Agnese Gini

Curriculum Vitae

Université du Luxembourg
2, avenue de l'Université
Esch-sur-Alzette, Luxembourg
Office: MNO E03 0335-020
☎ *+352 46 66 44 5914*
✉ *firstname.lastname@uni.lu*
agnesegini.github.io

Research Interests

Research Area: *Cryptology, Cryptanalysis*.
Lattice based cryptography, computational number theory, computer algebra for applications in classic and post-quantum cryptography.

Research Experiences

Since Jul. 2022 **Postdoctoral Researcher**, at *Interdisciplinary Centre for Security, Reliability and Trust of University of Luxembourg (SnT)*.

Nov. 2018 - Jul. 2022 **Doctoral Researcher**, at *Interdisciplinary Centre for Security, Reliability and Trust of University of Luxembourg (SnT)*, under supervision of Prof. Jean-Sébastien Coron.

Education

Nov. 2018 - Jul. 2022 **Ph.D. in Cryptography**, *Université du Luxembourg*, Esch-sur-Alzette, Luxembourg.

- **Ph.D. Thesis:** *On the hardness of the hidden subset sum problem: algebraic and statistical attacks*, under supervision of **Prof. Prof. Jean-Sébastien Coron**.

Sep. 2015 - Jun. 2018 **Master degree in Mathematics**, *Università di Pisa*, Pisa, Italy, *110/110 cum laude.*

- Computer algebra specialised curriculum.
- **M.Sc. Thesis:** *Supersingular Isogeny Diffie Hellman: Algorithms and Quantum Security*, under supervision of **Prof. Carlo Traverso** and **Prof. Dvornicich Roberto**.

Sep. 2011 - Jul. 2015 **Bachelor degree in Mathematics, Computational curriculum**, *Università di Pisa*, Pisa, Italy, *99/110.*

- **B.Sc. Thesis:** *The real radical computation*, under supervision of **Prof. Patrizia Gianni**.

2011 **High school degree**, *Liceo Scientifico XXV Aprile*, Pontedera, Italy, *100/100 cum laude.*

Publications

- *On the algebraic immunity of weightwise perfectly balanced functions* with Pierrick Méaux. Preprint `ia.cr/2023/495`
- *Weightwise perfectly balanced functions and nonlinearity* with Pierrick Méaux.(C2SI2023) Full version: `ia.cr/2022/1777`
- *Weightwise almost perfectly balanced functions: secondary constructions for all n and better weightwise nonlinearities* with Pierrick Méaux.(INDOCRYPT2022) Full version: `ia.cr/2022/1434`
- *On the weightwise nonlinearity of weightwise perfectly balanced functions* with Pierrick Méaux in Discrete Applied Mathematics `doi.org/10.1016/j.dam.2022.08.017` Full version: `ia.cr/2022/408`

- *Provably Solving the Hidden Subset Sum Problem via Statistical Learning* with Jean-Sébastien Coron. (MathCrypt2021) Full version: `https://ia.cr/2021/1007`
- *A Polynomial-Time Algorithm for Solving the Hidden Subset Sum Problem*, with Jean-Sébastien Coron. (CRYPTO2020) `doi.org/10.1007/978-3-030-56880-1_1`. Full version: `https://ia.cr/2020/461.pdf`
- *Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem* with Jean-Sébastien Coron. (NutMiC2019) `doi.org/10.1515/jmc-2019-0027`.

Activities

Talks.

- *About Hidden Subset Sum Problem and its cryptographic applications.*, UL-SP2 final workshop, June 6, 2023.
- *Weightwise perfectly balanced functions and nonlinearity*, C2SI2023 , May 31, 2023.
- *What we know (and do not) about the hidden subset sum problem*, CrossFyre23, April 23, 2023.
- *On the hardness of the hidden subset sum problem* at Women in Algebra and Symbolic Computations II, November 30, 2021.
- *Precomputed DL sets for speeding up cryptography have an expiration time* at UL, October 19, 2021.
- *Provably Solving the Hidden Subset Sum Problem via Statistical Learning* at MathCrypt2021, Virtual, August 15 2021.
- *Polynomial-Time Algorithm for Solving the Hidden Subset Sum Problem* at CRYPTO2020, Virtual `youtu.be/LXWtgl54Eos`, August 17-21 2020.
- *Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem* at NutMiC2019, Paris, June 27, 2019.
- *Short Integer Solutions A Worst-case to Average-case Reduction* at University of Luxembourg in Introduction to lattices and their applications in Computer Science and Cryptography- Seminar, June 14, 2019,
- *Supersingular Isogeny Diffie Hellman: Algorithms and Quantum Security* at CWI Amsterdam, September 12, 2018.

Schools.

- *Selected Areas in Cryptography (SAC) Summer School.* Virtual, October 19-23, 2020.
- *Selected topic on High Performance Computing Summer School.* Esch-sur-Alzette, Luxembourg, June 20-21, 2019
- *Mathematical Foundations of Asymmetric Cryptography Winter School.* Aussois, France, March 17-22, 2019

Conferences and workshop attendance.

EUROCRYPT2019, NutMiC2019, Luxembourg Number Theory Day 2019, EUROCRYPT2020, PKC2020, CRYPTO2020, MathCrypt2021,EUROCRYPT2022,EUROCRYPT2023,C2SI.

Doctoral Education Trainings.

- *PCAP: Programming Essentials in Python (Parts 1 and 2)* by Cisco Networking Academy, in the frame of UL Competence Centre courses. Spring 2021.
- *Elements of AI*, `elementsofai.lu` in the frame of UL Competence Centre courses. Spring 2021.
- *Number theory for cryptography.* Course taught by Prof. Dr. Gabor Wiese, in the training program of the SP2 DTU. Fall 2020.
- *Introduction to Cyber-Security.* Course taught by Tristan Madani, in the frame of the UL Doctoral Programme in Computer Science & Computer Engineering. Fall 2020.

- *Data visualisation and statistical graphics with STATA*. Course taught by Dr. Philipp Van Kerm, in the frame of the UL Transferable Skills Courses. June, 2020.
- *Algebraic Geometry*. Course taught by Prof. Dr. Sarah Scherotzke, in the frame of the UL Doctoral Programme in Mathematics & Applications. Fall 2019.
- *Introduction to Lattices and their Applications in Computer Science and Cryptography*. Seminars, in the frame of the UL Doctoral Programme in Computer Science & Computer Engineering. Spring 2019.
- *Blockchain and Distributed ledgers : from theory to programming*. Course in the frame of the UL Doctoral Programme in Computer Science & Computer Engineering. October 14-15, 2019.
- *Good Scientific Practice*. Course taught by Dr. Michael Gommel, in the frame of the UL Transferable Skills Courses. August 1-2, 2019.
- *Curves over Finite Fields*. Course taught by Prof. Dr. Gerard van der Geer, in the frame of the UL Doctoral Programme in Mathematics & Applications. Spring 2019.

Teaching Experiences

Spring 2023 **Teaching course**, *Software Foundations - Haskell*.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Fall 2022 **Master project supervisor**, *Commitments protocols as a tool for blockchain and cryptocurrencies*, Semester 3.
Master in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Fall 2022 **Teaching course**, *Security 1*.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Fall 2022 **Bachelor project supervisor**, *Cryptographic Hash Functions and the Fiat-Shamir paradigm*, Semester 3.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Spring 2022 **Bachelor project supervisor**, *Challenges of Secure Hash Algorithms*, Semester 2.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Fall 2021 **Bachelor project supervisor**, *Subset Sum Problem: theory and practice*, Semester 5.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Spring 2021 **Bachelor project supervisor**, *BCI for Patients unable of verbal communication*, Semester 2.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Fall 2020 **Bachelor project supervisor**, *Linear algebra low-level routines: theory and applications*, Semester 1.
Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

Year 2017/18 **Teaching assistant**, *Mathematics and Statistics*.
Dipartimento di Scienze Agrarie, Università di Pisa, Pisa, Italy

Sep. 2017 **Counselor**, *High-school student orientation*.
Dipartimento di Matematica, Università di Pisa, Pisa, Italy

- Reception students, editing of the open days journal, authorship article "Paper and pencil: TWIXT!"

Spring 2017 **Teaching assistant**, *Geometry and Linear Algebra*.
Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Pisa, Italy

Fall 2016 **Teaching assistant**, *Linear Algebra*.
Dipartimento di Ingegneria dell'Informazione, Università di Pisa, Pisa, Italy

Computer skills

Python	*Advanced*	C	*Good*
OS:	Windows, Linux (Ubuntu)	*Others:*	Github, LaTeX, Haskell, HPC

Languages

- **Italian:** Mother tongue.
- **English:** Fluent.
- **French:** Beginner.

References

- **Prof. Jean-Sébastien Coron**
  Department of Computer Science (DCS)
  Faculty of Science, Technology and Medicine (FSTM)
  Université du Luxembourg
  Esch-sur-Alzette, Luxembourg
  firstname.lastname@uni.lu