UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Activities and Publications Report

PhD Student: Daniele Lombardi

Student DR number: DR996240

PhD Cycle: XXXVII
PhD Cycle Chairman: Prof. Stefano Russo

PhD program student's start date: 01/01/2022
PhD program student's end date: 31/12/2024

Supervisor: Valentina Casola

e-mail: casolav@unina.it

PhD scholarship funding entity:
No scholarship.

December 8, 2024

General information

Daniele Lombardi received in year 2021 the Master Science degree in Computer Engineering from the University of Napoli Federico II. He attended a curriculum in Computer Engineering within the PhD program in Information Technology and Electrical Engineering.

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organization
1st	Virtualization technologies and their applications	Ad hoc course	5	Luigi De Simone	ITEE
1st	Statistical data analysis for science and engineering research	Ad hoc course	4	Roberto Pietrantuono	ITEE
1st	Data Science for Patient Record Analysis	Ad hoc course	3	Marcello Cinque	ITEE
2nd	Risk Assessment	MSc course	6	Alessandra De Benedictis	UniNa
3rd	Industrial Embedded Systems Design with the ARM Architecture	Ad hoc course	4	Mario Barbareschi	ITEE

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organization
1st	Summer School on Security Testing and Verification	Leuven, Belgium	4.8	21-23.09.2022	KU Leuven (Belgium)

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organization
1st	Seeqc: the digital quantum computing company	0.2	Marco Arzeo	Seeqc-EU srl	UniNa
1st	Can a Text-to-Speech Engine Generate Human Sentiments?	0.2	Prof. Vijay K. Gurbani	llinois Institute of Technology	UniNa
1st	Malware reverse engineering: foundations	0.4	Antonio Villani	Leonardo's Cybersecurity Division	University of Rome Sapienza
1st	IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE Editors	0.3	Dr. Derek Abbott, Dr. Paolo Bonato, Eszter Lukacs, Judy Brady	University of Adelaide, Australia, IEEE / Harvard University, USA, IEEE	IEEE
1st	Ciberconflitti e minacceper la pace e la	0.4	Simon Pietro Romano	University of Naples Federico II	RUniPace

	stabilità internazionale				
1st	Potential and challenges of next generation railway signaling systems: Moving Block and Virtual Coupling	0.2	Joelle Aoun	Faculty of Civil Engineering and Geosciences, Delft	UniNa
1st	Springer Nature Author Workshop: Open Access and Transformative Agreements in Italy	0.3	Martina Marchesi	Springer Nature	Springer Nature
1st	Explainable Natural Language Inference	0.3	Marco Valentino	University of Manchester, Manchester, United Kingdom	UniNa
1st	The role of the Italian National Cybersecurity Agency	0.4	Roberto Baldoni	Italian National Cybersecurity Agency	University of Rome Sapienza
1st	International cooperation on cybercrime – The criminal justice perspective	0.4	Matteo Lucchetti	CYBER 4.0, National Cybersecurity Competence Center	University of Rome Sapienza
1st	Blockchain in Business	0.3	G Mutarelli, L. Conforto	Capgemini Invest	UniNa
1st	PRIVACY-PRESERVING MACHINE LEARNING	0.4	Vittorio Prodomo	Universidad Carlos III of Madrid (uc3m), University of Napoli Federico II	UniNa
2nd	Resilience is the cybersecurity of the xxi century: a blockchain example	0.4	Fabio De Gaspari	Sapienza, University of Rome	Sapienza, University of Rome
2nd	9th IEEE International3.6 Workshop on Advances in Sensors and Interfaces	3.6	Daniela De Venuto	Department of Electric and Computer Engineering Polytechnic of Bari	Department of Electric and Computer Engineering Polytechnic of Bari
2nd	Ricerca e formazione nella società della transizione digitale	1	Nicola Mazzocca	DIETI - UniNa	CINI - DIETI
2nd	Come può tornarci utile la scienza	0.4	Giorgio Parisi	Sapienza University of Rome	UniNa
2nd	Data spaces discovery day	1	Valentina Casola, Giulia Giussani	UniNa, International Data	UniNa

				Spaces Association	
2nd	The 14th Ieee International Conference On Cloud Computing Technology And Science	5	Massimiliano Rak, Valentina Casola, Alessandra De Benedictis, Umberto Villano	University of Campania Luigi Vanvitelli, UniNa, UniNa, University of Sannio, Italy	Università degli Studi del Sannio – Benevento, CERICT
2nd	"CSAW 2023 – Puf-enabled Security Challenge"	2	David Hely	Grenoble INP	Grenoble INP - Esisar

Research activities

During these three years, Daniele Lombardi participated in the research of Physical Unclonable Functions as security primitive for resource-poor devices. In particular, he dealt with the aspects concerning the quantitative evaluation of PUFs, designing and implementing a platform, flexible and easy to use, that allows the automated evaluation of generic PUFs synthesized on FPGA technology. In addition, he proposed a family of protocols for secure communication between a pair of nodes and among dynamic members of a group in a network. Finally, the candidate also proposed a virtual PUF model, suitable in multi-user contexts.

In addition, Daniele Lombardi was also interested in the research concerning the design of critical systems, with particular reference to the railway domain. The research mainly focused on the design of safety mechanisms for the management of redundant systems in 2x2oo2 configuration. These activities resulted in: industrial prototypes, equipped with all documentations required by industry standards EN50128, tested on target architectures; and, some scientific publications on the testing of non-intrusive real-time systems and on the evaluation of interrupts mechanisms for predictability of critical systems.

Tutoring and supplementary teaching activities

Daniele Lombardi was a co-rapporteur in the following theses:

- Title: *The Concept of Virtual PUF and beyond: a comprehensive analysis, requirements and design prototypes*
  Student: Francesco Auriemma
  Rapporteur: Mario Barbareschi
  Type: Master Thesis

- Title: *Handling Cyber and Physical Security Incidents on Critical Infrastructures*
  Student: Angelo Pio Amirante

Rapporteur: Valentina Casola
Type: Thesis

- Title: *Mastering software log for test coverage*
  Student: Francesco Bianco
  Rapporteur: Mario Barbareschi
  Type: Master Thesis

- Title: *Design of a redundant system with symmetrical units for critical applications*
  Student: Maurizio Gaudino
  Rapporteur: Mario Barbareschi
  Type: Master Thesis

- Title: *Engineering a non-intrusive testing approach for hard real time systems*
  Student: Davide Marcello
  Rapporteur: Mario Barbareschi
  Type: Master Thesis

- Title: *Lightweight group key management:* the GK-PHEMAP protocol
  Student: Antonio Emmanuele
  Rapporteur: Mario Barbareschi
  Type: Master Thesis

- Title: *Online Execution-Trace Analysis in Real-Time Systems to Detect Timing Bugs*
  Student: Salvatore Della Torca
  Rapporteur: Valentina Casola
  Other co-rapporteurs: Salvatore Barone
  Type: Master Thesis

Credits summary

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	12	8,6	32,6	0
2nd	6	13,4	40,4	0

3rd	4	0	63	0

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
3rd	Tima Laboratory, University of Grenoble Alpes – Grenoble INP UGA – CNRS (France)	Giorgio di Natale, Director of Research (CNRS) - TIMA Director	26/05/2024 - 31/07/2024 28/08/2024 - 12/10/2024	Design and development of a fully automated platform for evaluation of generic PUFs synthesized on FPGA technology.

PhD Thesis

In his PhD Thesis, Daniele Lombardi investigated the challenges associated with designing secure resource-constrained devices through the adoption of Physical Unclonable Functions (PUFs). As a matter of fact, PUF is a promising technology for hardware security, offering unique and irreproducible characteristics that make them ideal for addressing security problems such as device identification, cryptographic key generation, and tamper resistance. Their distinctive features and ease of integration make them particularly well-suited for deployment in resource-constrained devices, such as those commonly found in the Internet of Things (IoT). However, despite the growing and evident attention of the scientific community over recent decades, their practical adoption is hindered by several significant unresolved challenges.

Before utilizing a PUF implementation, it is crucial to ensure its quality to avoid compromising the security of the system to protect. To this aim, the scientific community has proposed a set of quality metrics to quantitatively evaluate the performance of a PUF implementation. However, characterizing a PUF, by assessing its metrics, can be an economically and temporally expensive activity, as it requires employing a large number of devices to collect statistically significant data. Once the PUF assessment is complete, another issue arises concerning security applications based on PUFs. The limited resources available on devices to be secured necessitate applications that require minimal computational and memory resources. For instance, many such devices are equipped with ultra-low-power microcontrollers and are often battery-powered. Existing applications, however, often lack a thorough analysis demonstrating their secure and lightweight nature. Moreover, while various existing solutions address known problems such as mutual

authentication or group key management, not all of them are suitable for specific challenges of real-world IoT scenarios (e.g., dynamic membership of nodes). Finally, the relentless demand for more efficient and scalable resource usage, even at the Edge, has led to the adoption of multi-user paradigms. However, these paradigms are not fully compatible with the security properties offered by the current PUF model. For instance, a multi-user system with a PUF-based cryptographic keys management mechanism is clearly vulnerable to the "impersonation" problem if all users rely on the same PUF circuit.

To address these challenges, this thesis proposes a set of tools, methodologies, and models designed to guide and support the design, the implementation and the evaluation of PUF-based security solutions for resource-constrained devices. Specifically, the thesis introduces a flexible tool for large-scale, automated quantitative assessment of generic PUFs synthesized on FPGAs. To meet the demand for lightweight applications, the thesis presents a family of PUF-based protocols, along with an in-depth analysis and evaluation that demonstrates their feasibility in resource-constrained environments. Finally, the thesis illustrates how challenges related to the adoption of the multi-user paradigm in systems whose security relies on PUFs can be overcome by employing a new model of PUF.

Research products

Research results appear in 1 paper published in international journal, 2 papers under review in international journals, 6 contributions to international conferences and 1 contribution under review to international conference.

List of scientific publications

International journal papers

M. Barbareschi, V. Casola, A. Emmanuele, D. Lombardi
A Lightweight PUF-based Protocol for Dynamic and Secure Group Key Management in the IoT
IEEE Internet of Things Journal
VOL. 11, NO. 20, pp. 32969- 32984, 2024, DOI: 10.1109/JIOT.2024.3418207

M. Barbareschi, A. Emmanuele, D. Lombardi
Pioneering Virtual Physical Unclonable Functions
IEEE Transactions on Emerging Topics in Computing
Under the 1st round of revision

D. Lombardi, M. Barbareschi, V. Casola, E. Vatajelu, G. Di Natale
On the large-scale characterization of FPGA-based Physical Unclonable Functions
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
Under the 1st round of revision

International conference papers

M. Barbareschi, V. Casola, D. Lombardi

Lightweight Secure Keys Management Based on Physical Unclonable Functions,
International Workshop on Advances in Sensors and Interface (IWASI),
Bari, Italy, 8-9 June 2023, pp. 34-39, IEEE, doi: 10.1109/IWASI58316.2023.10164402.

M. Barbareschi, S. Barone, V. Casola, S. Della Torca, D. Lombardi
Automatic Test Generation to Improve Scrum for Safety Agile Methodology,
ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security,
Benevento, Italy, 29 August 2023, Article No.: 137, Pages 1 - 6, DOI: 10.1145/3600160.3605061

S. Barone, V. Casola, S. Della Torca, D. Lombardi

Timing Behavior Characterization of Critical Real-Time Systems through Hybrid Timing Analysis,
International Conference on System Reliability and Science (ICSRS),
Bologna, Italy, 22-23 November 2023, pp. 306-311, IEEE, DOI: 10.1109/ICSRS59833.2023.10381272.

M. Barbareschi, V. Casola, D. Lombardi

Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions,
IEEE International Conference on Cloud Computing Technology and Science (CloudCom),
Naples, Italy, 4-6 Dec. 2023, IEEE, pp. 273-278, DOI: 10.1109/CloudCom59040.2023.00051.

M. Barbareschi, V. Casola, A. Emmanuele, D. Lombardi

On the adoption of PUF for key agreement scheme in Internet of Things,
CF '24 Companion: Proceedings of the 21st ACM International Conference on Computing Frontiers: Workshops and Special Sessions,
Ischia, Italy, 1 July 2024, pp. 17 - 24, ACM, DOI: 10.1145/3637543.3654656

M. Barbareschi, V. Casola, A. Emmanuele, D. Lombardi
A comprehensive evaluation of interrupt measurement techniques for predictability in safety-critical systems,
ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security,
Vienna, Austria, 30 July 2024, Article No.: 172, pp. 1 - 10, ACM, DOI:10.1145/3664476.367045

F. Ferrandino, D. Lombardi, A. Cilardo

A One-LUT Physical Unclonable Function on AMD FPGAs,
DATE 2025: Late Breaking Results,
Under the 1st round of revision

Patents and/or spin offs

No

Awards and Prizes

The work "A group-key management protocol based on PUF" has been selected as finalist for the CSAW'23 International Competition in the Challenge "*PUF enabled security Challenge*", Valence (France), November 2023.

Date 10/12/2024

PhD student signature Daniele Lombardi

Supervisor signature Valentina Casola