

# 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](mailto:firstname.lastname@uni.lu)  
📁 [agnesegini.github.io](https://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 Nov. 2018 **Doctoral Researcher**, at *Interdisciplinary Centre for Security, Reliability and Trust of University of Luxembourg (SnT)*, under supervision of Prof. Jean-Sébastien Coron.

### Education

Since Nov. 2018 **Ph.D. in Cryptography**, *Université du Luxembourg*, Esch-sur-Alzette, Luxembourg, under supervision of **Prof. Jean-Sébastien Coron**.

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

Jun. 2018 ○ 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 - **Bachelor degree in Mathematics, Computational curriculum**, *Università di Pisa*, Pisa, Italy, *99/110*.

Jul. 2015 ○ **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

- *Provably Solving the Hidden Subset Sum Problem via Statistical Learning* with Jean-Sébastien Coron. (MathCrypt2021) Full version: [eprint.iacr.org/2021/1007.pdf](https://eprint.iacr.org/2021/1007.pdf)
- *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](https://doi.org/10.1007/978-3-030-56880-1_1). Full version: [eprint.iacr.org/2020/461.pdf](https://eprint.iacr.org/2020/461.pdf)
- *Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem* with Jean-Sébastien Coron. (NutMiC2019) [doi.org/10.1515/jmc-2019-0027](https://doi.org/10.1515/jmc-2019-0027).

### Activities

#### Talks.

- *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/LXWtg154Eos](https://youtu.be/LXWtg154Eos), 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.

#### 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

- |             |   |
|-------------|---|
| Fall 2021   | <b>Bachelor project supervisor</b> , <i>Subset Sum Problem: theory and practice</i> , Semester 5.<br>Bachelor in Computer Science, Université du Luxembourg, Esch-sur-Alzette, Luxembourg         |
| Spring 2021 | <b>Bachelor project supervisor</b> , <i>BCI for Patients unable of verbal communication</i> , Semester 2.<br>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

## 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