherubini, Prof. Luca Breveglieri.

Algoritmi e Architetture per Sistemi Crittografici – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Guido M. Bertoni.

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica I – 30 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Daniele M. Braga.

a.a. 2004-2005 (Esercitazioni: 58 ore, Responsabile Laboratorio: 36 ore)

Fondamenti di Crittografia – 20 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano (Campus Como). Titolare: Prof. Alessandra Cherubini, Prof. Luca O. Breveglieri.

Algebra & Logica II – 8 ore di didattica frontale come *Esercitatore*. Corso di Laurea Magistrale. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Alessandra Cherubini.

Informatica I – 30 ore di didattica frontale come *Esercitatore*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Luca O. Breveglieri.

Informatica II – 36 ore di didattica frontale come *Responsabile di Laboratorio*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Luigi Lavazza.

a.a. 2003-2004 (Responsabile Laboratorio: 48 ore)

Informatica II – 48 ore di didattica frontale come *Responsabile di Laboratorio*. Corso di Laurea di 1mo Livello. Facoltà di Ingegneria dell'Informazione, Politecnico di Milano. Titolare: Prof. Luigi Lavazza.

Attività di servizio agli studenti

Attività di Supervisione di Tesi di Dottorato

2021 – ongoing

Francesco Antognazza, Cycle XXXVI, (Major Research) "Hardware Implementation of Post-Quantum Cryptographic Algorithms for the IOT".
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Advisor: Prof. Gerardo Pelosi.

2021 – ongoing

Raul Zuleta Ticchione, Cycle XXXVI, Executive Ph.D., (Major Research) " Post-quantum ready mobile network communications: feasibility analysis and realization engineering.".
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Advisor: Prof. Gerardo Pelosi.

2019 – ongoing

Simone Perriello, Cycle XXXV, (Major Research) "Quantum Computing Algorithms: functional validation and performance assessment."
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Advisor: Prof. Gerardo Pelosi.

2017-2021

Nicholas Mainardi, Cycle XXXII, (Major Research) "From theoretical to real world cryptography: engineering homomorphic cryptographic primitives and language based security".
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Relatore: Prof. Gerardo Pelosi.

2012-2014

Michele Scandale, Cycle XXVIII (Minor Research), "Compiler techniques for the automated application of side-channel countermeasures on embedded devices".
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Relatore: Dr. Gerardo Pelosi.

2011-2014

Alessio Antonini, Cycle XXVI, (Major Research) "Vulnerability Detection and Countermeasures in Building Automation Networks and Cyber-Physical Systems".
PhD program in Information Technology (IT). Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Milano, Italy.
Co-Relatores: Prof. Luca O. Breveglieri, Dr. Gerardo Pelosi.

Attività di Supervisione di Tesi di Laurea Magistrale e Laurea Specialistica

a.y. 2021–2022

Luca dell'Oglio, April 2022, "Design, Realization and Performance Evaluation of a Low Latency High Throughput Authenticated Encryption Module". Laurea Magistrale in Ingegneria Informatica (Master of Science in Engineering of Computing Systems, MSc–IT), Politecnico di Milano.
Advisor: Prof. Gerardo Pelosi. Co-advisors: Prof. Alessandro Barenghi, Prof. Luca Breveglieri.

Emanuele Pisano, April 2022, "Application of LEDAcrypt cryptosystem in Oversonic Robotics project". Laurea Magistrale in Ingegneria Informatica (Master of Science in Engineering of Computing Systems, MSc–IT), Politecnico di Milano.
Advisor: Prof. Gerardo Pelosi. Co-Advisor: Prof. Alessandro Barenghi.

Costantino Vincifori, April 2022, "Performing SCA Against Block Ciphers Using Closest and Furthest Leakage Models". Laurea Magistrale in Ingegneria Informatica (Master of Science in Engineering of Computing Systems, MSc–IT), Politecnico di Milano.
Advisor: Prof. Gerardo Pelosi. Co-advisor: Prof. Alessandro Barenghi.

a.y. 2020–2021

Simone Andreotti, December 2021, "Learning with errors vs learning with rounding: a performance evaluation for homomorphic encryption". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatore: Prof. Alessandro Barenghi.

Federico Ferri, December 2021, "Design and implementation of a cryptographic ASIC circuit for elliptic curve scalar-point multiplications over binary fields". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatori: Prof. Alessandro Barenghi, Dr. Sivia Mella.

Marco Paci, June 2021, "Scalable in-Enclave ORAM Design for Multi-User Privacy-Preserving Substring Search Queries". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-Relatore: Prof. Alessandro Barenghi.

a.y. 2019–2020

Francesco Antognazza, July 2020, "Countering side channel attacks in an in-order RISC-V processor with a code morphing based execution mode". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatore: Prof. Alessandro Barenghi.

Andrea Pace, July 2020, "Improving Feature Extraction and Classification in Neural Network based Side Channel Attacks against Asymmetric Cryptosystems". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatori: Prof. Alessandro Barenghi, Dr. Sivia Mella.

Simone Bergonzi, June 2020, "Side channel attacks to LEDAcrypt: synthetic analysis and practical countermeasure validation". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-Relatore: Prof. Alessandro Barenghi.

a.a. 2018–2019

Davide Sampietro, July 2019, "ObSQRE: efficient full-text index for oblivious substring search queries with Intel SGX". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatore: Eng. Nicholas Mainardi.

a.a. 2017–2018

Simone Perriello, April 2019, "Design and implementation of a quantum circuit to solve the Information Set Decoding problem". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Marco Sartini, April 2019, "Feasibility Analysis of Horizontal Side channel attacks against Elliptic curve cryptosystems". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

a.a. 2016–2017

Nicola Galloro, December 2017, "Combining traditional and side channel cryptanalyses: a case study on SIMON, PRESENT and SIMEK". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Guglielmo Pietro Filippo Molinari, December 2017, "Analysis and Benchmarking of Privacy-preserving Methods to Access Outsourced Data". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano. Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Niccolò Izzo, December 2017, "Reliably Achieving and Efficiently Preventing Rowhammer Attacks". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Alessandro Barenghi. Co-relatore: Dr. Gerardo Pelosi.

a.a. 2015–2016

Davide Botti, April 2017, "Architectural characterization of passive side channel leakage: the case of ARM Cortex-A7.". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Alessandro Barenghi. Co-relatore: Dr. Gerardo Pelosi.

Stefano Kevin Sanfilippo, December 2016, "A compiler-based technique for automated analysis and protection against side-channel attacks.". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano. Relatore: Dr. Alessandro Barenghi. Co-relatore: Dr. Gerardo Pelosi.

a.a. 2014–2015

Nicholas Mainardi, April 2016, "A predicated grammar for X509 certificates and its parser: systematically checking for syntactic soundness of digital certificates". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano. Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Emanuele De Donatis, April 2016, "Differential power analysis on embedded multicore platforms: experimenting with contactless power measurements". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano. Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Davide Wilfredo Attila Macocchi, December 2015, "Progettazione e Validazione di Circuiti Aritmetico-logici Resistenti a Crittanalisi di Tipo *Side-channel*". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano. Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

a.a. 2013–2014

Dario Navoni, "Security in Building Automation Systems: a Study on Multi-party Key-agreement Protocols". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Francesco Fiduccia, "Fine-tuning of a Toolchain for the Automated Application of Side-channel Software Countermeasure". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano, Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Giovanni Agosta, Dr. Alessandro Barenghi.

a.a. 2012–2013

Michele Beretta, Alessandro Di Federico, "Snake: a privacy-aware online social network providing anonymity of outsourced data at rest". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

Massimo Maggi, "Automated Side-channel Vulnerability Detection and Countermeasure Application via Compiler-based Techniques". Laurea Magistrale in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Dr. Alessandro Barenghi.

a.a. 2010–2011

Fabio Pozzi, "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". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano, Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Ing. Alessandro Barenghi.

a.a. 2009–2010

Roberto Dossi, Andrea Vavassori, "Accesso concorrente a strutture di indicizzazione per dati cifrati". Laurea Specialistica in Ingegneria Informatica, Università degli Studi di Bergamo.
Relatore: Prof. Stefano Paraboschi. Co-relatore: Dr. Gerardo Pelosi.

a.a. 2009–2010

Tommaso Bolis, "Progettazione di strutture di indicizzazione per la ricerca su dati cifrati, in uno scenario di data-outsourcing, in regime di concorrenza". Laurea Specialistica in Ingegneria Informatica, Università degli Studi di Bergamo.
Relatore: Prof. Stefano Paraboschi. Co-relatore: Dr. Gerardo Pelosi.

Antonio Parata, "Individuazione automatica di vulnerabilità in applicazioni PHP mediante Static Taint Analysis". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Giovanni Agosta. Co-relatore: Dr. Gerardo Pelosi, Ing. Alessandro Barenghi.

a.a. 2006–2007

Alessandro Barenghi, "Innovative and complex cryptographic functions: how to efficiently compute a Tate pairing in hardware (algorithm, design methodology, architecture and evaluation)". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

a.a. 2005–2006

Claudio Filipponi, "Crittografia basata sull'Identità: Studio, Progetto e Valutazione di Architetture HW per il Calcolo della Tate Pairing in Caratteristica Tre". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

Paolo Curti, "Dispositivi Hardware per Crittografia: una Rassegna su Componentistica Commerciale, Funzioni e Struttura". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

a.a. 2004–2005

Luigi Sportiello, "Sistemi Crittografici basati su Identità (IBE): Studio, Progetto Software e Valutazione delle Prestazioni". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

a.a. 2003–2004

Simone De Capitani, "Studio, Analisi e Sviluppo Software di Metodi per la Determinazione dell'ordine di curve ellittiche su campi di Galois GF(q)". Università degli Studi dell'Insubria Facoltà di Scienze Matematiche, Fisiche e Naturali, Como.
Relatore: Prof. Franco Cazzaniga. Co-relatore: Ing. Gerardo Pelosi, Dott. Pasqualina Fragneto.

Paolo Licini, "Studio e Valutazione di Primitive Crittografiche Identity-Based Basate su Squared Tate Pairing per curve iperellittiche". Laurea Specialistica in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca Breveglieri.
Co-relatore: Ing. Gerardo Pelosi, Dott. Pasqualina Fragneto, Ing. Guido M. Bertoni.

ATTIVITÀ DI SUPERVISIONE DI TESI DI LAUREA DI PRIMO LIVELLO E DI LAUREA TRIENNALE

a.a. 2009–2010

Santi Raffa, "yACCESS: a Cryptographic Filesystem Layer in Userspace". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Ing. Alessandro Barenghi.

Yilai Chen, Antonio Dionisio, "Studio di Fattibilità per la progettazione di un coprocessore per il calcolo di funzioni di pairing". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Ing. Alessandro Barenghi.

Maurizio Dal Corno, "Return into Itself: costruzione di un insieme di istruzioni Turing-completo, per iniezione di codice in vulnerabilità di tipo buffer-overflow, mediante letture disallineate nel segmento di codice dell'eseguibile". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Ing. Alessandro Barenghi.

Andrea Cazzola, Giovanni Francesco Del Nero, "Implementazione di un attacco pratico al crittosistema C2 per la protezione di diritti digitali CPRM/CPPM". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Dr. Gerardo Pelosi. Co-relatore: Ing. Alessandro Barenghi.

Steven Capelli, "Applicazione web sicura per condivisione dati in ambito di Social Networking". Laurea in Ingegneria Informatica. Università degli Studi di Bergamo.
Relatore: Prof. Stefano Paraboschi. Co-relatore: Dr. Gerardo Pelosi.

Daniele Rogora, "Fattorizzazione di interi su cheda grafica: ottimizzazione e valutazione del General Number Field Sieve". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Giovanni Agosta. Co-relatore: Dr. Gerardo Pelosi, Ing. Alessandro Barenghi.

Marco Guarnieri, Eros Magri, "Sviluppo di un' Applicazione Web-Based Sicura per il Data-outsourcing". Laurea in Ingegneria Informatica. Università degli Studi di Bergamo.
Relatore: Prof. Stefano Paraboschi. Co-relatore: Dr. Gerardo Pelosi.

Davide Mora, "Il problema dell'offuscamento della posizione dell'utente nei Location-Based Services". Laurea in Ingegneria Informatica. Università degli Studi di Bergamo.
Relatore: Prof. Giuseppe Psaila. Co-relatore: Dr. Gerardo Pelosi.

a.a. 2005–2006

Matteo Ghilotti, "Ottimizzazione in HW del Crittosistema RSA". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca O. Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

Riccardo Galbiati, "Progetto e Implementazione di un Coprocessore per Crittografia con RSA". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca O. Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

Jacopo Doria, "Progetto e Valutazione di un Coprocessore per Firma Digitale con RSA". Laurea in Ingegneria Informatica, Politecnico di Milano.
Relatore: Prof. Luca O. Breveglieri. Co-relatore: Ing. Gerardo Pelosi.

Attività Professionali

ATTIVITÀ IN PROGETTI DI RICERCA INTERNAZIONALI IN QUALITÀ DI *co-principal investigator*

- "**WorkingAge - Smart Working environments for all Ages**"
  From 1st Feb 2019 to 31st January 2022 (extended until 31st July 2022)
  GRANT AGREEMENT ID: 826232.
  FUNDED UNDER: H2020-EU.3.1.4.1, H2020-EU.3.1.4.2. (OVERALL BUDGET: EUR 3 997 166,25)
  PROGRAMME(S): H2020-EU.3.1.4.1. - ACTIVE AGEING, INDEPENDENT AND ASSISTED LIVING & H2020-EU.3.1.4.2. - INDIVIDUAL AWARENESS AND EMPOWERMENT FOR SELF-MANAGEMENT OF HEALTH.
  TOPIC(S): SC1-DTH-03-2018 - ADAPTIVE SMART WORKING AND LIVING ENVIRONMENTS SUPPORTING ACTIVE AND HEALTHY AGEING.
  CALL FOR PROPOSAL: H2020-SC1-DTH-2018-1.
  FUNDING SCHEME: RIA - RESEARCH AND INNOVATION ACTION.

  Coordinated by: Instituto Tecnólogico de Castilla y Leon (ITCL), Spain

  Gerardo Pelosi is Co-Principal Investigator
  as person in charge of the proposal for the Politecnico di Milano group of participants (POLIMI) with an EU Contribution amount equal to **EUR 370 000**, **00**.

  Project objective:
  WorkingAge will focus on the usage of innovative Human Computer Interaction (HCI) methods, including augmented reality, virtual reality, gesture/voice recognition and gaze tracking to measure the user's psychological/emotional/health state, as well as it will focus on Internet of Things (IoT) technologies to measure environmental conditions, taking into consideration gender, ethics and security aspects.
  The WorkingAge project will create a sustainable and scalable product that will empower its user's comfort by easing their work life, attenuating the impact of aging in their autonomy, health and well-being. This unobtrusive, adaptive solution will analyze the need of employees in three different real working settings and living environments. The aim is to supervise health while promoting healthy habits of the users in their working/living environment in order to improve their active life conditions, while preserving the security and privacy of the measured data.
  [url: https://cordis.europa.eu/project/rcn/219015/factsheet/en]

ATTIVITÀ DI RICERCA FINANZIATE DA CONTRATTI DI RICERCA INDIVIDUALI

- Principal investigator at Politecnico di Milano DEIB of the consultant contract of the duration of 6 (six) months, from June 2022 to December 2022, jointly with Università Politecnica delle Marche - DII, entitled: *Design and development of post-quantum cryptographic solutions based on error correcting codes*, stipulated between the Politecnico di Milano, represented by the Director of the Department of Electronics, Information and Bioengineering and **Next Ingegneria dei Sistemi S.p.A. Rome, Italy.**
  Amount funded: **EUR 24 000**, **00**.
- Principal investigator of the research contract of the duration of 1 (one) year, from May 30th, 2019 to May 29th, 2020, entitled: *Side Channel Attacks and Countermeasures for Embedded Software*, stipulated between the Politecnico di Milano, represented by the Director of the Department of Electronics, Information and Bioengineering and **STMicroelectronics S.r.l.**
  Amount funded: **EUR 30 000**, **00**.

- Principal investigator of the research contract of the duration of 3 (three) years, from January 2020 to January 2023, entitled: *Quantum Computing Algorithms: functional validation and performance assessment on the Atos Quantum Learning Machine*, stipulated between the Politecnico di Milano, represented by the Director of the Department of Electronics, Information and Bioengineering and **Atos Italia S.p.A.**
  Amount funded: **EUR 110 000**, **00**.
- Scientific advisor of a Ph.D. student with an industrially sponsored scholarship in the area of Computer Science and Engineering for the Ph.D. programme in Information Technology at Politecnico di Milano (XXXVI cycle call), 2021-2023. Funding company: **STMicroelectronics S.r.l.**
  Amount funded: **EUR 72 000**, **00**.
- Scientific advisor of an Executive Ph.D. student enrolled in the PhD programme in Information Technology - area of Computer Science and Engineering - at Politecnico di Milano (XXXVI cycle call), 2021-2024. Funding Company: **GoQuantum: Post-quantum industrial and telecom encryption solutions provider**.
  Amount funded: **EUR 30 000**, **00**.

ATTIVITÀ IN PROGETTI DI RICERCA INTERNAZIONALI

- "**RECIPE - REliable power and time-ConstraInts-aware Predictive management of heterogeneous Exascale systems**"
  From 1st May 2018 to 30th April 2021.
  GRANT AGREEMENT ID: 801137.
  FUNDED UNDER: H2020-EU.1.2.2. (OVERALL BUDGET: EUR 3 290 800)
  PROGRAMME(S): H2020-EU.1.2.2. - FET PROACTIVE.
  TOPIC(S): FETHPC-02-2017 - TRANSITION TO EXASCALE COMPUTING.
  CALL FOR PROPOSAL: H2020-FETHPC-2017.
  FUNDING SCHEME: RIA - RESEARCH AND INNOVATION ACTION.
  RECIPE Principal Investigator - Politecnico di Milano (POLIMI): Prof. William Fornaciari.

  Role in the project: member of the key personnel of the POLIMI group of participants.
  Project objective:
  The current HPC facilities will need to grow by an order of magnitude in the next few years to reach the Exascale range. The dedicated middleware needed to manage the enormous complexity of future HPC centers, where deep heterogeneity is needed to handle the wide variety of applications within reasonable power budgets, will be one of the most critical aspects in the evolution of HPC infrastructure towards Exascale. This middleware will need to address the critical issue of reliability in face of the increasing number of resources, and therefore decreasing mean time between failures. To close this gap, RECIPE provides: a hierarchical runtime resource management infrastructure optimizing energy efficiency and ensuring reliability for both time-critical and throughput-oriented computation; a predictive reliability methodology to support the enforcing of QoS guarantees in face of both transient and long-term hardware failures, including thermal, timing and reliability models; and a set of integration layers allowing the resource manager to interact with both the application and the underlying deeply heterogeneous architecture, addressing them in a disaggregate way. Quantitative goals for RECIPE include: 25% increase in energy efficiency (performance/watt) with an 15% MTTF improvement due to proactive thermal management; energy-delay product improved up to 25%; 20% reduction of faulty executions. The project will assess its results against the following set of real world use cases, addressing key application domains ranging from well established HPC applications such as geophysical exploration and meteorology, to emerging application domains such as biomedical machine learning and data analytics. To this end, RECIPE relies on a consortium composed of four leading academic partners (POLIMI,UPV,EPFL,CeRICT); two supercomputing centers, BSC and PSNC; a research hospital, CHUV, and an SME, IBTS, which pro-

vide effective exploitation avenues through industry-based use cases.
[url: https://cordis.europa.eu/project/rcn/215836/factsheet/en]

- "**SafeCOP - Safe Cooperating Cyber-Physical Systems using Wireless Communication**"
ECSEL JOINT UNDERTAKING PROJECT
CALL: H2020-ECSEL-2015-1-RIA-TWO-STAGE - RESEARCH AND INNOVATION ACTIONS (RIA) – GRANT AGREEMENT NUMBER: 692529.
From 1st April 2016 to 31st March 2019.
Role in the project: member of the key personnel of the POLIMI group of participants.
Person in charge of the proposal for the Politecnico di Milano (POLIMI) group of participants:
Prof. William Fornaciari.
Project objective:
SafeCOP (Safe Cooperating Cyber-Physical Systems using Wireless Communication) will establish a safety assurance approach, a platform architecture, and tools for cost-efficient and practical certification of cooperating cyber-physical systems (CO-CPS).
SafeCOP targets safety-related CO-CPS characterized by use of wireless communication, multiple stakeholders, dynamic system definitions, and unpredictable operating environments. In this scenario, no single stakeholder has the overall responsibility over the resulted system-of-systems; safe cooperation relies on the wireless communication; and security and privacy are important concerns. Although such CO-CPS can successfully address several societal challenges, and can lead to new applications and new markets, their certification and development is not adequately addressed by existing practices.
SafeCOP will provide an approach to the safety assurance of CO-CPS, enabling thus their certification and development. The project will define a platform architecture and will develop methods and tools, which will be used to produce safety assurance evidence needed to certify cooperative functions. SafeCOP will extend current wireless technologies to ensure safe and secure cooperation. SafeCOP will also contribute to new standards and regulations, by providing certification authorities and standardization committees with the scientifically validated solutions needed to craft effective standards extended to also address cooperation and system-of-systems issues. SafeCOP brings clear benefits in terms of cross-domain certification practice and implementations of cooperating systems in all addressed areas: automotive, maritime, healthcare and robotics. The advantages include lower certification costs, increased trustworthiness of wireless communication, reduced effort for verification and validation, lower total system costs, shorter time to market and increased market share.
[url: http://cordis.europa.eu/project/rcn/203404_en.html]

- "**M2DC - Modular Microserver DataCentre**"
EU PROJECT - HORIZON 2020 PROGRAMME - RESEARCH AND INNOVATION ACTIONS (RIA) - CALL: H2020-ICT-2015 - TOPIC: ICT-04-2015 – PROPOSAL NUMBER: 688201.
From 1st January 2016 to to 31st December 2018.
Person in charge of the proposal for the Politecnico di Milano (POLIMI) group of participants:
Prof. William Fornaciari.
Role in the project:
Task leader – T1.1 "Application requirements", and member of the key personnel of the POLIMI group of participants.
Project objective:
Modular Microserver DataCentre (M2DC) will investigate, develop and demonstrate (Technology Readiness Level 7) a modular, highly-efficient, cost-optimized server architecture composed of heterogeneous microserver computing resources, being able to be tailored to meet requirements from various application domains such as image processing, cloud computing or even HPC. To achieve this objective, M2DC will be built on three main pillars:

[Pillar 1] A flexible server architecture that can be easily customised, maintained and updated so as to

enable adaptation of the data centre. Open server architecture will enable integration of computing resources with constrained thermal power dissipation such as embedded CPUs, GPUs, FPGAs, manycore processors integrated using established standards such as COM Express.

[Pillar 2] Advanced management strategies [Pillar 2a] and system efficiency enhancements (SEE) [Pillar 2b] will improve the behaviour of the system during runtime. The server architecture will include built-in enhancements (e.g., for computing acceleration, energy efficiency, dependability and security, behaviour monitoring, etc.) on system level.

[Pillar 3] Well-defined interfaces to surrounding software ecosystem will allow for an easy integration into existing data centre management solutions through the use of the latest middleware software for resource management, provisioning, etc.

The results of these three pillars will be combined to produce TCO (Total Cost of Ownership)-optimized appliances, deployed in a real data centre environment and seamlessly interacting with existing infrastructure to run real-life applications.
[url: http://cordis.europa.eu/project/rcn/199583_en.html]

- "**MANGO: exploring Manycore Architectures for Next-GeneratiOn HPC systems**"
EU PROJECT - HORIZON 2020 PROGRAMME - RESEARCH AND INNOVATION ACTIONS (RIA) - CALL: H2020-FETHPC-2014SEE - TOPIC: FETHPC-1-2014 - HPC CORE TECHNOLOGIES, PROGRAMMING ENVIRONMENTS AND ALGORITHMS FOR EXTREME PARALLELISM AND EXTREME DATA APPLICATIONS – PROPOSAL NUMBER: 671668.
From 1st October 2015 to 30th September 2018.
Person in charge of the proposal for the Politecnico di Milano (POLIMI) group of participants:
Prof. William Fornaciari.
Role in the project:
Task leader – T1.5 "Software Stack Specification", and member of the key personnel of the POLIMI group of participants.
Project objective:
MANGO targets to achieve extreme resource efficiency in future QoS-sensitive HPC through ambitious cross-boundary architecture exploration for performance/power/predictability (PPP) based on the definition of new-generation high-performance, power-efficient, heterogeneous architectures with native mechanisms for isolation and quality-of-service, and an innovative two-phase passive cooling system. Its disruptive approach will involve many interrelated mechanisms at various architectural levels, including heterogeneous computing cores, memory architectures, interconnects, run-time resource management, power monitoring and cooling, to the programming models. The system architecture will be inherently heterogeneous as an enabler for efficiency and application-based customization, where general-purpose compute nodes (GN) are intertwined with heterogeneous acceleration nodes (HN), linked by an across-boundary homogeneous interconnect. It will provide guarantees for predictability, bandwidth and latency for the whole HN node infrastructure, allowing dynamic adaptation to applications. MANGO will develop a toolset for PPP and explore holistic pro-active thermal and power management for energy optimization including chip, board and rack cooling levels, creating a hitherto inexistent link between HW and SW effects at all layers. Project will build an effective large-scale emulation platform. The architecture will be validated through noticeable examples of application with QoS and high-performance requirements.
Ultimately, the combined interplay of the multi-level innovative solutions brought by MANGO will result in a new positioning in the PPP space, ensuring sustainable performance as high as 100 PFLOPS for the realistic levels of power consumption (<15MWatt) delivered to QoS-sensitive applications in large-scale capacity computing scenarios providing essential building blocks at the architectural level enabling the full realization of the ETP4HPC strategic research agenda
[url: http://cordis.europa.eu/project/rcn/197942_en.html]

- "**TOISE - Trusted Computing for European Embedded Systems"**
  ENIAC JOINT UNDERTAKING, ENIAC-2010-1 – NUMBER: 282557-2. HTTP://WWW.TOISE.EU
  From 1st January 2011 to 1st December 2013.
  Person in charge of the proposal for the Politecnico di Milano (POLIMI) group of participants:
  Prof. Luca Breveglieri.
  Role in the project:
  member of the key personnel of the POLIMI group of participants.
  Project Objective:
  For the future European applications such as Smart Grids for electricity network, smart low energy controlled home appliance, smart logistics and monitoring of goods, environmental or infrastructure sensor networks, and more generally more wireless communications and more networking functionalities, a number of technologies need to be developed and put in place to make the solutions smarter and more secure. TOISE proposes to address the secure tamper resistant solutions needed by the related embedded applications. Trusted Computing now in practise for the PC and workstation area provides a proven approach face to new attacks, by implementing a chain of authentication and integrity from the boot of the computing platform to the applications set up. The objective of TOISE is to define, develop and validate trust hardware and firmware mechanisms applicable both to lightweight embedded devices and as security anchors within related embedded platforms. The aim is to maintain Europe as a worldwide player in the field of efficient implementation of secure integrated devices to address the future European applications. A large initiative is proposed to align a common European position in the area. This will be actually a effort from major European semiconductor, fables and foundry players (Austriamicrosystems, Atmel, Infineon, Numonyx, NXP and STMicroelectronics), four IP providers (Intrinsic-ID, Magillem, Secure IC, Virage Logic) for PUF and secure IP infrastructure, two SME experts in Security solutions or evaluation labs (Brightsight, Fox-IT), five SME experts in Power line communications (AZCom), Metering (Elster), Energy management (MW Energie AG, Mixed Mode), Wireless network for Energy management and Public Health and Administration (TST), competent research groups in the participating countries to support related R&D (Cea Leti and Telecom ParisTech, CNM and UC, FHG SIT and RWTH, ICCS, PoliMi and UniMiB, TUE, BUT),and leaders in the market of secure and safety
  [url: http://cordis.europa.eu/project/rcn/201953_en.html]
- "**PrimeLife - Bringing sustainable privacy and identity management to future networks and services**", EU FRAMEWORK PROGRAMME 7, ICT-2007.1.4 – NUMBER: 216483.
  HTTP://WWW.PRIMELIFE.EU
  From 1st March 2008 to 30th June 2011.
  Person in charge of the proposal for the University of Bergamo (UNIBG) group of participants:
  Prof. Stefano Paraboschi.
  Role in the project:
  member of the key personnel of the UNIBG group of participants.
  Project Objective:
  Individuals in the Information Society want to protect their autonomy and retain control over personal information, irrespective of their activities. Information technologies hardly consider those requirements, thereby putting the privacy of the citizen at risk. Today, the increasingly collaborative character of the Internet enables anyone to compose service and contribute and distribute information. Individuals will contribute throughout their life leaving a life-long trail of personal data. This raises substantial new privacy challenges: A first technical challenge is how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities. A second challenge is how to maintain life-long privacy. PrimeLife will resolve the core privacy and trust issues pertaining to these challenges. Its long-term vision is to counter the trend to life-long personal data trails data without compromising on functionality. We will build upon and expand the sound foundation of the FP6 project PRIME that has

shown how privacy technologies can enable citizens to execute their legal rights to control personal information in on-line transactions. Resolving these issues requires substantial progress in many underlying technologies. PrimeLife will substantially advance the state of the art in the areas of human computer interfaces, configurable policy languages, web service federations, infrastructures and privacy-enhancing cryptography. PrimeLife will ensure that the community at large adopts privacy technologies. To this effect PrimeLife will work with the relevant Open Source communities and standardization bodies, and partner projects. It will further organize workshops with interested parties such as partner projects to transfer technologies and concepts. This will also validate the project's results on a large scale. European industry will be strengthened by providing building blocks for trustworthy treatment of customers' data. [url: http://cordis.europa.eu/project/rcn/85453_en.html]

ATTIVITÀ IN PROGETTI DI RICERCA NAZIONALI

- "**PEPPER: Privacy E Protezione di dati PERsonali**"
  ITALIAN NATIONAL RESEARCH PROJECT (PRIN-2008).
  (local project leader: Prof. Stefano Paraboschi)
  Topics: database & information systems privacy; secure indexing in relational databases.
- "**SESAME - Scalable Efficient Secure Autonomic MEsh networks**"
  ITALIAN NATIONAL RESEARCH PROJECT (PRIN-2007). Work Package 3: Security.
  (local project leader: Prof. Fabio Martignon)
  Topic: enhanced architectures for access control management and user's privacy protection.
- "**Cryptographic Databases**"
  ITALIAN NATIONAL RESEARCH PROJECT (PRIN-2006)
  (local project leader: Prof. Stefano Paraboschi)
  Topic: models for encrypted data management in relational databases.
- "**Let's Research**"
  EUROPEAN SOCIAL FOUNDING FRAMEWORK PROJECT (FSE-2006), ID. N. 410978,
  (local project leader: Prof. Stefano Paraboschi)
  Topic: information security, with emphasis in the areas of access control, key management and authentication in the "database-as-a-service" scenario.

Attività di valutatore in processi di valutazione della ricerca

Ago. 2022 - Set. 2022

Commissario valutatore per la procedura pubblica di selezione indetta con D.R. N. 452/22 del 12/5/2022, per la copertura di N. 1 posto di ricercatore a tempo determinato (RTD) ai sensi dell'art. 24 comma 3, lettera A della legge 240/2010 e del regolamento d'ateneo vigente SC 09/H1 - SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI SSD ING-INF/05 - SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI, presso il Dipartimento di Ingegneria Gestionale, dell'Informazione e della Produzione dell'Università degli Studi di Bergamo.
Decreto Rettorale di nomina avente data 03-08-2022, repertorio (Rep.) 672/2022, protocollo 0138394/VII/1.

Nov. 2021 - Gen. 2022

Nomina, da parte dell'Agenzia Nazionale per la Valutazione del Sistema Universitario e della Ricerca (ANVUR), come revisore nel contesto delle attività di valutazione della ricerca a livello nazionale italiano (VQR) per il periodo 2015-2019,

Attività come membro di commissioni giudicatrici per l'esame finale di corsi di dottorato di ricerca

Apr. 2020

Nomina come membro della commissione giudicatrice per l'esame finale del corso di dottorato di ricerca in "Ingegneria e Scienze Applicate - Curriculum Tecnologie per l'ingegneria dell'informazione e la meccatronica" XXXII ciclo, dell'Università degli Studi di Bergamo. Decreto rettorale di nomina Rep. 153/2020 prot. 58129/III/6 del 6.04.2020 - [UOR: SI000050 - Classif. III/6].

Attività come valutatore esterno di tesi di dottorato di ricerca

Nov. 2021 - Gen. 2022

Revisore esperto invitato dalla Scuola di Alta Formazione Dottorale (SAFD), dell'Università degli Studi di Bergamo, nell'ambito del corso di studi in Ingegneria e Scienze Applicate (ISA), come valutatore di una tesi di dottorato.
XXXIV ciclo del programma di dottorato – S.S.D.: ING-INF/05.
Titolo della tesi di dottorato revisionata: "Technologies for the secure collection, sanitization, processing and release of data".

Feb. 2020 - Mar. 2020

Revisore esperto invitato dal coordinatore del programma di dottorato in Ingegneria e Scienze dell'Informazione – Curriculum Systems Engineering, Telecommunications and HW/SW platforms, dell'Università degli Studi dell'Aquila PhD Program in Information and Communication Technologies at Dipartimento di Ingegneria e scienze dell'Informazione (DISIM), come valutatore di una tesi di dottorato.
XXXII ciclo del programma di dottorato – S.S.D.: ING-INF/05.
Titolo della tesi di dottorato revisionata: "A Security Framework for Wireless Sensor Networks".

Nov. 2019 - Gen. 2020

Revisore esperto invitato dalla Scuola di Alta Formazione Dottorale (SAFD), dell'Università degli Studi di Bergamo, nell'ambito del corso di studi in Ingegneria e Scienze Applicate (ISA), come valutatore di una tesi di dottorato.
XXXII ciclo del programma di dottorato – S.S.D.: ING-INF/05.
Titolo della tesi di dottorato revisionata: "Protecting Resources and Regulating Access in Centralized and Decentralized Cloud Systems".

Dic. 2016 – Feb. 2017

Revisore esperto invitato dalla Scuola di Alta Formazione Dottorale (SAFD), dell'Università degli Studi

di Bergamo, nell'ambito del corso di studi in Ingegneria e Scienze Applicate (ISA), come valutatore di una tesi di dottorato. XXIX ciclo del programma di dottorato – S.S.D.: ING-INF/05.
Titolo della tesi di dottorato revisionata: "Model-based Techniques for the Design of Modern Software Systems".

Attività come membro di associazioni e iniziative della Comunità Europea

Oct. 2021 -

Esperto selezionato dall'associazione European Open Science Cloud (EOSC - https://www.eosc.eu) come membro del gruppo di lavoro su *e-science Authentication and Authorisation Infrastructure (AAI)* per conto del Politcnico di Milano.

Attività come selezionatore di progetti di ricerca internazionali e nazionali

- Revisore esperto invitato formalmente dal Research Council of Norway (RCN) per la valutazione d'eccellenza scientifica, impatto e sviluppo delle proposte di progetto finanziato riguardanti argomenti in ambito ICT e in particolare computer security come specificato nella open-ended call del RCN intitolata "Collaborative Project on Digital Security and Artificial Intelligence, Robotics and Autonomous Systems." (https://www.forskningsradet.no/en/call-for-proposals/2020/digital-security/) Periodo di attività: Giugno - Ottobre 2022.
- Revisore esperto invitato formalmente dal Research Council of Norway (RCN) per la valutazione d'eccellenza scientifica, impatto e sviluppo delle proposte di progetto finanziato riguardanti argomenti in ambito ICT e in particolare computer security, cryptography, hardware security and data security and privacy, sottoposte alla valutazione del RCN entro il 2 Febbraio 2022. Attività svolta da Aprile a Maggio 2022. https://www.forskningsradet.no/en/
- Revisore esperto e *Rapporteur* invitato (Dicembre 2021) dall'Università Ca' Foscari di Venezia (UNIVE) per la valutazione dell'eccellenza scientifica delle proposte di progetto finanziato e del curriculum vitae dei rispettivi *principal investigator* partecipanti al programma internazionale "G@V - Research and Training for Global Challenges" dell'Università Ca' Foscari di Venezia cofinanziato dalla Commissione Europea (Grant Agreement no. 945361) tramite lo schema *Marie Skłodowska-Curie Actions*.
- Revisore esperto invitato (Gennaio 2019) dal *National Center of Science and Technology Evaluation* (NCSTE, http://www.ncste.kz/en) – Ministry of Education and Science – Astana, Republic of Kazakhstan, per la valutazione di sei richieste di finanziamento nell'ambito del piano nazionale kazako per lo sviluppo di progetti di ricerca in ambito cybersecurity (nel triennio 2019-2021) come dal bando pubblicato nel Dicembre 2018 dal *Ministry of Defense of the Republic of Kazakhstan* (RoK).
- Revisore esperto invitato (Luglio 2018) dal Ministero dell'Istruzione, Università e Ricerca (MIUR) per valutare il profilo scientifico dei ricercatori partecipanti al Bando 2017 del programma "Rita Levi Montalcini" volto a attrarre giovani ricercatori in Italia e/o incoraggiare il ritorno di giovani ricercatori italiani all'estero. Il programma di assunzione segue l'art.6, del decreto ministeriale no. 1006 (18A01307) (GU Serie Generale n.47 del 26-02-2018) del 20 Dicembre 2017; e si rivolge a giovani studiosi di tutte le nazionalità che siano in possesso del titolo di dottorato di ricerca (PhD), o equivalente, e che abbiano svolto attività di insegnamento o attività di ricerca post-dottorato per almeno tre anni all'estero in riconosciute Università o enti di ricerca.

- Revisore esperto invitato (Giugno 2018) dall'Università di Verona per la valutazione scientifica dei progetti biennali presentati nell'ambito del bando di ateneo dell'Università di Verona per il finanziamento di *Progetti per la Ricerca di Base 2017*. S.S.D. ING-INF/05; ERC PE6_1, PE6_2.
- Revisore esperto invitato (Marzo 2018) dall'*Agenzia Nazionale delle Ricerche* (ANR) francese – *Comitato di valutazione scientifica: CES 25 - Infrastrutture di comunicazione ad alte prestazioni (comunicazioni, informatica e archiviazione), Scienza e tecnologie dell'informazione*, per la valutazione di una richiesta di finanziamento nell'ambito del piano nazionale francese di finanziamento quadriennale ai progetti di ricerca fondamentale presentati nel 2018.
  Agence Nationale de la Recherche (ANR) – Appel à projets générique 2018. Instrument de financement: Projet de recherche collaborative - Entreprise (PRCE). Catégorie R&D: Recherche fondamentale. Comité D'évaluation Scientifique (CES) Sélectionné 25 – Infrastructures de communication hautes performances (réseau, calcul et stockage), Sciences et technologies logicielles.
- Revisore esperto invitato (Luglio 2017) dalla Commissione Europea (DG Connect – Cybersecurity & Digital Privacy - Unit H 1), come membro della commissione di valutazione per il progetto finanziato H2020 "REASSURE – Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience", Project ID: 731591, Funding scheme: RIA–*Research and Innovation Action*, 1 Gennaio 2017 – 31 Dicembre 2019, url: http://cordis.europa.eu/project/rcn/207201_en.html.

ATTIVITÀ DI SERVIZIO COME MEMBRO DI COMMISSIONI DI VALUTAZIONI COMPARATIVE PER INCARICHI DIDATTICI E DI RICERCA ISTITUITE DAL POLITECNICO DI MILANO

- Componente della commissione giudicatrice incaricata della selezione pubblica per il conferimento di posti n. 1 per lo svolgimento di attività di ricerca a tempo determinato per la durata di 12 mesi nell'ambito del programma di ricerca denominato "Disegno e testing di algoritmi di HPC su architetture quantistiche – Sviluppare algoritmi per quantum computers"; presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano.
  Prot. n./Prot. no. 224491. Data/Date 30/09/2022. Rep. n. /Index no. 9868/2022.
  Codice Procedura: 2022_ASSEGNI_DEIB_89.
- Membro della Commissione per l'esame di ammissione ai corsi di dottorato di ricerca in *Information Technology* 38esimo ciclo del Politecnico di Milano, 2022. Decreto Rettorale 01 Giugno 2022 - Prot. n. 0136412 del 01/06/2022 - [UOR:32 - Classif. III/6]
- Componente (con anche funzioni di segretario verbalizzante) della commissione giudicatrice incaricata della selezione pubblica per il conferimento di n. 1 incarico di collaborazione per attività di supporto alla ricerca: "Analisi e rappresentazione di dati georeferenziati, con aspetti di adattività a vari contesti e aspetti di security e privacy"; presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano.
  Bando n. 38/2021/DEIB. Prot. n. 0071295 del 29/04/2021 - [UOR: SI000129 - Classif. VII/16]
- Componente (con anche funzioni di segretario verbalizzante) della commissione giudicatrice incaricata della selezione pubblica per il conferimento di n. 1 incarico di collaborazione per attività di supporto alla ricerca: "Metodi di Analisi Dati per elaborare Gesti Umani utilizzando tecniche di Machine Learning, realizzando un prototipo per gesti complessi"; presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano.
  Bando n. 35/2020/DEIB. Prot. n. 0089564 del 17/06/2020 - [UOR: SI000129 - Classif. VII/16]
- Componente della commissione giudicatrice incaricata della selezione pubblica per il conferimento di posti n. 1 per lo svolgimento di attività di ricerca a tempo determinato per la durata di 12 mesi nell'ambito del programma di ricerca denominato "Ottimizzazione di architetture per reti neurali convoluzionali: architetture dei calcolatori"; presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano.
  Prot.n. 227941; Data 19/12/2019; Rep.n. 9770/2019.
  Codice Procedura: 2019_ASSEGNI_DEIB_252.
- Presidente della commissione incaricata della procedura di valutazione comparativa per il conferimento di un assegno di ricerca presso il Dipartimento di Elettronica, Informazione e Bioingegneria per attività dal titolo: "Ideazione e valutazione della complessitÃ di algoritmi per Quantum Computing".
  Prot. n./Prot. no. 10509; Data 24/01/2020; Rep. n./Index no. 682/2020. Codice Procedura: 2020_ASSEGNI_DEIB_3.
- Componente della commissione incaricata della procedura di valutazione comparativa per il conferimento di due incarichi di collaborazione presso il Dipartimento di Elettronica, Informazione e Bioingegneria per attività di supporto alla ricerca bando nr. 87/2019 - DEIB: "Architetture per Reti Neurali Convoluzionali".
  Prot. n. 0225288 del 17/12/2019 - [UOR: SI000129 - Classif. VII/16]
- Componente della commissione incaricata della procedura di valutazione comparativa per il conferimento di un incarico di collaborazione presso il Dipartimento di Elettronica, Informazione e Bioingegneria per attività di supporto alla ricerca bando nr. 70/2019 - DEIB: "Stima e controllo a livello microarchitetturale del consumo energetico di sistemi embedded".
  Prot. n. 0170618 del 11/10/2019 - [UOR: SI000129 - Classif. VII/16]
- Presidente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 12 mesi nell'ambito

del programma di ricerca denominato “Tecniche crittografiche di protezione e indicizzazione dei dati: tecniche crittografiche per la sicurezza dei dati nella ricerca di sottostringhe su dati remoti.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0163855. 17 Ottobre 2019.

- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 12 mesi nell’ambito del programma di ricerca denominato “Metodologie e tecniche per il progetto di architetture per reti neurali convoluzionali profonde / Metodologie di progetto e tecniche di mapping.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0156215. 7 Ottobre 2019.
- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 12 mesi nell’ambito del programma di ricerca denominato “Miglioramento della predicibilità temporale di sistemi di calcolo *multicore*. Analisi dell’efficacia nell’uso di tecniche basate su *probabilistic-WCET analysis*.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0156233. 4 Ottobre 2019.
- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 12 mesi nell’ambito del programma di ricerca denominato “Interfacce HCI accessibili e avanzate per ambienti di *smart working* / Studio di un’interfaccia accessibile per estrarre informazioni dalla voce nel progetto WorkingAge.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0146905. 16 Settembre 2019.
- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 12 mesi nell’ambito del programma di ricerca denominato “Progettazione, realizzazione e validazione di un prototipo per l’analisi dell’interazione vocale nel progetto WorkingAge.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0146906. 16 Settembre 2019.
- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un posto per lo svolgimento di attivitá di ricerca a tempo determinato per la durata di 16 mesi nell’ambito del programma di ricerca denominato “Sicurezza dei dispositivi di memoria tradizionale e innovativa non-volatile. Modelli di rischio e attacchi per tenologie di memoria non volatile.” Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Numero di Protocollo interno del Politecnico di Milano: 2019 III/13 N. 0124922. 31 Luglio 2019.
- Componente della commissione giudicatrice della selezione pubblica indetta per il conferimento di un incarico di collaborazione per lo svolgimento di attivitá di supporto alla ricerca “Estensione del Framework TAFFO con stimatori di prestazioni basati su tecniche di machine learning”. Presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Milano.
Bando nr. 57/2019 - DEIB. Numero di Protocollo interno del Politecnico di Milano: 0122193 del 16/07/2019 [UOR: SI000129 - Classif. VII/16].
- Membro della commissione giudicatrice incaricata della valutazione comparativa per il conferimento di incarichi di collaborazione presso il Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria per le attività di docenza/didattica integrativa di tutorato dell’a.a. 2018/2019 su fondi Miur/Fondi di Ateneo.
Avvisi pubblici delle procedure comparative:
Prot. n. 0051800 del 27/03/2019 - [UOR: SI000129 - Classif. VII/16] – 2nd semester, 2do bando.
Prot. n. 0015322 del 06/02/2019 - [UOR: SI000129 - Classif. VII/16] – 2nd semester, 1mo bando.

(errata corrige) n. 0018071 del 12/02/2019 - [UOR: SI000129 - Classif. VII/16] – 2do sem., 1mo bando.
Prot. n. 0107412 del 17/10/2018 - [UOR: SI000129 - Classif. VII/16] – 1mo semestre. 2do bando.
Prot. n. 0085659 del 31/08/2018 - [UOR: SI000129 - Classif. VII/16] – 1mo semestre. 1mo bando.

- Membro della commissione giudicatrice incaricata della valutazione comparativa per il conferimento di un incarico di collaborazione presso il Dipartimento di Elettronica, Informazione e Bioingegneria per attività di supporto alla ricerca: "Modellazione a livello micro-architetturale del consumo di potenza". Avviso pubblico: prot. n. 0070541 del 13/07/2018 - [UOR: SI000129 - Classif. VII/16]
- Membro della commissione giudicatrice incaricata della valutazione comparativa per il conferimento di un incarico di collaborazione presso il Dipartimento di Elettronica, Informazione e Bioingegneria per attività di supporto alla ricerca: "Gestione dell'attività di Dissemination nell'ambito del progetto SafeCOP". Avviso pubblico: prot. n. 0022630 del 05/03/2018 - [UOR: SI000129 - Classif. VII/16]
- Membro della commissione giudicatrice incaricata della valutazione comparativa per il conferimento di incarichi di collaborazione presso il Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria per le attività di docenza/didattica integrativa di tutorato dell'a.a. 2017/2018 su fondi Miur/Fondi di Ateneo.
  Avvisi pubblici delle procedure comparative:
  Prot. n. 0047066 del 11/05/2018 - [UOR: SI000129 - Classif. VII/16] – 2do semestre. 3zo bando.
  Prot. n. 0031380 del 28/03/2018 - [UOR: SI000129 - Classif. VII/16] – 2do semestre. 2do bando.
  Prot. n. 0008503 del 30/01/2018 - [UOR: SI000129 - Classif. VII/16] – 2do semestre. 1mo bando.
  Prot. n. 0106730 del 15/11/2017 - [UOR: SI000129 - Classif. VII/16] – 1mo semestre. 2do bando.
  Prot. n. 0078667 del 06/09/2017 - [UOR: SI000129 - Classif. VII/16] – 1mo semestre. 1mo bando.
- Membro della commissione giudicatrice nominata per l'attribuzione di un assegno di ricerca presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), del Politecnico di Milano, dal titolo: "Ottimizzazione automatica delle applicazioni nell'ambito di sistemi dedicati e ad elevate prestazioni"
  Codice procedura interno del Politecnico di Milano: 2017ASSEGNI_DEIB51.
  Numero di Protocollo interno del Politecnico di Milano: 13-III-0096387, del 18 Ottobre 2017.
- Membro della commissione giudicatrice incaricata della valutazione comparativa per il conferimento di incarichi di collaborazione presso il Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria per le attività di docenza/didattica integrativa di tutorato dell'a.a. 2016/2017 su fondi Miur/Fondi di Ateneo.
  Avvisi pubblici della procedura comparativa.
  Prot. n. 0038444 del 05/05/2017 - [UOR: SI000129 - Classif. VII/16] – 2da call. Prot. n. 0088856 del 08/11/2016 - [UOR: SI000129 - Classif. VII/16] – 1ma call.

Organizzazione di conferenze e workshops

- TPC Co-chair of the 14th International Workshop on Security and High Performance Computing Systems (SHPCS 2019) – The 17th International Conference on High Performance Computing & Simulation (HPCS 2019). Dublin, Ireland. July 15–19, 2019. (ISBN: 978-1-xxxx-xxxx-x)
- TPC Co-chair and Co-Organizer of the 6th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2019), Valencia, Spain. January 21th, 2019. Proc. ACM.
(ISBN: 978-1-4503-6182-8)
- TPC Co-chair of the 13th International Workshop on Security and High Performance Computing Systems (SHPCS 2018) – The 16th International Conference on High Performance Computing & Simulation (HPCS 2018). Orléans, France. July 16–20, 2018. (ISBN: 978-1-5386-7878-7, BMS Part Number CFP1878H-ART) [url: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8514311]
- TPC Co-chair of the Special Session on Architectures and Hardware for Security Applications (AHSA) – 21st Euromicro Conference on Digital Systems Design DSD/SEAA 2018, Prague, Czech Republic, August 29–31, 2018. Proc. IEEE-CPS 2018. ISBN: 978-1-5386-7377-5.
- TPC Co-chair and Co-Organizer of the 5th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2018), Manchester, United Kingdom, January 22-24, 2018. Proc. ACM.
(ISBN: 978-1-4503-6374-7)
- TPC Chair and Co-Organizer of the 4th HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2017), Stockholm, Sweden, 24th January 2017. Proc. ACM.
(ISBN: 978-1-4503-4869-0)
- TPC Chair and Co-Organizer of the 3rd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2016), Prague, Czech Republic, 20th January 2016. Proc. ACM.
(ISBN: 978-1-4503-4065-6)
- TPC Chair and Co-Organizer of the 2nd HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2015), Amsterdam, The Netherlands, 19th January 2015. Proc. ACM.
(ISBN: 978-1-4503-3187-6)
- TPC Chair and Co-Organizer of the 1st HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2 2014), Vienna, Austria, 20th January 2014. Proc. ACM.
(ISBN: 978-1-4503-2484-7)

Attività come Associate Editor di riviste e membro di comitato editoriale

2019 – ongoing Associate editor of the 3rd Edition of Springer's *Encyclopedia on Cryptography, Security and Privacy*. Main responsibility: identify entries to be covered within the area and, for each entry, identifying outstanding researchers recognized as a reference leader in the topic for providing the entry content for the encyclopedia.

November, 2019 – ongoing Editorial Board member of Cryptography Journal. ISSN 2410-387X. MDPI.

July 21st, 2016 – ongoing. Associate Editor and editorial board member of the *Microprocessors and Microsystems* (MICPRO) *Journal*: Embedded Hardware Design, Elsevier BV. ISSN: 0141-9331.
Subject Area and Category: Computer Science–Hardware and Architecture, Computer Science–Computer Networks and Communications, Computer Science–Software, Computer Science–Artificial Intelligence.
Coverage: 1978-ongoing. H-index: 29.
(Source: Scimago Journal Ranking 2015)

August 25th, 2016 – ongoing. Associate Editor and editorial board member of the *Security and Communication Networks* (SCN) *Journal*, John Wiley and Sons, Inc. and Hindawi.
ISSN: 1939-0114 (Print), 1939-0122 (Online).
Subject Area and Category: Computer Science–Computer Networks and Communications, Computer Science–Information Systems. Coverage: 2009-ongoing. H-index: 15.
(Source: Scimago Journal Ranking 2015)

October 1st, 2011 – April 17th, 2013. Editorial Board Member of the *IEEE Systems Journal* – Special Issue on Security and Privacy in Complex Systems. Vol. 7, No. 2 June 2013 and Vol. 7, No. 3 September 2013. ISSN: 1932-8184.
Subject Area and Category: Engineering–Control and Systems Engineering; Engineering–Electrical and Electronic Engineering. Coverage: 2008-ongoing. H-index: 27.
(Source: Scimago Journal Ranking 2015)

Attività come membro di comitato scientifico di programma di conferenze internazionali

Gerardo Pelosi ha svolto attività di servizio nei comitati di programma delle seguenti confererenze:

2022

- The 21th IEEE International Conference on Trust, security and Privacy in Computing and Communications (TrustCom-2022), October 28–30, 2022, Wuhan, China. Proc. IEEE CPS 2022.
- 2022 IEEE International Conference on Cyber Security and Resilience (IEEE-CSR 2021), July 27-29, 2022 - Virtual Conference http://ieee-csr.org
- 2022 IEEE Conference on Communications and Network Security (CNS), Sep. 25 - 28, 2022. Austin, United States. Proc. IEEE 2022.
- 17th DPM International Workshop on Data Privacy Management (DPM 2022), Sep. 26 - 30, Copenhagen, Denmark. Proc. Springer LNCS 2022. co-located with the 27th European Symposium on Research in Computer Security (ESORICS 2022)
- 12th International Conference on Communication and Network Security (ICCNS 2022), December 1-3, 2022, China. Proc ACM 2022.
- The 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 30 October - 3 November 2022, San Diego, California, USA. Proc. IEEE 2022.
- 20th International Conference on Applied Cryptography and Network Security (ACNS 2022), June 20-23, 2022. Rome, Italy. Proc. LNCS, Springer 2022.
- 19th International Conference on Security and Cryptography (SECRYPT 2022), Lisbon, Portugal, July 11-13, 2022. Proc. ScitePress 2022.
- 2022 IEEE International Conference on Cyber-Security and Resilience (IEEE CSR 2022), virtual event, July 27-29, 2022. Proc. IEEE CPS 2022.
- 8th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2022), Xi'an, China, October 16-18, 2022. Proc. LNCS, Springer 2022.
- 25th Euromicro Conference on Digital System Design (DSD) – Special session on Architecture and Hardware for Security Applications (AHSA), Maspalomas, Gran Canaria, Spain, Aug. 31th – Sept. 2nd, 2022. Proc. IEEE CPS & IEEE Xplore DL 2022.

2021

- 2021 Top Picks in Hardware and Embedded Security Workshop - IEEE Hardware Security and Trust Technical Committee (IEEE HSTTC), https://www.ieee-hsttc.org/top-picks/. Co-located with the 2021 40th International Conference On Computer Aided Design (ICCAD 2021). November 1-4. Virtual. Proc. IEEE 2021.
- 7th Workshop on Security and Privacy in the Cloud (SPC 2021) which will be held virtually on October 7, 2021 in conjunction with the IEEE Conference on Communications and Network Security (CNS 2021). Proc. IEEE 2021.
- 20th Workshop on Privacy in the Electronic Society (WPES 2021), November 15, 2021. Seoul, South Korea, in conjunction with the ACM CCS conference. Proc. ACM 2021.
- 20th International Conference on Cryptology abd Network Security (CANS 2021), December 13-15, 2021. Vienna, Austria. Proc. LNCS, Springer 2021.
- 9th IEEE Conference on Communications and Network Security 2021 (IEEE CNS 2021). Virtual event (due to covid19 pandemic), 4-6 October 2021. Proc. IEEE 2021.
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2021), November 1-4, 2021, virtual event (due to covid19 pandemic). Proc.: IEEE/ACM 2021, Press: IEEE 2021.
- 7th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2021), November 19-21, 2021. Fujian Normal University, Fuzhou, China. Proc. LNCS, Springer 2021.

- IEEE Cyber Security & Resilience Conference (CSR 2021). Virtual event (due to covid19 pandemic), 26-28 July 2021. Proc. IEEE 2021.
- 18th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2021), September 16th, 2021, co-located with CHES 2021 and held in cooperation with IACR (www.iacr.org). Proc. IEEE-CPS.
- 11th IFIP International Conference on New technologies, Mobility & Security (NTMS 2021) April 19-21, 2021. Villejuif (Paris), Ile de France, 94800, France. Proc. IEEE 2021.
- 16th International Workshop on Data Privacy Management (DPM 2021), October 4-8, 2021, Darmstadt, Germany (co-located with ESORICS 2021). Proc. Springer LNCS 2021.
- 24th Euromicro Conference on Digital System Design (DSD 2021) – Special session on Architecture and Hardware for Security Applications (AHSA), Palermo, Italy, September 1-3, 2021. Proc. IEEE CPS & IEEE Xplore DL 2021.
- 2nd International Workshop on Code-Based Cryptography (CBCrypto 2021), Munich, Germany, 1-22 of June 2021. Proceedings: Lecture Notes in Computer Science, Springer 2021.
- 18th International Conference on Security and Cryptography (SECRYPT 2021), web-event (due to covid-19 pandemic), July 6-8, 2021. Proc. ScitePress 2021.
- 7th International Conference on Mathematics and Computing (ICMC 2021), Shibpur, West Bengal, India, March 02-05, 2021. Proc. Advances in Intelligent Systems and Computing (AISC) Series, Springer 2021.

2020

- Top Picks in Hardware and Embedded Security Workshop 2020 (TopinHES-20), 5 November 2020, Austin, TX, USA. Workshop co-located with ICCAD 2020 with presentations related to a shortlist of papers selected from conference papers that have appeared in leading hardware security conferences including but not limited to DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, USENIX Security, ASIA CCS, NDSS, and ACM CCS during the six years period 1/1/2014 – 12/31/2019.
- The 8th IEEE International Conference on Smart City and Informatization (iSCI 2020 Internet of Things and Smart Sensing), December 29, 2020 - January 1, 2021. Guangzhou, China. Proc. IEEE 2020.
- Seventeenth Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2020), September 13th, 2020, co-located with CHES 2020 and held in cooperation with IACR (www.iacr.org). Proc. IEEE-CPS.
- (Program Vice Chair) The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020). November 10–13, 2020. Guangzhou, China. Proc. IEEE 2020.
- 15th DPM International Workshop on Data Privacy Management (DPM 2020). September 17–18, 2020. Surrey, United Kingdom. Co-located with ESORICS 2020 in United Kingdom, September 2020. Proc. LNCS Springer 2020.
- Sixth International Workshop on Security and Privacy in the Cloud (SPC'20) 29 June – 1 July 2020, Avignon, France. Proc. IEEE 2020.
- 13th International Conference on Security of Information and Networks (SIN 2020), Istanbul, Turkey, September 10-13, 2020. Proceedings ACM ICPS 2020.
- 11th IFIP International Conference on New Technologies, Mobility & Security. July 6–6, 2020. Paris, France. Proc. IEEE 2020.
- 6th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2020), Tianjin, China, 22-23 August 2020. Proc. LNCS Springer 2020.
- 17th International Conference on Security and Cryptography (SECRYPT 2020), Lieusant, Paris, France, July 8-10, 2020. Proc. ScitePress 2019.
- 8th IEEE Conference on Communications and Network Security 2020 (IEEE CNS 2020). Avignon, France, 29 June - 1 July, 2020. Proc. IEEE 2020.
- 11th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE'20). Lugano, Switzerland, April 1-3, 2020. Proc. Lecture Notes in Computer Science, Springer 2020.

- 23rd Euromicro Conference on Digital System Design (DSD 2020) – Special session on Architecture and Hardware for Security Applications (AHSA), Portorož, Slovenia, August 26–28, 2020. KPortoRoz, Slovenia, August 26th-28th, 2020. Proc. IEEE CPS & IEEE Xplore DL 2020.
- International Workshop on Code-Based Cryptography (CBCrypto 2020), held in conjunction with Eurocrypt 2020. Zagreb, Croatia, May 9-10, 2020. Proceedings: Lecture Notes in Computer Science, Springer 2020.

2019

- 12th International Conference on Security of Information and Networks, September 12-15, Sochi, Russia. Proc. by ACM ICPS 2019.
- The 5th International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2019). November 12-15, 2019. Guangzhou, China. Proc. Lecture Notes in Computer Science, Springer 2019.
- Seventh International Symposium on Security in Computing and Communications (SSCC'19), Trivandrum, Kerala, India. December 18-21, 2019. Proc. Lecture Notes in Computer Science, Springer 2020.
- 22nd Euromicro Conference on Digital System Design (DSD 2019) – Special session on Architecture and Hardware for Security Applications (AHSA). Kallithea, Chalkidiki, Greece, Aug. 28-30, 2019. Proc. IEEE CPS & IEEE Xplore DL 2019.
- 16th International Conference on Security and Cryptography (SECRYPT 2019), July 26-28, 2019, Prague, Czech Republic. Proc. ScitePress 2019.
- 16th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2019), August 29, 2019, Atlanta, USA. Proc. IEEE-CPS.
- 5th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2019) Copenhagen, Denmark, 14-17 July 2019.
- 56th ACM/EDAC/IEEE Design Automation Conference (DAC 2019), June 2-6, Las Vegas, Nevada, USA. Proceedings ACM. (Invited External Reviewer)
- 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS'2019) – Security track. June 24-26, 2019. Canary Island, Spain. Proc. printed by IEEE CPS, copyright IEEE 2019.
- 5th International Conference on Mathematics and Computing (ICMC 2019), February 07-09, 2019 at Kalinga Institute of Industrial Technology, Bhubaneswar, India. Springer Proceedings in Mathematics & Statistics, Springer 2019.

2018

- Top Picks in Hardware and Embedded Security 2018 (TopinHES-18), 5-8 November 2018, San Diego, CA, USA. Workshop co-located with ICCAD 2018 with presentations related to a shortlist of papers selected from conference papers that have appeared in leading hardware security conferences including but not limited to DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, USENIX Security, ASIA CCS, NDSS, and ACM CCS during the six years period 2012 – 2017.
- 4th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2018), 10-12 December 2018, Santa Clara, CA, USA. IEEE Computer Society 2018.
- The 4th International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2018). December 11-13, 2018. Melbourne, Australia. Proc. Lecture Notes in Computer Science, Springer 2018.
- 11th International Conference On Security Of Information and Networks (SIN 2018), 10–12 September 2018, Cardiff, Wales, United Kingdom. Proc. ACM 2018.
- 13th International Workshop on Data Privacy Management (DPM 2018), co-located with the 23rd European Symposium on Research in Computer Security (ESORICS 2018), 6–7 September 2018, Barcelona, Spain. Proc. Lecture Notes in Computer Science, Springer 2018.

- 15th International Conference on Security and Cryptography (SECRYPT 2018), July 26-28, 2018, Porto, Portugal. Proc. ScitePress 2018.
- 15th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2018), September 13, 2018, Amsterdam, The Netherlands. Proc. IEEE-CPS.
- 9th IFIP International Conference on New Technologies, Mobility & Security (NTMS 2018), 26–28 February 2018. Paris, France. Technically co-sponsored by IEEE, IEEE COMSOC & IFIP TC6.5 WG. Proc. IEEE 2018.
- 4th IEEE Smart World Congress (SmartWorld 2018), Guangzhou, China, October 8-12, 2018. Proc. IEEE 2018.
- Sixth International Symposium on Security in Computing and Communications (SSCC'18), September 19–22, 2018, Bangalore, India. Proc. Springer – Communications in Computer and Information Science (CCIS) Series 2018.
- 21st Euromicro Conference on Digital Systems Design DSD/SEAA 2018 – Special Session on Architectures and Hardware for Security Applications (AHSA), August 29–31, 2018. Prague, Czech Republic Proc. IEEE-CS 2018.
- 55th ACM/EDAC/IEEE Design Automation Conference (DAC 2018), 24 Jun - 28 Jun 2018, San Francisco, CA, USA. Proceedings ACM. (Invited External Reviewer)
- 4th International Conference on Mathematics and Computing (ICMC 2018), January 9-11, 2018 Indian Institute of Technology (BHU), Varanasi, India. Springer Proceedings in Mathematics & Statistics, Springer India 2019.

2017

- 3rd International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2017), 13-15 December 2017, Melbourne, Australia. Proc. IEEE 2017.
- 16th ACM Workshop on Privacy in the Electronic Society (WPES 2017), October 30, 2017, Dallas, Texas, USA. Co-located with the 24th ACM Conference on Computer and Communications Security, 30 October – 3 November 2017. Proc. ACM.
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2017), November 13-16, 2017, Irvine Marriott, Irvine, California, USA. Proc.: IEEE/ACM 2017, Press: IEEE 2017.
- The 10th International Conference on Security of Information and Networks (SIN 2017), 13-15 October 2017, Manipal University Jaipur, Rajasthan, India. Proc. ACM-ICPS.
- 14th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2017), September 25, 2017, Taipei, Taiwan. Proc. IEEE-CPS.
- 54th Design Automation Conference (DAC 2017), External Reviewer for the Embedded and Cross-Layer Security track), June 18–22, 2017, Austin, TX, USA. Proc. ACM/IEEE 2017.
- 20th Euromicro Conference on Digital Systems Design DSD/SEAA 2017 – Special Session on Architectures and Hardware for Security Applications (AHSA), August 30th - Sept. 1st, 2017. Vienna, Austria. Proc. IEEE-CS 2017.
- 14th International Conference on Security and Cryptography (SECRYPT 2017), July 24-26, 2017, Madrid, Spain. Proc. ScitePress 2017.
- 11th International Conference on Frontier of Computer Science and Technology (FCST-2017), 21-23 June 2017, Exeter, UK. Proc. IEEE Computer Society 2017.
- International Conference on Mathematics and Computing (ICMC 2017), January 17-21, 2017 at Haldia, India. Springer Proceedings in Mathematics & Statistics, Springer India 2017.

2016

- 15th Workshop on Privacy in the Electronic Society (WPES 2016), co-located with the 23rd ACM Conference on Computer and Communications Security, Hofburg Palace, Vienna, Austria, October 24 – 28, 2016 Proc. ACM 2017.

- 11th International Workshop on Data Privacy Management (DPM 2016), co-located with the 21st European Symposium on Research in Computer Security (ESORICS 2016), 26–30 September 2016, Heraklion, Crete, Greece. Proc. Lecture Notes in Computer Science, Springer 2016.
- 2nd International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2016), 8–10 December 2016, Yanuca Island, Fiji. Proc. 2016 IEEE International Conference on Date of Conference on Computer and Information Technology (CIT), DOI: 10.1109/CIT.2016.125. IEEE 2017.
- 2nd International Forum on Research and Technologies for Society and Industry (RTSI 2016) - Technologies for smarter societies. Bologna, Italy, 7-9 September 2016. Proc. IEEE Computer Society.
- 10th WISTP International Conference on Information Security Theory and Practice (WISTP 2016), Heraklion, Crete, Greece, 26-27 September 2016. Proc. Springer-Verlag LNCS 2016.
- 15th International Conference on Cryptology and Network Security (CANS 2016), November 14-16, 2016, Milano, Italy. Proc. Springer LNCS 2016.
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2016), November 7–10, 2016, Austin, TX, USA. Proc.: IEEE/ACM 2016, Press: IEEE.
- 13th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2016), August 16, 2016, Santa Barbara, CA, USA. Proc. IEEE-CPS.
- 13th International Conference on Security and Cryptography (SECRYPT 2016), 26-28 July 2016, Lisbon, Portugal. Proc. SciTePress.
- The 9th International Conference on Security of Information and Networks (SIN 2016), 20-22 July 2016, Rutgers University, New Jersey, USA. Proc. ACM.
- 53rd Design Automation Conference (DAC 2016), External Reviewer for the Hardware and Embedded Systems Security track), June 5–9, 2016, Austin, TX, USA. Proc. ACM/IEEE.

2015

- IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2015), November 2–6, 2015, Austin, TX, USA. Proc.: IEEE/ACM 2015, Press: IEEE.
- International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2015) Hangzhou, China, 16-18 November, 2015. Proc. IEEE.
- 12th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2015), September 13, 2015, Saint-Malo, France. Proc. IEEE-CPS.
- 8th International Conference on Security of Information and Networks (SIN 2015), September 8–10, 2015 Sochi/Russia Proc. ACM.
- 12th International Conference on Security and Cryptography (SECRYPT 2015), 20–22 July, 2015, Colmar, Alsace, France. Proc. SciTePress.
- 9th International Conference on Frontier of Computer Science and Technology (FCST 2015), August 26–28, 2015, Dalian, China. Proc. IEEE Computer Society CPS.
- 9th International Conference on Network and System Security (NSS 2015), November 3–5, 2015, New York City, USA. Proc. Springer-Verlag LNCS.
- 52th Design Automation Conference (DAC 2015), External Reviewer for the Embedded Systems and Software track, and the Security track), June 7–11, 2015, San Francisco, CA, USA. Proc. ACM/IEEE.
- The 2015 International Symposium on Advances in Computing, Communications, Security, and Applications (ACSA 2015), February 24–26, 2015, Jeju, Korea.

2014

- 8th International Symposium on Digital Forensics and Information Security (DFIS 2014), December 17–19, 2014, Guam, USA.
- 7th International Conference on Security of Information and Networks (SIN 2014), September 9–11, 2014, School of Computing Science, Glasgow University, UK. Proc. ACM.
- 12th IEEE international conference on Dependable, Autonomic and Secure Computing (DASC 2014), August 24-27, 2014, Dalian, China. Proc. IEEE-CS.

- 11th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2014), September 23, 2014, Busan, South Korea. Proc. IEEE-CPS.
- International Symposium on Cyberspace Safety and Security (CSS 2014), 20-22 August 2014, Paris, France. Proc. IEEE-CS.
- 11th International Conference on Security and Cryptography (SECRYPT 2014), August 28-30, 2014, Vienna, Austria.
- 6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications (ACSA-14). April 23-25, 2014, Busan, Korea.
- 8th International Conference on Network and System Security (NSS 2014), Xi'an, China. October 16-18, 2014. Proc. Springer-Verlag LNCS.
- 51th Design Automation Conference (DAC 2014), Expert Reviewer Subcommitee: Hardware and Embedded Systems Security - Embedded Systems Design Methodologies), June 1-5, 2014, San Francisco, CA, USA. Proc. ACM.
- HiPEAC Workshop on Cryptography and Security in Computing Systems (CS^2), Vienna, Austria, 20th January 2014. Proc. ACM.

2013

- 5th International Symposium on Cyberspace Safety and Security (CSS 2013), Zhangjiajie, China, November 13-15, 2013. Proc. Springer-LNCS.
- 10th workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2013). August 20th, 2013, Santa Barbara, California, USA. IEEE 2013.
- 50th Design Automation Conference (DAC 2013), Expert Reviewer Subcommitee: Embedded Systems and Software (Embedded System Validation, Verification, Security, Dependability – Embedded Systems Design Methodologies), June 2-6, 2013, Austin, Texas, USA. Proc. ACM.
- The 7th International Conference on Network and System Security (NSS 2013). June 3-4, 2013. Madrid, Spain. Proc. Springer-Verlag LNCS.

2012

- 4th International Symposium on Cyberspace Safety and Security (CSS 2012). December 12-13, 2012, Melbourne, Australia. Proc. Springer-Verlag LNCS.
- International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA Summer 2012). June 26-28 2012, Vancouver, Canada.
- International Conference on Security and Cryptography (SECRYPT 2012), July 24-27, 2012, Rome, Italy.
- 49th Design Automation Conference (DAC 2012), Expert Reviewer Subcommitee: Embedded Systems and Software, June 3-7, 2012, San Francisco, California, USA. Proc. ACM.
- WISTP2012 - Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, June 19-22, 2012, London, United Kingdom. Proc. Springer-Verlag LNCS.
- 6th International Conference on Network and System Security (NSS 2012), November 21-23, 2012, Wu Yi Shan, Fujian, China. Proc. Springer-Verlag LNCS.

2011

- 9th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2011), December 12-14, 2011, Sydney Australia. (IEEE Computer Society Proceedings.)
- 8th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2011), September 28th, 2011, Nara (L-topia Nara), Japan. Proc. IEEE-CS.
- 5th International Conference on Network and System Security (NSS 2011), September, 2011, Milan, Italy. (IEEE Computer Society Proceedings; EI, ISTP, and INSPEC indexed.)
- 6th International Conference on Security and Cryptography (SECRYPT 2011), July 18-21, 2011, Seville, Spain. (Springer-Verlag CCIS Series book. CEPIS UPGRADE Journal. REICIS.)

- 5th Workshop on Information Security Theory and Practice – Security and Privacy of Mobile Devices in Wireless Communication (WISTP 2011), June 1-3, 2011, Heraklion, Crete, Greece. IFIP WG 11.2: Pervasive Systems Security. (Springer-LNCS)
- 6th International Workshop on Flexible Database and Information System Technology (FlexDBIST-2011). In conjunction with the International Conference on Database and Expert Systems Applications (DEXA 2011), August 29-September 2, 2011, Toulouse, France.

2009 - 2010

- 4th International Conference on Network and System Security (NSS 2010), September 1-3, 2010, Melbourne, Australia. (IEEE and IEEE Computer Society Technical Committee on Scalable Computing.)
- 5th International Conference on Security and Cryptography (SECRYPT 2010), July 26-28, 2010, Athens, Greece. (IACR–International Association for Cryptologic Research, WfMC–Workflow Management Coalition, Springer-Verlag CCIS Series book.)
- 4th Workshop on Information Security Theory and Practice (WISTP 2010), April 12-14, 2010, Passau, Germany. IFIP WG 11.2: Pervasive Systems Security. (Springer-LNCS)
- 5th International Workshop on Flexible Database and Information Systems Technology (FlexDBIST-10), August 30-September 3, 2010, Bilbao, Spain. In conjunction with DEXA-2010, 21th International Conference on Database and Expert Systems Applications. (IEEE)
- 4th International Workshop on Flexible Database and Information System Technology, (FlexDBIST-09), August 31-September 4, 2009, Linz, Austria. In conjunction with DEXA-2009, 20th International Conference on Database and Expert Systems Applications. (IEEE)

Attività come revisore scientifico per riviste e atti di conferenze internazionali

Gerardo Pelosi ha svolto attività come revisore per le seguenti riviste e conferenze internazionali:

2021

- IEEE Transactions on Emerging Topics in Computing (TETC), 2021. ISSN: 2168-6750. Impact Factor: 3.826. IEEE Computer Society 2021.

2020

- 25th European Symposium on Research in Computer Security (ESORICS) 2020. Guildford, United Kingdom, September 14-18 2020. Proceedings, Lecture Notes in Computer Science, Springer 2020.
- EAI SecureComm 2020 – 16th EAI International Conference on Security and Privacy in Communication Networks October 21-23, 2020, Washington DC, United States. Proceedings, Lecture Notes in Computer Science, Springer 2020.
- ACM SIGMOD/PODS International Conference on Management of Data. Portland, Oregon, USA, June 14-19, 2020. Proc. ACM 2020.
- Journal of Computer Security (JCS), ISSN (print): 0926-227X, ISSN (online): 1875-8924, SCImago Journal Rank (SJR): 0.373. IOS Press 2020.

2019

- 28th ACM International Conference on Information and Knowledge Management (CIKM), 3–7 November 2019, Beijing, China. Proceedings ACM 2019.
- 26th ACM Conference on Computer and Communications Security (CCS 2019), 11-15 November 2019, London, United Kingdom. Proceedings ACM SIGSAC 2019.
- 24th European Symposium on Research in Computer Security (ESORICS 2019), 23-27 September 2019, Luxembourg City, Luxembourg. Proceedings, Lecture Notes in Computer Science, Springer 2019.
- Transactions on Computer-Aided Design of Integrated Circuits and Systems, ISSN: 0278-0070. IF 2.089. IEEE 2019.
- Future Generation Computer Systems (FGCS) journal. ISSN: 0167-739X. IF 2017: 4.639, 5-Year IF: 4.968, SNIP: 2.472, SJR: 0.844. Elsevier, 2019.
- 39th IEEE International Conference on Distributed Computing Systems (ICDCS 2019), July 7-10, 2019. Dallas, Texas, USA.
- Computers & Security Journal (CoSe), ISSN: 0167-4048. Elsevier 2019.
- IEEE Transactions on Emerging Topics in Computing (TETC). ISSN: 2168-6750. Impact Factor: 3.826. IEEE Computer Society 2019.

2018

- International Journal of Information Security (IJIS). ISSN: 1615-5262, e-ISSN: 1615-5270. Springer-Verlag Berlin Heidelberg 2018.
- Computers & Security Journal (CoSe), ISSN: 0167-4048. Elsevier 2018.
- IEEE Transactions on Very Large Scale Integration (VLSI) Systems, ISSN: 1063-8210. Impact Factor: 1.744, IEEE 2018.
- International Journal of Network Security (IJNS), ISSN 1816-353X, e-ISSN 1816-3548, 2018.
- Microprocessors and Microsystems Journal. ISBN: 0141-9331. Impact Factor: 1.025, Elsevier 2018.
- IEEE Transactions on Circuits and Systems I, ISSN: 1549-8328 (print), Impact Factor: 2.407, IEEE 2018.

- Journal of Computer Security (JCS), ISSN (print): 0926-227X, ISSN (online): 1875-8924, SCImago Journal Rank (SJR): 0.373. IOS Press 2018.
- IEEE Embedded Systems Letters (ESL), ISSN (print): 1943-0663, ISSN (online): 1943-0663, SCImago Journal Rank (SJR): 0.357 (2016). IEEE 2018.
- IET Computers & Digital Techniques, ISSN (online): 1751-861X, ISSN (print): 1751-8601, 5-yrs Impact Factor: 0.589, SCImago Journal Rank (SJR): 0.210, SNIP: 0.722. IET 2018.
- IEEE Transactions on Reliability (TR), ISSN: 0018-9529, Impact Factor: 2.287, SCImago Journal Rank (SJR): 1.93. IEEE 2018.
- Journal of Information Security and Applications, 2018. ISSN: 2214-2126, eISSN: 2214-2134. Elsevier 2018.
- Transactions on Data Privacy: Foundations and Technologies, 2018. ISSN: 1888-5063; ISSN (Digital): 2013-1631. Scimago Journal Ranking (SJR) impact factor 2015: 0.553.
- IEEE Access journal. ISSN: 2169-3536. Impact Factor: 3.244, IEEE 2017.
- The 13th ACM ASIA Conference on Information, Computer and Communications Security (ACM ASIACCS 2018), Proc. ACM 2018.
- IEEE Internet of Things Journal (IoT-J). eISSN: 2327-4662. Impact Factor: 7.596. IEEE 2018. Published by: IEEE Computer Society, IEEE Communications Society, IEEE Sensors Council.
- IEEE Transactions on Emerging Topics in Computing (TETC). ISSN: 2168-6750. Impact Factor: 3.826. IEEE Computer Society 2018.
- 21st International conference on Design automation and Test in Europe (DATE 2018), March 19 - 23, 2018. Dresden, Saxony, Germany. Proc. IEEE 2018.
- 34th IEEE International Conference on Data Engineering (ICDE 2017), April 16th – 20th 2018. Paris, France. Proc. IEEE-Computer Society, 2018.

2017

- IEEE Access journal. ISSN: 2169-3536. Impact Factor: 3.244, IEEE 2017.
- 20th Information Security Conference (ISC 2017), Ho Chi Minh City, Viet Nam, 22-224th November, 2017. Proc. LNCS Springer 2017.
- 22nd European Symposium on Research in Computer Security (ESORICS 2017), Oslo, Norway on September 11–13, 2017. Proceedings, Lecture Notes in Computer Science, Springer 2017.
- 18th International Conference on Engineering Applications of Neural Networks (EANN 2017), Athens, Greece, August 25-27, 2017. Proceedings, Lecture Notes in Computer Science, Springer CCIS "Communications in Computer and Information Science", 2017.
- IEEE Transactions on Reliability (TR), ISSN: 0018-9529, Impact Factor: 2.287, SCImago Journal Rank (SJR): 1.93. IEEE 2017.
- IEEE Transactions on Emerging Topics in Computing (TETC), ISSN: 2168-6750, SCImago Journal Rank (SJR): 0.4. IEEE 2017.
- Computers & Security Journal (CoSe), ISSN: 0167-4048, 5-Year Impact Factor: 1.783, SCImago Journal Rank (SJR): 1.020. Elsevier 2017.
- International Journal on Future Generation Computer Systems (FGCS), ISSN: 0167-739X, 5-Year Impact Factor: 2.335, SCImago Journal Rank (SJR): 1.483. Elsevier 2017.
- IEEE Internet of Things Journal (IoT-J), ISSN: 2327-4662, IEEE 2017.

2016

- 17th International Conference on Design, Automation and Test in Europe (DATE 2017), March 27-31, 2017, Lausanne, CH. Proc. IEEE 2017.
- ACM Transactions on Autonomous and Adaptive Systems (TAAS) ISSN: 1556-4665, e-ISSN:1556-4703, 2016.
- IEEE Transactions on Information Forensics & Security (TIFS), ISSN: 1556-6013 (I.F. 2.441), 2016.
- International Annual Conference AEIT 2016, Sutainable Development in the Mediterranean Area *Energy and ICT Networks of the Future*, Capri, Italy, 5-7 October 2016. IEEE Italy Section.

- Proceedings of the Very Large Database (VLDB) Endowment, 2016.
- IEEE Transactions on Cloud Computing (TCC), ISSN: 2168-7161, IEEE 2016.
- IEEE Systems Journal (ISJ), ISSN: 1932-8184, (IF: 1.98) IEEE 2016.
- IEEE Internet of Things Journal (IoT-J), ISSN: 2327-4662, IEEE 2016.
- 42nd International Conference on Very Large Data Beses (VLDB), September 5-9, 2016, New Delhi, India. Proc. of the VLDB Endowment, 2016.
- 9th European Workshop on Systems Security (EuroSec), 18 April 2016, London, UK. Proc. ACM.
- 4th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2016) – Affiliated with ETAPS 2016, Eindhoven, The Netherlands, April 3rd, 2016.
- IEEE Embedded Systems Letters (ESL), ISSN: 1943-0663, IEEE 2016.
- ACM Transactions on Database Systems (TODS), ISSN: 0362-5915, EISSN: 1557-4644 (5-Yr. IF: 1.47), ACM 2016.
- The 9th International Workshop on Privacy and Anonymity in the Information Society (PAIS'16), 15 March 2016, Bordeaux, France.
- International Journal of Information Security (IJIS). ISSN: 1615-5262, e-ISSN: 1615-5270 (5-Yr. IF: 0.963), Springer-Verlag Berlin Heidelberg 2016.
- International Journal of Network Security (IJNS), ISSN 1816-353X, e-ISSN 1816-3548, 2016.

2015

- ACM Computing Surveys. ISSN: 0360-0300, e-ISSN: 1557-7341 (5-Yr IF: 5.949), ACM 2015.
- The VLDB Journal - The International Journal on Very Large Data Bases. ISSN: 1066-8888, e-ISSN: 0949-877X (5-Yr. IF: 2.26), Springer Berlin Heidelberg, 2015.
- IEEE Transactions on Services Computing (TSC) - SI on Security and Dependability of Cloud Systems and Services, ISSN: 1939-1374, IEEE 2015.
- IEEE Internet of Things Journal (IoT-J), ISSN: 2327-4662, IEEE 2015.
- Journal of Systems and Software (JSS), Elsevier, ISSN: 0164-1212, (5-Yr IF: 1.322), 2015.
- 24th ACM International Conference on Information and Knowledge Management (CIKM 2015), Melbourne, Australia, October 19-23, 2015. Proc. ACM 2015.
- ACM Transactions on Database Systems (TODS), ISSN: 0362-5915, EISSN: 1557-4644 (5-Yr. IF: 1.47), ACM 2015.
- Computer Networks. International Journal of Computer and Telecommunications Networking, ISSN: 1389-1286 (5-Year IF: 1.871), Elsevier 2015.
- Security and Communication Networks Journal - John Wiley & Sons, Ltd., Online ISSN: 1939-0122, (IF: 0.433), 2015.
- Computers & Security Journal - The International Source of Innovation for the Information Security and IT Audit Professional, Elsevier, ISSN: 0167-4048, (5-Yr IF: 1.488), 2015.
- IEEE 9th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC-15) Politecnico di Torino, Turin, Italy, September 23-25, 2015. Proc. IEEE 2015.
- Future Generation Computer Systems (FGCS) - International Journal of Grid Computing and eScience, Elsevier, ISSN: 0167-739X, (5-Yr IF: 2.459), 2015.
- 29th IEEE International Parallel and Distributed Processing Symposium (IPDPS), May 25-29, 2015 Hyderabad International Convention Centre Hyderabad, INDIA. Proc. IEEE-CS 2015.

2014

- IEEE Internet of Things Journal (IoT-J), ISSN: 2327-4662, IEEE 2014.
- Computer Networks. International Journal of Computer and Telecommunications Networking, ISSN: 1389-1286 (5-Year IF: 1.871), Elsevier 2014.
- 16th International Conference on Information and Communications Security (ICICS 2014), Hong Kong, December 16-17, 2014. Proc. Springer-Verlag LNCS 2014.
- IEEE International Symposium on Circuits and Systems (ISCAS 2015), Lisbon, Portugal, May 24-27, 2015. Proc. IEEE 2015.

- IEEE's Transactions on Emerging Topics in Computing (TETC), ISSN: 2168-6750 (Print). IEEE Computer Society 2014.
- PROOFS: Security Proofs for Embedded Systems, Busan, Korea, September 27, 2014. LNCS post-proceeding, Springer Verlag 2014.
- 2014 IEEE Symposium on Intelligent Embedded Systems (IES'14). Orlando, Florida, December 9–12, 2014.
- Journal of Information Systems (IS). Databases: Their Creation, Management and Utilization. Elsevier, ISSN: 0306-4379, (5-Yr IF: 1.838), 2014.
- The IEEE/ACM International Conference on Computer-Aided Design, ICCAD'14, San Jose, CA, USA, November 3-6, 2014.
- International Journal of Network Security (IJNS), ISSN: 1816-353X (Print), ISSN: 1816-3548 (Online), 2014.
- International Journal of Communication Systems (IJCS), Wiley, Online ISSN: 1099-1131 (IF: 0.712), 2014.
- 25th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2014), Zurich, Switzerland, June 18–20, 2014. Proc. IEEE.
- 19th Australasian Conference on Information Security and Privacy (ACISP 2014). Wollongong, Australia, July 7–9, 2014. Proc. Springer.
- Future Generation Computer Systems (FGCS) - International Journal of Grid Computing and eScience, Elsevier, ISSN: 0167-739X, (5-Yr IF: 2.033), 2014.
- Journal of Information Security and Applications (JISA), Elsevier, ISSN: 2214-2126, 2014.
- Financial Cryptography and Data Security - 18th International Conference, FC 2014, Barbados, March 3–7, 2014, Proc. Springer 2014.
- Journal of Systems Architecture (JSA), Elsevier, ISSN: 1383-7621, (5-Yr IF: 0.765), 2014.
- Int'l Journal of Network Security (IJNS), ISSN: 1816-353X, e-ISSN: 1816-3548, 2014.
- Design, Automation and Test in Europe, DATE 2014, Dresden, Germany, March 24-28, 2014. EDAA 2014.

2013

- ACM Transactions on the Web (TWEB), ISSN: 1559-1131, e-ISSN: 1559-114X, (5-Yr IF: 0.871), 2013.
- Computing Journal, Springer, ISSN: 0010-485X, e-ISSN: 1436-5057, 2013.
- Journal of Systems and Software (JSS), Elsevier, ISSN: 0164-1212, (5-Yr IF: 1.322), 2013.
- The 6th International Conference on Security of Information and Networks, (SIN'13). Nov. 26-28, 2013, Aksaray, Turkey. ACM 2013.
- International Workshop on Security Proofs for Embedded Systems (PROOFS 2013), Santa Barbara, CA, USA, August 24, 2013.
- IEEE Transactions on Dependable and Secure Computing (TDSC), ISSN: 1545-5971 (IF: 2.093), 2013.
- Computer Networks. The International Journal of Computer and Telecommunications Networking. Elsevier, ISSN: 1389-1286 (5-Year IF: 1.520), 2013.
- 42nd International Conference on Parallel Processing (ICPP-2013), October 1-4, 2013 Ecole Normale Superieure de Lyon, Lyon, France.
- 14th Italian Conference on Theoretical Computer Science (ICTCS 2013), September 9-11, 2013 - Palermo, Italy.
- 16th IEEE Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT 2013), October 2-4, 2013. New York City, NY, USA.
- 4th International Conference on Intelligent Control and Information Processing (ICICIP 2013), June 9-11, 2013, Beijing, China.
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2013), June 2-3, 2013, Austin, TX, USA. IEEE 2013.

- 7th ACM/IEEE International Symposium on Networks-on-Chip (NOCS 2013), Tempe, Arizona, USA, April 21-24, 2013. IEEE-CS 2013.
- IEEE International Symposium on Circuits and Systems (ISCAS 2013), Beijing, China, May 19-23, 2013. IEEE 2013
- Design, Automation and Test in Europe, DATE 2013, Grenoble, France, March 18-22, 2013. EDAA 2013

2012

- International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE 2012). November 2-3, 2012, Indian Institute of Technology Madras, Chennai, India
- 9th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2012), Leuven, Belgium, 9 September, 2012.
- 3rd International Workshop on Quality in Web Engineering (QWE'12), Berlin, Germany, 23 July 2012. Co-located with the 12th International Conference on Web Engineering (ICWE).
- International Workshop on the Arithmetic of Finite Fields (WAIFI 2012), Bochum, Germany. July 16-19 2012, Springer, LNCS.
- 25th IEEE Computer Security Foundations Symposium, June 25–27, 2012. Harvard University, Cambridge, MA, USA.
- Journal of Systems and Software (JSS), Elsevier, ISSN: 0164-1212 (5-Year IF: 1.322), (February 2012).
- HOST-2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2012), June 3-4, Moscone Center, San Francisco, CA. IEEE Computer Society.
- IEEE Systems Journal - Special Issue on Security and Privacy in Complex Systems. IEEE, ISSN: 1932-8184 (5-Yr IF: 0.92), 2012.
- The 18th International Symposium on High Performance Computer Architecture (HPCA 2012), February 25-29, 2012, New Orleans, Louisiana, USA. IEEE Computer Society.

2011

- 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP 2012), 15–17 February 2012, Garching, Germany. IEEE Computer Society. (External Reviewer - September 2011).
- International Journal of Network Security (IJNS), ISSN 1816-353X [Print], ISSN 1816-3548 [Online], August 2011.
- Journal of Systems and Software (JSS), Elsevier, ISSN: 0164-1212 (5-Year IF: 1.322), July 2011.
- The 14th Information Security Conference (ISC 2011), October 26-29 Xi'an, China (Springer-LNCS).
- 19th IFIP/IEEE International Conference on Very Large Scale Integration VLSI-SoC October 3-5, 2011, Hong Kong, China. External reviewer.
- 13th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), September 25-28, Nara, Japan (Springer-LNCS).
- 9th IEEE Symposium on Application Specific Processors (SASP 2011) June 5-6, 2011, San Diego, CA, USA.
- Proceedings of the VLDB Endowment (PVLDB), ISSN: 2150-8097, March 2011. External reviewer.
- The Computer Journal, Oxford University Press, Online ISSN: 1460-2067, Print ISSN: 0010-4620 (5-Yr IF: 0.954), March 2011.
- Sensors–Open Access Journal, ISSN 1424-8220; CODEN: SENSC9 (February 2011).
- 4th International Workshop on Privacy and Anonymity in the Information Society (PAIS 2011), co-located with EDBT/ICDT, ACM.
- IEEE Transactions on Parallel and Distributed Systems (TPDS), Special Issue on High-Performance Computing with Accelerators, IEEE, ISSN: 1045-9219 (5-Yr IF: 1.4)), January 2011.
- 48th Design Automation Conference (DAC-48, 2011), secondary reviewer.
- IEEE Conference on Design Automation & Test in Europe (DATE 2011). Track A6 - Secure, Dependable and Adaptive Systems. Track D9 - Architectural and Microarchitectural Design.

- 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2011).

2005 – 2010

- Twelfth International Conference on Information and Communications Security (ICISC 2010), Springer LNCS.
- Workshop on Privacy in the Electronic Society (WPES 2010), ACM.
- Second IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2010), IEEE-CS.
- The 30th International Conference on Distributed Computing Systems (ICDCS 2010), IEEE.
- 14th International Conference Financial Cryptography and Data Security (FC 2010), Springer LNCS.
- 43rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO-43, 2010), secondary reviewer.
- International Journal of Network Security (IJNS 2011, IJNS 2010, IJNS 2009, IJNS 2006).
- IEEE Transactions on Industrial Informatics (TII). IEEE, ISSN: 1551-3203 (5-Yr IF: 5.165), 2010.
- ACM Conference on Computer and Security Conference (CCS 2009, CCS 2008).
- The ACM Cloud Computing Security Workshop (CCSW 2009).
- Workshop on Cryptographic Hardware and Embedded Systems (CHES 2009, CHES 2007, CHES 2005, CHES 2004), Springer LNCS.
- Annual Computer Security Applications Conference (ACSAC 2009), ACM.
- IEEE International Conference on Communications (ICC 2009).
- ACM Transactions on Information and System Security (TISSEC 2009).
- IEEE Transaction on Computer (TOC). IEEE, ISSN: 0018-9340 (5-Yr IF: 1.379), 2008.
- Journal of Systems and Software (JSS), ISSN: 0164-1212 (5-Year IF: 1.322), 2008.
- International Workshop on the Arithmetic of Finite Fields (WAIFI 2008), Springer LNCS.
- IEEE/ACM International Conference on Design Automation and Test in Europe (DATE 2006).
- IEEE Transaction on Computer (TOC). IEEE, ISSN: 0018-9340 (5-Yr IF: 1.379), 2005.

Elenco completo delle pubblicazioni e indici bibliometrici

LISTA DELLE PUBBLICAZIONI

INDICI BIBLIOMETRICI

Google Scholar [url: http://scholar.google.com/citations?user=Rlp-N_gAAAAJ]
2006 – 9 Gennaio 2023 Citazioni: 2745 h-index: 29 i10-index: 74
2017 – 9 Gennaio 2023 Citazioni: 1273 h-index: 19 i10-index: 40

Elsevier Scopus – Author ID: 16643986100 [url: http://www.scopus.com/authid/detail.url?authorId=16643986100]
2006 – 9 Gennaio 2023 Citazioni: 1284 h-index: 20 Num. di pubblicazioni in *Scopus database*: 122

Open Researcher & Contributor ID (ORCID): 0000-0002-3812-5429 [url: http://orcid.org/0000-0002-3812-5429]

RIVISTE SCIENTIFICHE INTERNAZIONALI CON COMITATO DI REVISIONE

JR.29. Alessandro Barenghi, Gioele Falcetti and **Gerardo Pelosi**, "Locating Side Channel Leakage in Time through Matched Filters". Cryptography Journal. Cryptography 2022, 6(2), 26. MDPI 2022. Open Access. ISSN: 2410-387X. (DOI: https://doi.org/10.3390/cryptography6020026)

JR.28. Alessandro Barenghi, Diego Carrera, Silvia Mella, Andrea Pace, **Gerardo Pelosi**, and Ruggero Susella. "Profiled Side Channel Attacks against the RSA Cryptosystem using Neural Networks."
Journal of Information Security and Applications. Vol. 66, May 2022. Article No. 103122. ISSN: 2214-2134. E-ISSN: 2214-2126. Elsevier.
(DOI: https://doi.org/10.1016/j.jisa.2022.103122

JR.27. Nicholas Mainardi, Alessandro Barenghi and **Gerardo Pelosi**, "Privacy-aware Character Pattern Matching over Outsourced Encrypted Data." ACM Digital Threats: Research and Practice (DTRAP). Vol. 3, Issue 1, Article No.: 7 (March 2022). pages 1–38. ISSN: 2692-1626. EISSN: 2576-5337. ACM 2022.
(DOI: https://doi.org/10.1145/3462333)

JR.26. Alessandro Barenghi, Luca Breveglieri, Niccoò Izzo and **Gerardo Pelosi**, "Exploring Cortex-M microarchitectural side channel information leakage." IEEE Access. Volume 9. Nov. 2021. Print ISSN: 2169-3536. Online ISSN: 2169-3536. pages 156507-156527. IEEE 2021. Manuscript Number: Access-2021-31164.
(DOI: https://dx.doi.org/10.1109/ACCESS.2021.3124761)

JR.25. Francesco Antognazza, Alessandro Barenghi, and **Gerardo Pelosi**. "Metis: An Integrated Morphing Engine CPU to Protect against Side Channel Attacks." IEEE Access. Volume 9. May. 2021. Print ISSN: 2169-3536. Online ISSN: 2169-3536. pages 69210–69225. IEEE 2021. (DOI: https://dx.doi.org/10.1109/ACCESS.2021.3077977)

JR.24. Alessandro Barenghi, William Fornaciari, **Gerardo Pelosi**, and Davide Zoni. "Scramble Suit: A Profile Differentiation Countermeasure to Prevent Template Attacks". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD). *39(9):1778–1791* September 2020. Print ISSN: 0278-0070. Online ISSN: 1937-4151. IEEE 2020. (DOI:https://dx.doi.org/10.1109/TCAD.2019.2926389)

JR.23. Giovanni Agosta, Alessandro Barenghi, and **Gerardo Pelosi**. "Compiler-based Techniques to Secure Cryptographic Embedded Software against Side Channel Attacks". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD). *39(8):1550–1554* August 2020. Print ISSN: 0278-0070. Online ISSN: 1937-4151. IEEE 2020. (DOI: https://dx.doi.org/10.1109/TCAD.2019.2912924)

JR.22. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi** and Paolo Santini. "A Finite Regime Analysis of Information Set Decoding Algorithms". Algorithms journal 2019, Vol. 12, issue 10, 209, pages 1–35. ISSN: 1999-4893. MDPI AG, 2019. Basel, Switzerland. Special Issue "Coding Theory and Its Application", G. Liva, A. Graell i Amat, A. Wachter-Zeh (editors). Open Access (release date Oct. 25th, 2019). (DOI: https://doi.org/10.3390/a12100209)

JR.21. Nicholas Mainardi, Alessandro Barenghi and **Gerardo Pelosi**. "Plaintext recovery attacks against linearly decryptable fully homomorphic encryption schemes". In *Computers & Security Journal (CoSe)*, Volume 87, 17 pages, November 2019. ISSN: 0167-4048 (print). Elsevier 2019.
(DOI: https://doi.org/10.1016/j.cose.2019.101587)

JR.20. 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)

JR.19. 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)

JR.18. 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)

JR.17. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Enforcing authorizations while protecting access confidentiality". *Journal of Computer Security (JCS)*, vol. 26, no. 2, pp. 143–175. January 2018. ISSN: 0926-227X (Print), 1875-8924 (Online).
(DOI: http://dx.doi.org/10.3233/JCS-171004)

JR.16. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Three-server swapping for access confidentiality". *IEEE Transactions on Cloud Computing (TCC)*, Vol. 6, Issue 2, (Issue date: April-June 2018), pp. 492–505, June 2018. Print ISSN: 2168-7161.
(DOI: http://dx.doi.org/10.1109/TCC.2015.2449993)

JR.15. 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)

JR.14. 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)

JR.13. 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)

JR.12. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Shuffle Index: Efficient and Private Access to Outsourced Data". *ACM Transactions on Storage (TOS)*, 11(4):1–54, Article 19, October 2015. ISSN: 1553-3077 (Print), 1553-3093 (Online). (DOI: http://dx.doi.org/10.1145/2747878)

JR.11. 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)

JR.10. 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)

JR.9. 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)

JR.8. 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)

JR.7. 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)

JR.6. 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)

JR.5. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Supporting Concurrency and Multiple Indexes in Private Access to Outsourced Data". *Journal of Computer Security (JCS)*, 21(3):425–461, July 2013. ISSN: 0926-227X (Print), 1875-8924 (Online). (DOI: http://dx.doi.org/10.3233/JCS-130468)

JR.4. Giovanni Agosta, Francesco Bruschi, **Gerardo Pelosi**, and Donatella Sciuto. "A Transform-Parametric Approach to Boolean Matching". *IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 28(6):805–817, June 2009. ISSN: 0278-0070. (DOI: http://dx.doi.org/10.1109/TCAD.2009.2016547)

JR.3. Guido Bertoni, Luca Breveglieri, Liqun Chen, Pasqualina Fragneto, Keith A. Harrison, and **Gerardo Pelosi**. "A Pairing SW Implementation for Smart-Cards". *Journal of Systems and Software (JSS)*, 81(7):1240–1247, July 2008. ISSN: 0164-1212. (DOI: http://dx.doi.org/10.1016/j.jss.2007.09.022)

JR.2. Guido M. Bertoni, Luca Breveglieri, Pasqualina Fragneto, and **Gerardo Pelosi**. "Parallel Hardware Architectures for the Cryptographic Tate Pairing". *International Journal of Network Security (JNS)*, 7(1):31–37, July 2008. ISSN: 1816-353X (Print), 1816-3548 (Online).

JR.1. Giovanni Agosta, Luca Breveglieri, **Gerardo Pelosi**, and Martino Sykora. "Programming Highly Parallel Reconfigurable Architectures for Symmetric and Asymmetric Cryptographic Applications". *Journal of Computers (JoC)*, 2(9):50–59, September 2007. ISSN: 1796-203X. (DOI: http://dx.doi.org/10.4304/jcp.2.9.50-59)

CONTRIBUTI EDITORIALI

ED.6. 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: https://dl.acm.org/doi/proceedings/10.1145/3304080)

ED.5. 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.4. 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.3. 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.2. **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)

ED.1. Israel Koren, **Gerardo Pelosi**. (Editors). Proceedings of the HiPEAC Workshop on *Cryptography and Security in Computing Systems (CS2 '14)*. Vienna, Austria, January 20, 2014. ACM New York, NY, USA. 2014.
ISBN 978-1-4503-2484-7 (DOI: http://dl.acm.org/citation.cfm?id=2556315)

CONTRIBUTI IN LIBRI INTERNAZIONALI CON COMITATO DI REVISIONE

IB.12. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi** and Paolo Santini. "Analysis of In-Place Randomized Bit-Flipping Decoders for the Design of LDPC and MDPC Code-based Cryptosystems." In E-Business and Telecommunications - 17th International Conference, ICETE 2020, Online Event, July 8–10, 2020, Revised Selected Papers. Mohammad S. Obaidat and Jalel Ben-Othman (Eds) Series: Communications in Computer and Information Science (CCIS), Volume 1484, 2021. Copyright holder: Springer Nature Switzerland AG 2021). Publisher name: Springer, Cham. Print ISBN: 978-3-030-90427-2, Online ISBN: 978-3-030-90428-9. Series Print ISSN: 1865-0929, Series Online ISSN: 1865-0937. DOI: https://doi.org/10.1007/978-3-030-90428-9_7

IB.11. Ariel Oleksiak, Michal Kierzynka, Wojciech Piatek, Micha vor dem Berge, Wolfgang Christmann, Stefan Krupop, Mario Porrmann, Jens Hagemeyer, René Griessl, Meysam Peykanu, Lennart Tigges, Sven Rosinger, Daniel Schlitt, Christian Pieper, Udo Janssen, Holm Rauchfuss, Giovanni Agosta, Alessandro Barenghi, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Joao Pita Costa, Mariano Cecowski, Robert Plestenjak, Justin Cinkelj, Loïc Cudennec, Thierry Goubier, Jean-Marc Philippe, Chris Adeniyi-Jones, Javier Setoain, Luca Ceva. "M2DC – A Novel Heterogeneous Hyperscale Microserver Platform". In Christoforos Kachris, Babak Falsafi, Dimitrios Soudris (Eds.), *Hardware Accelerators in Data Centers*, pages 109–128. Springer International Publishing, 2019 (First online: 22 August 2018). ISBN: 978-3-319-92791-6 (Print) 978-3-319-92792-3 (Online).
(DOI: https://doi.org/10.1007/978-3-319-92792-3_6)

IB.10. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Access Privacy in the Cloud". In Indrakshi Ray and Indrajit Ray and Pierangela Samarati, editors, *From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of his 70th Birthday*, pages 186-205 (20 pages). Lecture Notes in Computer Science, vol. 11170 (Lect. Notes ComputerFestschrift). Also part of the Security and Cryptology book sub series. November 2018, Springer International Publishing, Switzerland.
Copyright 2018, Springer Nature Switzerland AG. ISBN: 978-3-030-04833-4 (Print) 978-3-030-04834-1 (Online).
Series Print ISSN 0302-9743. Series Online ISSN 1611-3349.
(DOI: http://dx.doi.org/10.1007/978-3-030-04834-1_10) [First on line, Nov. 30th, 2018]

IB.9. Giovanni Agosta, Alessandro Barenghi, Tomasz Ciesielczyk, Rahul Dutta, William Fornaciari, Thierry Goubier, Jens Hagemeyer, Lars Kosmann, Nicholas Mainardi, Ariel Oleksiak, **Gerardo Pelosi**, Wojciech Piatek, Christian Pieper, Mario Porrmann, Daniel Schlitt and Michele Zanella. Chapter title: "The M2DC Approach towards Resource-efficient Computing". In Alessandra Bagnato and Ricardo Couceiro and Juliana Monteiro and Dijana Petrovska-Delacrétaz and Arminda Lopes and Élvio Gouveia (Editors). Opportunities and Challenges for European Projects. pp. 150–176. ScitePress. January 2017. ISBN: 978-989-758-361-2 (DOI: https://doi.org/10.5220/0008862601500017, URL: https://www.scitepress.org/ProceedingsDetails.aspx?ID=EeN757UbCeU=&t=1)

IB.8. 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.7. 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 47–59. 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_3)

IB.6. 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).
(URL: http://www.crcpress.com/product/isbn/9781482228892#)

IB.5. Alessandro Barenghi, Luca Breveglieri, Fabrizio De Santis, Filippo Melzani, Andrea Palomba, and **Gerardo Pelosi**. "Design Time Engineering of Side Channel Resistant Cipher Implementations". In Atilla Elçi, Josef Pieprzyk, Alexander G. Chefranov, Mehmet A. Orgun, Huaxiong Wang, and Rajan Shankaran, editors, *Theory and Practice of Cryptography Solutions for Secure Information Systems, Advances in Information Security, Privacy, and Ethics (AISPE)*, pages 133–157. IGI Global, Hershey, PA, USA, February 2013. ISBN: 978-1-466-64030-6 (Print), 978-1-466-64031-3 (Online). (DOI: http://dx.doi.org/10.4018/978-1-4666-4030-6.ch006)

IB.4. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Mauro Pelliccioli, and **Gerardo Pelosi**. "Injection Technologies for Fault Attacks on Microprocessors". 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.3. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Selective Exchange of Confidential Data in the Outsourcing Scenario". In Jan Camenisch, Simone Fischer-Hübner, and Kai Rannenberg, editors, *Privacy and Identity Management for Life*, pages 181–198. Springer, Berlin, Heidelberg, October 2011. ISBN: 978-3-642-20316-9 (Print), 978-3-642-20317-6 (Online).
(DOI: http://dx.doi.org/10.1007/978-3-642-20317-6)

IB.2. **Gerardo Pelosi**. "Secure Audit Logs". In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security* (2nd Ed.), pages 1097–1099. Springer, New York, NY, USA, January 2011. ISBN: 978-1-4419-5905-8 (Print), 978-1-4419-5906-5 (Online), 978-1-4419-5907-2 (Bundle).
(DOI: http://dx.doi.org/10.1007/978-1-4419-5906-5)

IB.1. **Gerardo Pelosi**. "Secure Index". In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security* (2nd Ed.), pages 1116–1119. Springer, New York, NY, USA, January 2011. ISBN: 978-1-4419-5905-8 (Print), 978-1-4419-5906-5 (Online), 978-1-4419-5907-2 (Bundle).
(DOI: http://dx.doi.org/10.1007/978-1-4419-5906-5)

CONFERENZE INTERNAZIONALI CON COMITATO DI REVISIONE

IC.78. Francesco Antognazza, Alessandro Barenghi, **Gerardo Pelosi**, ad Ruggero Susella, "An Efficient Unified Architecture for Polynomial Multiplications in Lattice-based Cryptoschemes". In *Proceedings of the 9th International Conference on Information Systems Security and Privacy* (ICISSP 2023), February 22–24, 2023, Lisbon, Portugal. SciTePress 2023. [to appear]

IC.77. Francesco Antognazza, Alessandro Barenghi, **Gerardo Pelosi**, ad Ruggero Susella, "A Flexible ASIC-oriented Design for a Full NTRU Accelerator". In *Proceedings of the 28th Asia and South Pacific Design Automation Conference* (ASPDAC '23), January 16–19, 2023, Tokyo, Japan. ACM, New York, NY, USA, 7 pages. (DOI: https://doi.org/10.1145/3566097.3567916) [to appear]

IC.76. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi** and Paolo Santini. "Performance bounds for QC-MDPC codes decoders." In Antonia Wachter-Zeh, Hannes Bartz, Gialuigi Riva (Ed.s), *Proceedings of the International Workshop on Code-Based Cryptography (CBCrypto 2021), Munich, Germany, June 21–22, 2021, Revised Selected Papers*, volume 13150 of Lecture Notes in Computer Science, pages 95–122, Springer International Publishing March 2022 (Copyright holder: Springer Nature Switzerland AG 2022). ISBN: 978-3-030-98364-2 (Print). 978-3-030-98365-9 (Online). Also part of the Security and Cryptology book sub series (LNCS, volume 13150) Series Print ISSN: 0302-9743. Series Online ISSN: 1611-3349. (DOI: https://doi.org/10.1007/978-3-030-98365-9_6)

IC.75. Alessandro Barenghi, Diego Carrera, Silvia Mella, Andrea Pace, **Gerardo Pelosi**, and Ruggero Susella. "Profiled Attacks against the Elliptic Curve Scalar Point Multiplication." In Min Yang, Chao Chen, and Yang Liu, editors, *Network and System Security - 15th International Conference, NSS 2021, Tianjin, China, October 23, 2021, Proceedings*, volume 13041 of Lecture Notes in Computer Science, pages 238-257, Springer International Publishing, October 2021. Springer Nature Switzerland AG. ISBN: 978-3-030-92707-3 (Print) 978-3-030-92708-0 (Online), Series ISSN 0302-9743, Series E-ISSN 1611-3349. (DOI: https://doi.org/10.1007/978-3-030-92708-0_15)

IC.74. Simone Perriello, Alessandro Barenghi and **Gerardo Pelosi**, "A Complete Quantum Circuit to Solve the Information Set Decoding Problem." In Proc. of the *IEEE International Conference on Quantum Computing and Engineering, QCE 2021, Broomfield, CO, USA, October 18-22, 2021* (Fully virtual event). IEEE Computer Society 2021. Electronic ISBN:978-1-6654-1691-7. Print on Demand(PoD) ISBN:978-1-6654-1692-4. IEEE 2021. (DOI: https://doi.org/10.1109/QCE52317.2021.00056)

IC.73. Simone Perriello, Alessandro Barenghi and **Gerardo Pelosi**, "A Quantum Circuit to Speed-up the Cryptanalysis of Code-based Cryptosystems." International Workshop on Post-quantum Cryptography for Secure Communications (PQC-SC). In Joaquin Garcia-Alfaro and Radha Poovendran and Hervé Debar and Moti Yung (Eds.) Proceedings Part II of the *17th EAI International Conference on Security and Privacy in Communication Networks - SecureComm 2021, Virtual event, September 6-9, 2021*, pp. 458-474. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST) vol. 399. Springer, Cham. Print ISBN: 978-3-030-90021-2. eBook ISBN: 978-3-030-90022-9. Series ISSN: 1867-8211. Springer International Publishing 2021. (DOI: https://doi.org/10.1007/978-3-030-90022-9_25)

IC.72. Alessandro Barenghi, Matteo Brevi, William Fornaciari, **Gerardo Pelosi** and Davide Zoni. "Integrating Side Channel Security in the FPGA Hardware Design Flow." In *Proceedings of the 11th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) 2020, Lugano, Switzerland, April 1–3, 2020, Revised Selected Papers*, Guido Bertoni and Francesco Regazzoni (editors), Volume 12244 of Lecture Notes in Computer Science, pages 275-290, Springer, Cham 2021. ISBN: 978-3-030-68772-4 (Print) 978-3-030-68773-1 (Online). Copyright: Springer Nature Switzerland AG 2021. Also part of the Security and Cryptology book sub series. Series Print ISSN: 0302-9743. Series Online ISSN: 1611-3349 (DOI: https://doi.org/10.1007/978-3-030-68773-1)

IC.71. Nicholas Mainardi, Davide Sampietro, Alessandro Barenghi and **Gerardo Pelosi**, "Efficient Oblivious Substring Search via Architectural Support". Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC 2020), Austin, Texas, USA. December 07–11, 2020. ACM 2020, New York, NY, USA. ISBN: 978-1-4503-8858-0/20/12 (DOI: https://doi.org/10.1145/3427228.3427296)

IC.70. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi**, and Paolo Santini, "A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems". In P. Samarati, S. De Capitani Di Vimercati, M. Obaidat, J. Ben-Othman (eds), *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - Volume 3: SECRYPT, Lieusaint - Paris, France, July 8-10, 2020*, pp. 238-249. SciTePress 2020. ISBN 978-989-758-446-6. (DOI: https://doi.org/10.5220/0009891702380249) **Best paper award**

IC.69. Alessandro Barenghi and **Gerardo Pelosi**, "A Comprehensive Analysis of Constant Time Polynomial Inversion for Post-quantum Cryptosystems". In M. Palesi, G. Palermo, C. Graves, and E. Arima (editors), *Proceedings of the 17th*

ACM International Conference on Computing Frontiers (CF '20), May 11-13, 2020, Catania, Italy. ACM, New York, NY, USA, 8 pages. ISBN: 978-1-4503-7956-4/20/05 (DOI: http://dx.doi.org/10.1145/3387902.3397224)

IC.68. Alessandro Barenghi and **Gerardo Pelosi**, "Constant Weight Strings in Constant Time: a Building Block for Code-based Post-quantum Cryptosystems". In M. Palesi, G. Palermo, C. Graves, and E. Arima (editors), *Proceedings of the 17th ACM International Conference on Computing Frontiers (CF '20), May 11-13, 2020, Catania, Italy*. ACM, New York, NY, USA, 8 pages. ISBN: 978-1-4503-7956-4/20/05 (DOI: http://dx.doi.org/10.1145/3387902.3392630)
The related software implementation is permanently available at https://doi.org/10.5281/zenodo.3747545 and received the ACM Artifact Evaluated badges: **Functional, Reusable, Available and Result Reproduced**.

IC.67. Alessandro Barenghi, William Fornaciari, Andrea Galimberti, **Gerardo Pelosi**, and Davide Zoni. "Evaluating the Trade-offs in the Hardware Design of the LEDAcrypt Encryption Functions." In Danilo De Marchi, Teresa Serrano Gotarredona,and Roland Thewes, editors, Proceedings of the 26th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2019, Genova, Italy, November 27-29, 2019. New York, NY, USA, November 2019.
Electronic ISBN: 978-1-7281-0996-1. Print on Demand(PoD) ISBN: 978-1-7281-0997-8.
(DOI: http://dx.doi.org/10.1109/ICECS46596.2019.8964882)

IC.66. Nicholas Mainardi, Alessandro Barenghi, **Gerardo Pelosi**,"Privacy Preserving Substring Search Protocol with Polylogarithmic Communication Cost." Proceedings of the the 35th Annual Computer Security Applications Conference (ACSAC 2019), San Juan, Puerto Rico, USA. December 9-13, 2019. ACM 2019. ISBN: 978-1-4503-7628-0/19/12 (DOI: http://dx.doi.org/10.1145/3359789.3359842).
The related software implementation is permanently available at https://dx.doi.org/10.5281/zenodo.3384814 and received the ACM Artifact Evaluated badge at the **reusable** level.

IC.65. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi** and Paolo Santini. "LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate". In Marco Baldi, Edoardo Persichetti, Paolo Santini. *Proceedings of the 7th International Workshop, CBC 2019, Darmstadt, Germany, May 18–19, 2019, Revised Selected Papers*, volume 11666 of Lecture Notes in Computer Science, pages 11–43, Springer International Publishing 2019 (Copyright holder: Springer Nature Switzerland AG 2019). ISBN: 978-3-030-25921-1 (Print). 978-3-030-25922-8 (Online). Also part of the Security and Cryptology book sub series (LNCS, volume 11666) Series Print ISSN: 0302-9743. Series Online ISSN: 1611-3349. (DOI: https://doi.org/10.1007/978-3-030-25922-8_2)

IC.64. Niccolò Izzo, Alessandro Barenghi, Luca Breveglieri, **Gerardo Pelosi**, Paolo Amato. "A Secure and Authenticated Host to Memory Communication Interface". In Francesca Palumbo, Michela Becchi, Martin Schulz and Kento Sato (editors), *Proceedings of the 16th ACM International Conference on Computing Frontiers (CF'19), Alghero, Sardinia, Italy, April 30 - May 2, 2019*, pages 386-391, New York, NY, USA, May 2019. ACM. ISBN: 978-1-4503-6685-4/19/05. (DOI: http://dx.doi.org/10.1145/3310273.3323401)

IC.63. 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.62. 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.61. 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.60. 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.59. 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.58. 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.57. 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.56. 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.55. Sabrina De Capitani Di Vimercati, Sara Foresti, Riccardo Moretti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati, "A dynamic tree-based data structure for access privacy". In Proceedings of the *8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2016), 12-15 December 2016, Luxembourg City, Grand Duchy of Luxembourg*, pages 187:1-187:8. IEEE Computer Society 2017. ISBN: 978-1-5090-1446-0 (Print on Demand), 978-1-5090-1445-3 (Electronic). ISSN: 2330-2194, ISSN: 2330-2186 (Electronic).
(DOI: http://dx.doi.org/10.1109/CloudCom.2016.0068)

IC.54. 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.53. 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.52. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Access Control for the Shuffle Index". In proceedings of *30th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec 2016), Trento, Italy, July 18-20, 2016*. Silvio Ranise and Vipin Swarup (editors), Volume 9766 of Lecture Notes in Computer Science, pages 130-147, Springer International Publishing 2016. ISBN: 978-3-319-41482-9 (Print) 978-3-319-41483-6 (Online). Series ISSN: 0302-9743
(DOI: http://dx.doi.org/10.1007/978-3-319-41483-6_10)

IC.51. 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.50. Giovanni Agosta, Alessandro Barenghi, **Gerardo Pelosi**, "Automated Instantiation of Side-Channel Attacks Countermeasures for Software Cipher Implementations". In Gianluca Palermo, John Feo, Antonino Tumeo and Hubertus Franke (editors), *Proceedings of the 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.49. 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, 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 January 2016. ISSN: 10716572, ISBN: 978-147998691-0. (DOI http://dx.doi.org/10.1109/CCST.2015.7389663)

IC.48. Alessandro Barenghi, Alessandro Di Federico, **Gerardo Pelosi**, and Stefano Sanfilippo. "Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-proof?". In *Computer Security - ESORICS 2015 - Proceedings of the 20th European Symposium on Research in Computer Security, Vienna, Austria – September 21-25, 2015 - Part I*, Günther Pernul, Peter Y. A. Ryan, Edgar Weippl (editors), Volume 9326 of Lecture Notes in Computer Science, pages 429–446, Switzerland, September 2015. 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.47. 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 52th Annual Design Automation Conference, DAC'15*, San Francisco, CA, USA, June 7–11, 2015, pages 33:1–33:6, 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.46. Giovanni Agosta, Alessandro Barenghi, **Gerardo Pelosi**, and Michele Scandale. "Towards Transparently Tackling Functionality and Performance Issues Across Different OpenCL Platforms". In Shuichi Ichikawa and Tomoaki Tsumura (editors), *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.45. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Protecting access confidentiality with data distribution and swapping". In Xindong Wu, Hai Jin, Manish Parashar, and Laurence T. Yang (editors), *Proceedings of the 4th IEEE International Conference on Big Data and Cloud Computing (BDCloud 2014)*, Sydney, Australia - December 3–5, 2014, pages 167–174, Piscataway, NJ, USA, December 2014. IEEE Computer Society. ISBN-13: 978-1-4799-6719-3 (Print).
(DOI: http://dx.doi.org/10.1109/BDCloud.2014.59)

IC.44. Alessio Antonini, Alessandro Barenghi, **Gerardo Pelosi**, and Saman Zonouz, "Security Challenges in Building Automation and SCADA", In Fabio Garza, Gordon Thomas, Daniel A. Pritchard (editors), *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.43. Giovanni Agosta, Alessandro Barenghi, and **Gerardo Pelosi**, "Securing Software Cryptographic Primitives for Embedded Systems against Side Channel Attacks", In Fabio Garza, Gordon Thomas, Daniel A. Pritchard (editors), *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.2014.6987032)

IC.42. 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. (DOI: http://dx.doi.org/10.1145/2659651.2659709)
Best Paper Award

IC.41. Alessandro Barenghi and **Gerardo Pelosi**. "On the Security of Partially Masked Software Implementations". In M. S. Obaidat, A. Holzinger and P. Samarati, editors, *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). (DOI: http://dx.doi.org/10.5220/0005120504920499)

IC.40. 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.39. 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.38. Giovanni Agosta, Iyad Al Khatib, **Gerardo Pelosi**, and Heikki Teriö. "Security Integration in Medical Device Design: Extension of an Automated Bio-medical Engineering Design Methodology". In Shahram Latifi, editor, *Proceedings of the 11th International Conference on Information Technology: New Generations, ITNG 2014, Las Vegas, Nevada, USA, 7–9 April, 2014*, pages 416–421, Washington, DC, USA, April 2014. IEEE Computer Society.
ISBN: 978-1-4799-3187-3 (Print). (DOI: http://dx.doi.org/10.1109/ITNG.2014.3)

IC.37. Alessio Antonini, Alessandro Barenghi, and **Gerardo Pelosi**. "Security Analysis of Building Automation Networks: Threat Model and Viable Mitigation Techniques". In Dieter Gollmann and Hanne Riis Nielson, editors, *Secure IT Systems - Proceedings of the 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18–21, 2013*, 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.36. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Distributed Shuffling for Preserving Access Confidentiality". In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security - ESORICS 2013 - Proceedings of the 18th European Symposium on Research in Computer Security, Egham, UK, September 9–13, 2013*, volume 8134 of Lecture Notes in Computer Science, pages 628–645, Berlin, Heidelberg, September 2013. Springer-Verlag. ISBN: 978-3-642-40202-9 (Print) 978-3-642-40203-6 (Online),
ISSN: 0302-9743. (DOI: http://dx.doi.org/10.1007/978-3-642-40203-6_35)

IC.35. Giovanni Agosta, Alessandro Barenghi, **Gerardo Pelosi**, and Michele Scandale. "Enhancing Passive Side-Channel Attack Resilience through Schedulability Analysis of Data-Dependency Graphs". In Javier Lopez, Xinyi Huang, and Ravi Sandhu, editors, *Network and System Security. Proceedings of the 7th International Conference, NSS 2013, Madrid, Spain, June 3–4, 2013*, volume 7873 of Lecture Notes in Computer Science, pages 692–698, Berlin, Heidelberg, June 2013. Springer. ISBN: 978-3-642-38630-5 (Print), 978-3-642-38631-2 (Online), ISSN: 0302-9743.
(DOI: http://dx.doi.org/10.1007/978-3-642-38631-2_58)

IC.34. Giovanni Agosta, Alessandro Barenghi, Massimo Maggi, and **Gerardo Pelosi**. "Compiler-Based Side Channel Vulnerability Analysis and Optimized Countermeasures Application". In Yervant Zorian, Donatella Sciuto, and Charles Alpert, editors, *Proceedings of the 50th Annual Design Automation Conference, DAC '13, 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.33. Giovanni Agosta, **Gerardo Pelosi**, and Ettore Speziale. "On Task Assignment in Data Intensive Scalable Computing". In N. Desai and W. Cirne, editors, *Proceedings of the 17th Workshop on Job Scheduling Strategies for Parallel Processing, JSSPP 2013, Boston, Massachusetts, USA, 24 May 2013*, volume 8429 of Lecture Notes in Computer Science, pages 1–20, Berlin, Heidelberg, 2014. Springer-Verlag. ISBN: 978-3-662-43779-7 (Print).
(DOI: http://dx.doi.org/10.1007/978-3-662-43779-7_8)

IC.32. Alessandro Barenghi, **Gerardo Pelosi**, and Fabio Pozzi. "Drop-In Control Flow Hijacking Prevention through Dynamic Library Interception". In Shahram Latifi, editor, *Proceedings of the 10th International Conference on Information Technology: New Generations, ITNG 2013, Las Vegas, Nevada, USA, 15–17 April, 2013*, pages 640–647, Washington, DC, USA, April 2013. IEEE Computer Society. ISBN: 978-0-7695-4967-5 (Print).
(DOI: http://dx.doi.org/10.1109/ITNG.2013.99)

IC.31. Alessandro Barenghi, **Gerardo Pelosi**, and Francesco Regazzoni. "Simulation-Time Security Margin Assessment against Power-Based Side Channel Attacks". In Dimitrios Serpanos and Marilyn Wolf, editors, *Proceedings of the 7th Workshop on Embedded Systems Security (WESS 2012), A Workshop of the Embedded Systems Week (ESWEEK 2012), October 11, 2012, Tampere, Finland, 2012*, New York, NY, USA, October 2012. ACM.
ISBN: 978-1-4503-1286-8/12/10.

IC.30. Alessandro Barenghi, Luca Breveglieri, Mariagrazia Fugini, and **Gerardo Pelosi**. "Smart Meters and Home Gateway Scenarios". In Americo Cicchetti and Cecilia Rossignoli, editors, *Proceedings of itAIS 2012 – IX Conference of the Italian Chapter of AIS Organization change and Information Systems: Working and Living Together in New Ways – Università Cattolica del Sacro Cuore, Rome Campus (Italy), September 28th and 29th, 2012, Roma (RM), September 2012*. ITHUM Srl. ISBN: 978-88-6685-085-4.

IC.29. Giovanni Agosta, Alessandro Barenghi, and **Gerardo Pelosi**. "A Code Morphing Methodology to Automate Power Analysis Countermeasures". In Patrick Groeneveld, Donatella Sciuto, and Soha Hassoun, editors, *Proceedings of the 49th Annual Design Automation Conference 2012, DAC '12, San Francisco, CA, USA, June 3–7, 2012*, pages 77–82, New York, NY, USA, June 2012. ACM. ISBN: 978-1-4503-1199-1.
(DOI: http://dx.doi.org/10.1145/2228360.2228376)

IC.28. Giovanni Agosta, Alessandro Barenghi, Antonio Parata, and **Gerardo Pelosi**. "Automated Security Analysis of Dynamic Web Applications through Symbolic Code Execution". In Shahram Latifi, editor, *Proceedings of the Ninth International Conference on Information Technology: New Generations, ITNG 2012, Las Vegas, Nevada, USA, 16–18 April, 2012*, pages 189–194, Washington, DC, USA, April 2012. IEEE Computer Society. ISBN: 978-1-4673-0798-7 (Print). (DOI: http://dx.doi.org/10.1109/ITNG.2012.167)

IC.27. Giovanni Agosta, Alessandro Barenghi, and **Gerardo Pelosi**. "Exploiting Bit-level Parallelism in GPGPUs: a Case Study on KeeLoq Exhaustive Search Attacks". In Gero Mühl, Jan Richling, and Andreas Herkersdorf, editors, *ARCS Workshops, Proceedings of the 3rd Workshop on Parallel Programming and Run-Time Management Techniques for Many-Core Architectures, PARMA '12, Munich, Germany, 28–29 February, 2012*, volume 200 of Lecture Notes in Informatics (LNI), pages 385–396, Bonn, Germany, February 2012. Gesellschaft für Informatik (GI). ISBN: 978-1-4673-1913-3 (Print), 978-3-88579-294-9 (Online), ISSN: 1617-5468.

IC.26. Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Maria Grazia Fugini, and **Gerardo Pelosi**. "Smart Metering in Power Grids: Application Scenarios and Security". In Syed Islam, editor, *Proceedings of the IEEE PES Innovative Smart Grid Technology Conference (IEEE PES ISGT2011 Asia), November 13–16, 2011, Perth, Australia*, pages 1–8, Piscataway, NJ, USA, November 2011. IEEE. ISBN: 978-1-4577-0873-2 (Print), 978-1-4577-0874-9 (Online), 978-1-4577-0875-6/11. (DOI: http://dx.doi.org/10.1109/ISGT-Asia.2011.6167108)

IC.25. Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, **Gerardo Pelosi**, and Andrea Palomba. "Fault Attack to the Elliptic Curve Digital Signature Algorithm with Multiple Bit Faults". In Mehmet A. Orgun, Atilla Elçi, Oleg B. Makarevich, Sorin A. Huss, Josef Pieprzyk, Lyudmila K. Babenko, Alexander G. Chefranov, and Rajan Shankaran, editors, *Proceedings of the 4th International Conference on Security of Information and Networks, SIN 2011, Sydney, NSW, Australia, November 14–19, 2011*, pages 63–72, New York, NY, USA, November 2011. ACM. ISBN: 978-1-4503-1020-8. (DOI: http://dx.doi.org/10.1145/2070425.2070438)

IC.24. Sabrina De Capitani Di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Supporting Concurrency in Private Data Outsourcing". In Vijay Atluri and Claudia Díaz, editors, *Computer Security - ESORICS 2011 - Proceedings of the 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12–14, 2011*, volume 6879 of Lecture Notes in Computer Science, pages 648–664, Berlin, Heidelberg, September 2011. Springer-Verlag. ISBN: 978-3-642-23821-5 (Print), 978-3-642-23822-2 (Online), ISSN: 0302-9743 (Print), 1611-3349 (Online). (DOI: http://dx.doi.org/10.1007/978-3-642-23822-2_35)

IC.23. Alessandro Barenghi and **Gerardo Pelosi**. "Security and Privacy in Smart Grid Infrastructures". In Franck Morvan, A Min Tjoa, and Roland R. Wagner, editors, *DEXA '11 Proceedings of the 2011 22nd International Workshop on Database and Expert Systems Applications, Toulouse, France, August 29–September 2, 2011*, pages 102–108, Washington, DC, USA, August 2011. IEEE Computer Society. ISBN: 978-1-4577-0982-1 (Print), 978-0-7695-4486-1 (Online), ISSN: 1529-4188. (DOI: http://dx.doi.org/10.1109/DEXA.2011.74)

IC.22. Alessandro Barenghi, **Gerardo Pelosi**, and Yannick Teglia. "Information Leakage Discovery Techniques to Enhance Secure Chip Design". In Claudio Agostino Ardagna and Jianying Zhou, editors, *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - Proceedings of the 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1–3, 2011*, volume 6633 of Lecture Notes in Computer Science, pages 128–143, Berlin, Heidelberg, June 2011. Springer-Verlag. ISBN: 978-3-642-21039-6 (Print), 978-3-642-21040-2 (Online). (DOI: http://dx.doi.org/10.1007/978-3-642-21040-2_9)

IC.21. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Efficient and Private Access to Outsourced Data". In *Proceedings of the 2011 31st International Conference on Distributed Computing Systems, ICDCS 2011, Minneapolis, MN, USA, June 20–24, 2011*, pages 710–719, Washington, DC, USA, June 2011. IEEE Computer Society. ISBN: 978-1-61284-384-1 (Print), 978-0-7695-4364-2 (Online), ISSN: 1063-6927. (DOI: http://dx.doi.org/10.1109/ICDCS.2011.37)

IC.20. Alessandro Barenghi, Luca Breveglieri, Israel Koren, **Gerardo Pelosi**, and Francesco Regazzoni. "Countermeasures against Fault Attacks on Software Implemented AES: Effectiveness and Cost". In *ESWeek '10 Sixth Embedded Systems Week. Proceedings of the 5th Workshop on Embedded Systems Security. WESS' 10, Scottsdale, AZ, USA. October 28, 2010*, pages 7:1–7:10, New York, NY, USA, October 2010. ACM. ISBN: 978-1-4503-0078-0. (DOI: http://dx.doi.org/10.1145/1873548.1873555)

IC.19. Alessandro Barenghi, **Gerardo Pelosi**, and Yannick Teglia. "Improving First Order Differential Power Attacks through Digital Signal Processing". In Oleg B. Makarevich, Atilla Elçi, Mehmet A. Orgun, Sorin A. Huss, Ludmila K. Babenko, Alexander G. Chefranov, and Vijay Varadharajan, editors, *Proceedings of the 3rd International Conference on Security of Information and Networks, SIN 2010, Rostov-on-Don, Russian Federation, September 7–11, 2010*, pages 124–133, New York, NY, USA, September 2010. ACM. ISBN: 978-1-4503-0234-0. (DOI: http://dx.doi.org/10.1145/1854099.1854126)

IC.18. Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, Mauro Pellicioli, and **Gerardo Pelosi**. "Fault Attack on AES with Single-Bit Induced Faults". In *Proceedings of the Sixth International Conference on Information Assurance and Security, IAS 2010, Atlanta, GA, USA, August 23–25, 2010*, pages 167–172. IEEE, August 2010. ISBN: 978-1-4244-7407-3 (Print). (DOI: http://dx.doi.org/10.1109/ISIAS.2010.5604061)

IC.17. Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, Mauro Pellicioli, and **Gerardo Pelosi**. "Low Voltage Fault Attacks to AES". In Jim Plusquellic and Ken Mai, editors, *HOST 2010, Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 13–14 June 2010, Anaheim Convention Center, CA, USA*, pages 7–12, Los Alamitos, CA, USA, June 2010. IEEE Computer Society. ISBN: 978-1-4244-7811-8 (Print), 978-1-4244-7810-1 (Online). (DOI: http://dx.doi.org/10.1109/HST.2010.5513121)

IC.16. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Encryption-Based Policy Enforcement for Cloud Storage". In David H. C. Du and Michel Raynal, editors, *30th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2010 Workshops), 21–25 June 2010, Genova, Italy*, pages 42–51, Washington, DC, USA, June 2010. IEEE Computer Society. ISBN: 978-1-4244-7471-4 (Print), 978-0-7695-4079-5 (Online), ISSN: 1545-0678. (DOI: http://dx.doi.org/10.1109/ICDCSW.2010.35)

IC.15. Giovanni Agosta, Alessandro Barenghi, Fabrizio De Santis, and **Gerardo Pelosi**. "Record Setting Software Implementation of DES Using CUDA". In Shahram Latifi, editor, *Proceeding of the Seventh International Conference on Information Technology: New Generations, ITNG 2010, Las Vegas, Nevada, USA, 12–14 April 2010*, pages 748–755, Los Alamitos, CA, USA, April 2010. IEEE Computer Society. ISBN: 978-0-7695-3984-3 (Print). (DOI: http://dx.doi.org/10.1109/ITNG.2010.43)

IC.14. **Gerardo Pelosi** and Giuseppe Psaila. "SMaC: Spatial Map Caching Technique for Mobile Devices". In Sung Y. Shin, Sascha Ossowski, Michael Schumacher, Mathew J. Palakal, and Chih-Cheng Hung, editors, *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC), Sierre, Switzerland, March 22–26, 2010*, pages 1829–1830, New York, NY, USA, March 2010. ACM. ISBN: 978-1-60558-639-7. (DOI: http://dx.doi.org/10.1145/1774088.1774476)

IC.13. Giovanni Agosta, Alessandro Barenghi, Fabrizio De Santis, Andrea Di Biagio, and **Gerardo Pelosi**. "Fast Disk Encryption through GPGPU Acceleration". In *Proceedings of the 2009 International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2009, Higashi Hiroshima, Japan, December 8–11 2009*, pages 102–109, Los Alamitos, CA, USA, December 2009. IEEE Computer Society. ISBN: 978-0-7695-3914-0. (DOI: http://dx.doi.org/10.1109/PDCAT.2009.72)

IC.12. Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello, and **Gerardo Pelosi**. "Low Voltage Fault Attacks on the RSA Cryptosystem". In Luca Breveglieri, Israel Koren, David Naccache, Elisabeth Oswald, and Jean-Pierre Seifert, editors, *Proceeding of the Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009, Lausanne, Switzerland, September 6, 2009*, pages 23–31, Washington, DC, USA, September 2009. IEEE Computer Society. ISBN: 978-1-4244-4972-9 (Print), 978-0-7695-3824-2 (Online). (DOI: http://dx.doi.org/10.1109/FDTC.2009.30)

IC.11. Andrea Di Biagio, Alessandro Barenghi, Giovanni Agosta, and **Gerardo Pelosi**. "Design of a Parallel AES for Graphics Hardware Using the CUDA Framework". In *Proceedings of the 23rd IEEE International Symposium on Parallel and Distributed Processing, IPDPS 2009, Rome, Italy, May 23–29, 2009*, pages 1–8, Washington, DC, USA, May 2009. IEEE Computer Society. ISBN: 978-1-4244-3751-1 (Print), 978-1-4244-3750-4 (Online), ISSN: 1530-2075. (DOI: http://dx.doi.org/10.1109/IPDPS.2009.5161242)

IC.10. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, **Gerardo Pelosi**, and Pierangela Samarati. "Preserving Confidentiality of Security Policies in Data Outsourcing". In Vijay Atluri and Marianne Winslett, editors, *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society, WPES 2008, Alexandria, VA, USA, October 27, 2008*, pages 75–84, New York, NY, USA, October 2008. ACM. ISBN: 978-1-60558-289-4. (DOI: http://dx.doi.org/10.1145/1456403.1456417)

IC.9. Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, and **Gerardo Pelosi**. "A FPGA Coprocessor for the Cryptographic Tate Pairing over $\mathbb{F}_p$". In Shahram Latifi, editor, *Proceedings of the Fifth International Conference on Information Technology: New Generations (ITNG 2008), 7–8 April 2008, Las Vegas, Nevada, USA*, pages 112–119, Washington, DC, USA, April 2008. IEEE Computer Society. ISBN: 978-0-7695-3099-4. (DOI: http://dx.doi.org/10.1109/ITNG.2008.260)

IC.8. Giovanni Agosta and **Gerardo Pelosi**. "A Domain Specific Language for Cryptography". In *Proceedings of the Forum on Specification and Design Languages, FDL 2007, September 18–20, 2007, Barcelona, Spain*, pages 159–164, September 2007. Electronic Chips & Systems Design Initiative (ECSI). E-ISBN 978-2-9530504-0-0. ISSN: 1636-9874.

IC.7. Giovanni Agosta, Luca Breveglieri, **Gerardo Pelosi**, and Israel Koren. "Countermeasures against Branch Target Buffer Attacks". In Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, and Jean-Pierre Seifert, editors, in *Proceedings of the Fourth International Workshop on Fault Diagnosis and Tolerance in Cryptography, 2007, FDTC 2007, Vienna, Austria, 10 September 2007*, pages 75–79, Washington, DC, USA, September 2007. IEEE Computer Society. ISBN: 978-0-7695-2982-0 (Print), 0-7695-2982-8 (Online). (DOI: http://dx.doi.org/10.1109/FDTC.2007.4318987)

IC.6. Giovanni Agosta, Francesco Bruschi, **Gerardo Pelosi**, and Donatella Sciuto. "A Unified Approach to Canonical Form-based Boolean Matching". In Steven P. Levitan, editor, *Proceedings of the 44th Design Automation Conference, DAC 2007, San Diego, CA, USA, June 4–8, 2007*, pages 841–846, New York, NY, USA, June 2007. ACM. ISBN: 978-1-59593-627-1, ISSN: 0738-100X. (DOI: http://dx.doi.org/10.1145/1278480.1278689)

IC.5. Giovanni Agosta, Luca Breveglieri, **Gerardo Pelosi**, and Martino Sykora. "Programming Highly Parallel Reconfigurable Architectures for Public-Key Cryptographic Applications". In Shahram Latifi, editor, *Proceedings of the Fourth International Conference on Information Technology: New Generations (ITNG 2007), 2–4 April 2007, Las Vegas, NV, USA*, pages 3–10, Washington, DC, USA, April 2007. IEEE Computer Society. ISBN: 0-7695-2776-0 (Print), 978-0-7695-2776-5 (Online). (DOI: http://dx.doi.org/10.1109/ITNG.2007.160)

IC.4. Guido M. Bertoni, Luca Breveglieri, Liqun Chen, Pasqualina Fragneto, Keith A. Harrison, and **Gerardo Pelosi**. "A Pairing SW Implementation for Smart-Cards". In *Proceedings of the Fourth Irish Conference on the Mathematical Foundations of Computer Science and Information Technology, (MFCSIT'06) Cork, Ireland, 1–5, August 2006*, pages 267–271. National University of Ireland Press, August 2006. ISBN: 0-9552229-3-1 (Print).

IC.3. Cesare Alippi, **Gerardo Pelosi**, and Manuel Roveri. "Computational Intelligence Techniques to Detect Toxic Gas Presence". In Fernando Lopez Pefna and Enrique H. Ruspini, editors, *CIMSA 2006. Proceedings of 2006 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, July 12–14, La Coruna, Spain, 2006*, pages 40–44, Piscataway, NJ, USA, July 2006. IEEE. ISBN: 1-4244-0244-1 (Print), 1-4244-0245-X (Online). (DOI: http://dx.doi.org/10.1109/CIMSA.2006.250745)

IC.2. Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, and **Gerardo Pelosi**. "Parallel Hardware Architectures for the Cryptographic Tate Pairing". In Shahram Latifi, editor, *Proceedings of the Third International Conference on Information Technology: New Generations (ITNG 2006), 10–12 April 2006, Las Vegas, NV, USA*, pages 186–191, Washington, DC, USA, April 2006. IEEE Computer Society. ISBN: 0-7695-2497-4 (Print). (DOI: http://dx.doi.org/10.1109/ITNG.2006.107)

IC.1. Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, **Gerardo Pelosi**, and Luigi Sportiello. "Software Implementation of Tate pairing over GF(2^m)". In Georges G. E. Gielen, editor, *Proceedings of the Conference on Design, Automation and Test in Europe: Designers' Forum, DATE 2006, Munich, Germany, March 6–10, 2006*, pages 7–11, Leuven, Belgium, March 2006. European Design and Automation Association (EDAA). ISBN: 3-9810801-0-6, ISSN: 478061. (DOI: http://dx.doi.org/10.1145/1131355.1131358)

BREVETTI EUROPEI E INTERNAZIONALI

European Patents are examined to guarantee: novelty (through carrying out searches using worldwide foreign patent specifications, technical literature and databases), technical soundness, and adherence to formal requirements of the European Patent Office or other national/international intellectual property offices.

The following patents are results of collaborations with the Advanced System Technology Division of STMicroelectronics, Agrate (IT) and the HP Laboratories, Bristol (UK), concerning the design of secure devices and either the definition or the optimization of cryptographic application-specific protocols.

The order of inventors (authors) corresponds to the list of handmade signatures placed on the official documents, filled out on a first-come-first-served basis. Equal contribution and credit should be assigned to each author.

Official copies of the documents listed below can be found at the European Papent Office (EPO): http://www.epo.org/, or at the United States Patent and Trademark Office (USPTO): http://www.uspto.gov/)

When a European patent application is published together with the search report, it is known as an A1 publication. When this application is published without the search report, it is an A2 document. The search report is then published later as an A3 document.
When the patent is granted, it is published as a B document.

PT.10. Granted Patent: **US 8812845 B2**. 19 August 2014 (previously granted as US 8352736 B2, 8 January 2013).
Title: "Authentication Method".
Inventors: Liqun Chen, Keith Harrison, Guido Marco Bertoni, Pasqualina Fragneto, and **Gerardo Pelosi**.
Proprietor(s): STMicroelectronics Srl (IT), Hewlett-Packard Development Company, L.P. (US).
Prior publication data: US 2007180241 A1 – 2007-08-02.
Priority date: 2004-12-23.

PT.9. Granted Patent: **US 8381267 B2**. 19 February 2013.
Title: "Method of Processing Information to be Confidentially Transmitted".
Inventors: Guido Marco Bertoni, Pasqualina Fragneto, **Gerardo Pelosi**, Keith Harrison, and Liqun Chen.
Proprietor(s): STMicroelectronics Srl.
Prior publication data: US 2007260664 A1 – 2007-10-18.
Priority date: 2005-10-11.

PT.8. Granted Patent: **US 8223970 B2**. 17 July 2012.
Title: "Message Deciphering Method, System and Article".
Inventors: Roberto Valerio Sannino, Fabio Sozzani, Guido Marco Bertoni, **Gerardo Pelosi**, and Pasqualina Fragneto.
Proprietor(s): STMicroelectronics Srl (IT).
Prior publication data: US 2011058672 A1 – 2011-03-10. (Previously granted as US 7925010 B2 on 2011-04-12 with prior publication data: US 2005169464 A1 – 2005-08-04).
Priority date: 2003-12-24.

PT.7. Granted Patent: **US 8117251 B2**. 14 February 2012.
Title: "Computation of a Multiplication Operation with an Electronic Circuit and Method".
Inventors: Guido Marco Bertoni, Pasqualina Fragneto, Andrew Marsh, **Gerardo Pelosi**, and Moris Ravasio.
Proprietor(s): STMicroelectronics Srl (IT).
Prior publication data: US 2007260664 A1 – 2007-11-08.
Priority date: 2006-04-11.

PT.6. Granted Patent: **EP 1845442 B1**. 09 November 2011.
Title: "Computation of a Modular Multiplication with an Electronic Circuit".
Inventors: Guido Marco Bertoni, Pasqualina Fragneto, Andrew Marsh, **Gerardo Pelosi**, and Moris Ravasio.
Proprietor(s): STMicroelectronics Srl (IT), STMicroelectronics Limited (UK).
Prior publication data: EP 1845442 B1 – 2007-10-17.
Priority date: 2006-04-11.

PT.5. Granted Patent: **US 7929691 B2**. 19 April 2011.
Title: "Use of Bilinear Mappings in Cryptographic Applications".
Inventors: Keith Alexander Harrison, Liqun Chen, Guido Marco Bertoni, Pasqualina Fragneto, and **Gerardo Pelosi**.
Proprietor(s): Hewlett-Packard Development Company, L.P. (US).
Prior publication data: US 2008016346 A1 – 2008-01-17.
Priority date: 2004-12-23.

PT.4. Granted Patent: **US 7716483 B2**. 11 May 2010.
Title: "Method for Establishing a Communication between Two Devices".
Inventors: Fabio Sozzani, Roberto Valerio Sannino, Guido Marco Bertoni, **Gerardo Pelosi**, and Pasqualina Fragneto.
Proprietor(s): STMicroelectronics Srl (IT).
Prior publication data: US 2005125670 A1 – 2005-06-09.
Priority date: 2003-11-18.

PT.3. Granted Patent: **US 7620186 B2**. 17 November 2009.
Title: "Method for Establishing an Encrypted Communication by Means of Keys".
Inventors: Fabio Sozzani, Roberto Valerio Sannino, Guido Marco Bertoni, **Gerardo Pelosi**, and Pasqualina Fragneto.
Proprietor(s): STMicroelectronics Srl (IT).
Prior publication data: US 2005102507 A1 – 2005-05-12.
Priority date: 2003-09-29.

PT.2. Granted Patent: **EP 1675300 B1**, 01 October 2008.
Title: "Improvements in the Use of Bilinear Mappings in Cryptographic Applications".
Inventors: Keith Alexander Harrison, Liqun Chen, Guido Marco Bertoni, Pasqualina Fragneto, and **Gerardo Pelosi**.
Proprietor(s): Hewlett-Packard Development Company, L.P. (US), STMicroelectronics Srl (IT).
Prior publication data: EP 1675300 A1 – 2006-06-28.
Priority date: 2004-12-23.

PT.1. Granted Patent: **EP 1548976 B1**. 22 August 2007.
Title: "A Message Deciphering Method".
Inventors: Roberto Valerio Sannino, Fabio Sozzani, Guido Marco Bertoni, **Gerardo Pelosi**, and Pasqualina Fragneto.
Proprietor(s): STMicroelectronics Srl (IT).
Prior publication data: EP 1548976 A1 – 2005-06-29.
Priority date: 2003-12-24.

CONTRIBUTI A CONFERENZE INTERNAZIONALI SU INVITO

IP.10. Maurizio Atzori, Alessandro Barenghi, Sara Comai, Mariagrazia Fugini, Diego Marcia, **Gerardo Pelosi**, Manuela Sanguinetti, Vincenzo Scotti. "Improving Work Life Conditions via Portable Knowledge-Driven Recommender System.". In Sergio Greco, Maurizio Lenzerini, Elio Masciari and Andrea Tagarelli (Ed.s), Proceedings of the 29th Italian Symposium on Advanced Database Systems, Pizzo Calabro, Vibo Valentia, Italy, September 5–9, 2021. CEUR Workshop Proceedings Volume 2994, CEUR-WS.org 2021. ISSN: 1613-0073. (url: http://ceur-ws.org/Vol-2994)

IP.9. Rosa Maria Resende de Almeida, Adriana Grau Aberturas, Yolanda Bueno Aguado, Maurizio Atzori, Alessandro Barenghi, Gianluca Borghini, Carlos Alberto Catalina Ortega, Sara Comai, Raquel Losada Durán, Mariagrazia Fugini, Hatice Gunes, Basam Musleh, **Gerardo Pelosi**, Vincenzo Ronca, Licia Sbattella, Roberto Tedesco, Tian Xu.
"Decision Support Systems to Promote Health and Well-being of People of Working Age: the Case of the WorkingAge EU Project". In A. Orailoglu, M. Jung and M. Reichenbach (eds). Proceedings of the Embedded Computer Systems: Architectures, Modeling, and Simulation - 20th International Conference, SAMOS 2020, Samos, Greece, July 5-9, 2020. Lecture Notes in Computer Science, Volume 12471, pp. 336-347. Springer Cham, 2020.
ISBN: 978-3-030-60938-2 (Print), 978-3-030-60939-9 (Online).
(DOI: https://doi.org/10.1007/978-3-030-60939-9_24)

IP.8. Mariagrazia Fugini, Alessandro Barenghi, Sara Comai, **Gerardo Pelosi**, Roberto Tedesco, Marteyn van Gasteren, Carlos Alberto Catalina, Estefanía Arribas Leal, Raquel Losada Durán, Rosa Maria Martins de Almeida, Alexander Mertens,Vera Rick, Hatice Gunes, Tian Xu, Gianluca Borghini, Vincenzo Ronca, Hesam Sagha.
"WorkingAge: Providing Occupational Safety through Pervasive Sensing and Data Driven Behavior Modeling". In Piero Baraldi, Francesco Di Maio and Enrico Zio (eds). *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. ESREL 2020 PSAM 15. June 21-26, 2020. Venice, Italy*. Research Publishing, Singapore.
ISBN: 978-981-14-8593-0 (Print)
(DOI: https://doi.org/10.3850/978-981-14-8593-0)

IP.7. Giovanni Agosta, Carlo Brandolese, William Fornaciari, Nicholas Mainardi, **Gerardo Pelosi**, Federico Reghenzani, Michele Zanella, Gaetan Des Courchamps, Vincent Ducrot, Kevin Juilly, Sébastien Monot, Luca Ceva, "Accelerating Automotive Analytics: The M2DC Appliance Approach". In Pnevmatikatos D., Pelcat M., Jung M. (eds). Embedded Computer Systems: Architectures, Modeling, and Simulation. SAMOS 2019. Lecture Notes in Computer Science, volume 11733. Springer, Cham 2019.
ISBN: 978-3-030-27561-7 (Print), 978-3-030-27562-4 (Online).
(DOI: https://doi.org/10.1007/978-3-030-27562-4_33)

IP.6. Ariel Oleksiak, Michal Kierzynka, Wojciech Piatek, Micha Vor Dem Berge, Wolfgang Christmann, Stefan Krupop, Mario Porrmann, Jens Hagemeyer, René Griessl, Meysam Peykanu, Lennart Tigges, Sven Rosinger, Daniel Schlitt, Christian Pieper, Udo Janssen, Giovanni Agosta, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Mariano Cecowski, Robert Plestenjak, Justin Činkelj, Loïc Cudennec, Thierry Goubier, Jean-Marc Philippe, Chris Adeniyi-Jones, Luca Ceva and Holm Rauchfuss. "M2DC – Modular Microserver DataCentre with Heterogeneous Hardware". *Energy-efficient Servers for Cloud and Edge Computing 2017 Workshop (ENeSCE 2017)*, January 23, 2017, Stockholm, Sweden, co-located with HiPEAC 2017. (URL: http://conferences.microlab.ntua.gr/enesce2017/)
[without formal proceedings]

IP.5. Alessio Agneessens, Francesco Buemi, Stefano Delucchi, Massimo Massa, Giovanni Agosta, Alessandro Barenghi, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Enrico Ferrari, Dajana Cassioli, Luigi Pomante Leonardo Napoletani, Luciano Bozzi, Carlo Tieri, Maurizio Mongelli, "Safe Cooperative CPS: A V2I Traffic Management scenario in the SafeCOP project". In Andreas Gerstlauer and Walid Najjar (Eds.) Proceedings of the *2016 IEEE International Conference on Embedded Computer Systems: Architectures, MOdeling, and Simulation (IC-SAMOS 2016)*, Special Session on European Projects on heterogeneous microservers and parallel embedded computing, July 18–21, 2016. Samos, Greece, pages 320–327, New York, NY, USA, IEEE 2017.
ISBN: 978-1-5090-3077-4 (Print on Demand – PoD), 978-1-5090-3076-7 (Electronic).
IEEE Catalog Number: CFP1652A-ART. (DOI: http://dx.doi.org/10.1109/SAMOS.2016.7818365)

IP.4. Ariel Oleksiak, Michal Kierzynka, Giovanni Agosta, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Micha Vor Dem Berge, Wolfgang Christmann, Stefan Krupop, Mariano Cecowski, Robert Plestenjak, Justin Činkelj, Mario Porrmann, Jens Hagemeyer, René Griessl, Meysam Peykanu, Lennart Tigges, Loïc Cudennec, Thierry Goubier, Jean-Marc Philippe, Sven Rosinger, Daniel Schlitt, Christian Pieper, Chris Adeniyi-Jones, Udo Janssen, and Luca Ceva.
"Data Centres for IoT applications: the M2DC Approach". In Andreas Gerstlauer and Walid Najjar (Eds.) Proceedings of the *2016 IEEE International Conference on Embedded Computer Systems: Architectures, MOdeling, and Simulation (IC-SAMOS 2016)*, Special Session on European Projects on heterogeneous microservers and parallel embedded computing, July 18–21, 2016. Samos, Greece, pages 293–299, New York, NY, USA, IEEE 2017.
ISBN: 978-1-5090-3077-4 (Print on Demand – PoD), 978-1-5090-3076-7 (Electronic).
IEEE Catalog Number: CFP1652A-ART. (DOI: http://dx.doi.org/10.1109/SAMOS.2016.7818361)

IP.3. Ariel Oleksiak, Michal Kierzynka, Giovanni Agosta, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Micha Vor Dem Berge, Wolfgang Christmann, Stefan Krupop, Mariano Cecowski, Robert Plestenjak, Justin Činkelj, Mario Porrmann, Jens Hagemeyer, René Griessl, Meysam Peykanu, Lennart Tigges, Loïc Cudennec, Thierry Goubier, Jean-Marc Philippe, Sven Rosinger, Daniel Schlitt, Christian Pieper, Chris Adeniyi-Jones and Udo Janssen.
"The M2DC Project: Modular Microserver DataCentre".
In Proceedings of the *19th Euromicro Conference on Digital System Design*, Special Session on European Projects in Digital Systems Design, August 31 - September 2, 2016. Limassol, Cyprus, pages 68–74, 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.2016.76)

IP.2. **Gerardo Pelosi**, "Engineering Cryptographic Solutions for Trustworthy Computing Systems", Symposium on Computer Security and Critical Infrastructure, March 16–21, 2015, held at Universidad del Norte, Barranquilla, Colombia, during the 2015 Cátedra Europa International week [talk – without formal proceedings].

IP.1. **Gerardo Pelosi**, "Parallel Hardware for the Computation of Pairings", Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security, December 4–8, 2006, held at Institute for Pure and Applied Mathematics (IPAM) University of California, Los Angeles, CA, USA [talk – without formal proceedings].

CONTRIBUTI IN LIBRI NAZIONALI

NB.1. Franco Chiaraluce, Giuseppe Italiano, **Gerardo Pelosi**, Riccardo Focardi. "Sistemi di crittografia post-quantum e crittografia quantistica". In Roberto Baldoni, Rocco De Nicola e Paolo Prinetto (curatori), *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*. Libro Bianco del Laboratorio Nazionale di Cyber Security (CINI – Consorzio Interuniversitario Nazionale per l'Informatica). ISBN 978-889-4137-330, January 2018.
(URL: https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco)

POSTER A CONFERENZE INTERNAZIONALI CON COMITATO DI REVISIONE

PO.7. Alessandro Barenghi, William Fornaciari, **Gerardo Pelosi** and Davide Zoni. "Side-channel analysis of IoT CPUs: a microarchitectural perspective". Third Annual ARM Research Summit, 17–19 September 2018, Robinson College, Cambridge, UK. (Peer-reviewed project proposal evaluation with no formal proceedings. The primary agenda of the Summit is the discourse of ideas in varying degrees of maturity, and the advancement of research.)

PO.6. Ariel Oleksiak, Michal Kierzynka, Wojciech Piatek, Micha vor dem Berge, Wolfgang Christmann, Stefan Krupop, Mario Porrmann, Jens Hagemeyer, René Griessl, Meysam Peykanu, Lennart Tigges, and Jan Tlatlik, Sven Rosinger, Daniel Schlitt, and Christian Pieper, Holm Rauchfuss, Giovanni Agosta, Alessandro Barenghi, Carlo Brandolese, William Fornaciari, **Gerardo Pelosi**, Joao Pita Costa, Mariano Cecowski, Robert Plestenjak, Justin Cinkelj, Loic Cudennec, Thierry Goubier, Jean-Marc Philippe, Chris Adeniyi-Jones, Javier Setoain, Udo Janssen. "M^2DC – Modular Microserver Data Centre", 32nd International Conference, ISC High Performance 2017, June 18–22, 2017, Frankfurt, Germany.

PO.5. **Gerardo Pelosi** in collaboration with Giovanni Agosta, Alessandro Barenghi, 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 05–09, 2016, Austin, TX, USA.

PO.4. **Gerardo Pelosi** in collaboration with Giovanni Agosta, Alessandro Barenghi, and Massimo Maggi. 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.

PO.3. **Gerardo Pelosi** in collaboration with Giovanni Agosta and Iyad Al Khatib. 2014. "Automated Methodology Integrating Security and Privacy in the Design Process of Medical Devices". Work-in-Progress session at the 2014 Design Automation Conference (DAC'14), June 5, 2014, San Francisco, CA, USA.

PO.2. **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.

PO.1. **Gerardo Pelosi**, "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 (DATE 2010), March 12, 2010, Dresden, Germany.

TESI E RAPPORTI TECNICI

TR.12. Nicholas Mainardi, Alessandro Barenghi, **Gerardo Pelosi**. "Plaintext Recovery Attacks against Linearly Decryptable Fully Homomorphic Encryption Schemes." *International Association for Cryptologic Research (IACR) – Cryptology ePrint Archive*, Report 2020/264, 2020.
http://eprint.iacr.org/2020/264

TR.11. Paolo Santini, Alessandro Barenghi, **Gerardo Pelosi**, Marco Baldi, Franco Chiaraluce, "A Code-specific Conservative Model for the Failure Rate of Bit-flipping Decoding of LDPC Codes with Cryptographic Applications." *International Association for Cryptologic Research (IACR) – Cryptology ePrint Archive*, Report 2019/1441, 2019.
http://eprint.iacr.org/2019/1441
arXiv.org – Computer Science - Cryptography and Security. Technical report arXiv:1912.05182v1 [cs.CR], Dec 2019.
https://arxiv.org/abs/1801.08867v1.

TR.10. Alessandro Barenghi, Nicholas Mainardi, Gerardo Pelosi "Systematic Parsing of X.509: Eradicating Security Issues with a Parse Tree". *arXiv.org – Computer Science - Cryptography and Security*. Technical report arXiv:1812.04959 [cs.CR], Dec 2018. http://arxiv.org/abs/1812.04959

TR.9. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi**, Joachim Rosenthal, Paolo Santini, Davide Schipani, "Design and Implementation of a Digital Signature Scheme Based on Low-density Generator Matrix Codes". *arXiv.org – Computer Science - Cryptography and Security*. Technical report arXiv:1807.06127v1 [cs.CR], Jul. 2018.
https://arxiv.org/abs/1807.06127v1.

TR.8. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, **Gerardo Pelosi**, Paolo Santini, "LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes". *arXiv.org – Computer Science - Cryptography and Security*. Technical report arXiv:1801.08867v1 [cs.CR], Jan 2018. https://arxiv.org/abs/1801.08867v1.

TR.7. **Gerardo Pelosi** in collaboration with Alessandro Barenghi and Francesco Regazzoni, "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. **Gerardo Pelosi** in collaboration with Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, and Mauro Pellicioli, "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.
http://eprint.iacr.org/2010/130.pdf

TR.5. **Gerardo Pelosi** in collaboration with Pierangela Samarati, "Tools on Access Control Mechanisms", *PrimeLife - Bringing sustainable privacy and identity management to future networks and services. EU Framework Programme 7, ICT-2007.1.4 – ref. 216483, report H.2.4*, September 2009.

TR.4. **Gerardo Pelosi** "Algorithms Architectures and Protocols for Public-Key Cryptographic Systems with Innovative and Complex Functionalities: The Case of IBE and Compact Discrete Logarithm Systems", *Ph.D. Thesis in Information Technology, Politecnico di Milano*. (May 2007).

TR.3. **Gerardo Pelosi** in collaboration with Giovanni Agosta, "Countermeasures for the Simple Branch Prediction Analysis", *International Association for Cryptologic Research (IACR) – Cryptology ePrint Archive*, Report 2006/482. Dec. 2006.
http://eprint.iacr.org/2006/482.pdf

TR.2. **Gerardo Pelosi** "Gas Sensor Array Response Analysis by means of computational intelligence techniques". *Technical Report n. 2006.17 Politecnico di Milano*. January 2006.

TR.1. **Gerardo Pelosi** (in Italian) "Crittografia basata su curve ellittiche in aritmetica modulare: studio di fattibilità, ottimizzazione e realizzazione software per smart card". *Laurea* degree (M.Sc. italian equivalent, 5 years) in Telecommunication Engineering from Politecnico di Milano, Italy. February 2003.

ARTICOLI SOTTOPOSTI A VALUTAZIONE (*Peer-review*)

SB.2. Isabella Piacentini, Alessandro Barenghi and **Gerardo Pelosi**, "A Computation Interleaving Countermeasure against Profiled Side Channel Attacks."
(Submitted for peer-review evaluation)

SB.1. Simone Perriello, Alessandro Barenghi, and **Gerardo Pelosi**, "Quantum Circuits for Information Set Decoding.".
(Submitted for peer-review evaluation)

Associazioni scientifiche e professionali

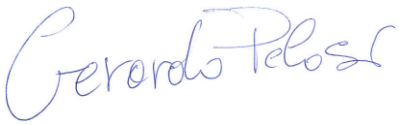
Erdős Number: 2
(Gerardo Pelosi → Israel Koren → Paul Erdős)

- HiPEAC Member
  European Network of Excellence on High Performance and Embedded Architecture and Compilation
- ACM Professional Member
  Association for Computing Machinery
- IEEE Member
  Institute of Electrical and Electronics Engineers
- IEEE Computer Society Member
- IEEE Communications Society Member
- IEICE Member
  Institute of Electronics, Information and Communication Engineers
- ISSA Member
  Information Systems Security Association
- De Componendis Cifris (Italian Cryptography National Association)
- Italian Cybersecurity National Laboratory Member
- INSTICC Member
  Institute for Systems and Technologies of Information, Control and Communication (http://www.insticc.org)

Milano, 9 Gennaio 2023

In Fede

Gerardo Pelosi



Autorizzo il trattamento dei dati personali precedentemente riportati ai sensi del D. Lgs. 196/2003: "Codice in materia di protezione dei dati personali" e delle successive modificazioni e integrazioni ai sensi del D.Lgs n. 101 del 10 agosto 2018 e del Regolamento Europeo 2016/679 (GDPR)