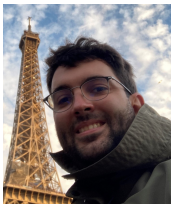
MARTINO BORELLO

PERSONAL DETAILS

Born in Milan, MI, Italy, on July 28^{th} 1986
Citizenship: Italian
Work Email: martino.borello@univ-paris8.fr
Personal Email: martino.borello@gmail.com
Homepage: www.math.univ-paris13.fr/~borello/
Married with three children



HIGHLIGHTS

- **Visiting positions in Germany, Ireland, Italy, Switzerland**
- **∼415 000€ of grants**
- **25 publications, 5 preprints**
- **Reviewer of many papers, 2 applications and a Ph.D. thesis**
- **Member of 6 committees of international conferences**
- **Organizer of seminars in France and Switzerland**
- **Editor of a Special Issue of AMC**
- **27 invited lectures and 12 talks**
- **More than 1200 hours of teaching (both undergrad and grad)**
- **Supervisions of 1 Ph.D. thesis and 10 Master projects**

EMPLOYMENT

Maître de Conférences (tenure) September 2016 - present

at Université de Paris 8,
2 Rue de la Liberté
93526 Saint–Denis, France

Équipe AGC3 at **LAGA** (**Université Paris 8** et Paris 13, CNRS)

Scientific Collaborator (postdoc) September 2014 - August 2016

at Mathematics Institute for Geometry and Applications,
EPFL SB MATHGEOM CSAG
Station 8 - CH-1015 Lausanne

Director: Prof. Eva Bayer-Fluckiger

Collaboration with Prof. Peter Jossen, ETH, Zürich

EDUCATION

PhD, **Pure and Applied Mathematics** January 2011 - January 2014
Università degli studi di Milano Bicocca, Milan, MI, Italy
Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length 72,
supervisors Prof. Francesca Dalla Volta (Milan) and Prof. Massimiliano Sala (Trento)
defended on January 16^{th} 2014
Concentration: Algebraic coding theory, Representation Theory,
Permutation Groups, Automorphisms of combinatorial structures
Minor: Cryptography

QUALIFICATION Abilitazione Scientifica Nazionale for Associate Professor (settore 01/A2, Geometry and Algebra) from the Italian MIUR

VISITING POSITIONS

Scientific Collaboration with Prof. W. Willems — October 2011 - December 2011
Otto von Guericke Universität, Magdeburg, Germany

Scientific Collaboration with Prof. W. Willems — April 2012 - June 2012
Otto von Guericke Universität, Magdeburg, Germany

Scientific Collaboration with Prof. G. Nebe — May 2013
RWTH Aachen University, Aachen, Germany

Scientific Collaboration with Dr. A. Malevich — November 2013
Leibniz Universität Hannover, Hannover, Germany

Academic visitor — March 2014 - May 2014
at Mathematics Institute for Geometry and Applications
EPFL, Lausanne, Switzerland

Academic visitor — July 2018
at Università degli Studi di Milano-Bicocca
Milan, Italy

Scientific Collaboration with Prof. E. Byrne — July 2022
University College Dublin, Dublin, Ireland

PRIZES AND GRANTS

- Projet IRN MaDeF, **1000€** — 2023
  coordinator: M. Borello
- Projet AAP Paris 8, **3505€** — 2023
  coordinator: M. Borello
- Individual Award for Educational Investment, **12000€** — 2023-2025
- ANR "Algèbre, preuves, protocoles, algorithmes, courbes, et surfaces pour les codes et leurs applications", **377 227,89€** — 2021-2025
  member of the Paris 8 pole, coordinator: A. Couvreur
  `https://barracuda.inria.fr/fr/`
- Prize Ulysse 2021 (France-Ireland), **5000€** — 2021-2022
  coordinators: M. Borello and E. Byrne
- Projet AAP Paris 8, **8910€** — 2018-2022
  coordinator: M. Borello
- Projet Exploratoire Premier Soutien (PEPS), **6000€** — 2017-2018
  coordinator: M. Borello
- *"Fondazione Famiglia Legnanese" Scholarship*, **3000€** — 2009
- *"Istituto Nazionale di Alta Matematica" Scholarships*, **12000€** — 2005-2007
- *"Mu Alpha Theta-Fast" Prize* for the use of modern mathematics — 2005
- *"Istituto Lombardo, Accademia di Scienze e Lettere" Scholarships*, **6000€** — 2001-2004

PUBLICATIONS

1. M. Borello, *The automorphism group of a self-dual* $[72, 36, 16]$ *binary code does not contain elements of order* 6, **IEEE Transactions on Information Theory** 58(12): 7240–7245 (2012)
(DOI:10.1109/TIT.2012.2211095)
2. M. Borello and W. Willems, *Automorphism of order* $2p$ *in binary self-dual extremal codes of length a multiple of* 24, **IEEE Transactions on Information Theory** 59(6): 3378–3383 (2013)
(DOI:10.1109/TIT.2013.2243802)
3. M. Borello, F. Dalla Volta and G. Nebe, *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain* $\mathcal{S}_3$, $\mathcal{A}_4$ *or* D_8, **Advances in Mathematics of Communications** 7(4): 503–510 (2013)
(DOI:10.3934/amc.2013.7.503)
4. M. Borello, *The automorphism group of a self-dual* $[72, 36, 16]$ *code is not an elementary abelian group of order* 8, **Finite Fields and Their Applications** 25: 1–7 (2014)
(DOI:10.1016/j.ffa. 2013.07.007)
5. M. Borello and G. Nebe, *On involutions in extremal self-dual codes and the dual distance of semi self-dual codes*, **Finite Fields and Their Applications** 33: 80–89 (2015)
(DOI:10.1016/j.ffa.2014.11.008)
6. M. Borello, *On the automorphism groups of binary linear codes*, Topics in Finite Fields, **Contemporary Mathematics** 632 (2015)
(DOI:10.1090/conm/632)
7. E. Bayer-Fluckiger, M. Borello and P. Jossen, *Inhomogeneous minima of mixed signature lattices*, **Journal of Number Theory** 167: 88–103 (2016)
(DOI:10.1016/j.jnt.2016.03.010)
8. M. Borello and J. de la Cruz, *Some new results on the self-dual* $[120, 60, 24]$ *code*, **Finite Fields and Their Applications** 50: 17–34 (2018)
(DOI:10.1016/j.ffa.2017.11.004)
9. M. Borello and O. Mila, *Symmetries of weight enumerators and applications to Reed-Muller codes*, **Advances in Mathematics of Communications** 13(2): 313–328 (2019)
(DOI:10.3934/amc.2019021)
10. M. Borello, P. Moree and P. Solé, *Asymptotic performance of metacyclic codes*, **Discrete Mathematics** 343(7) (2020)
(DOI:10.1016/j.disc.2020.111885)
11. M. Borello, J. de la Cruz and W. Willems, *A Note on Linear Complementary Pairs of Group Codes*, **Discrete Mathematics** 343(8) (2020)
(DOI:10.1016/j.disc.2020.111905)
12. M. Borello and W. Willems, *Group codes over fields are asymptotically good*, **Finite Fields and Their Applications** 68: 101738 (2020)
(DOI:10.1016/j.ffa.2020.101738)
13. M. Bonini and M. Borello, *Minimal linear codes arising from blocking sets*, **Journal of Algebraic Combinatorics** 53(2): 327–341 (2021)
(DOI:10.1007/s10801-019-00930-6)
14. M. Borello and A. Jamous, *Dihedral codes with prescribed minimum distance*, In: Bajard J.C., Topuzolu A. (eds) Arithmetic of Finite Fields. WAIFI 2020. **Lecture Notes in Computer Science**, vol 12542. Springer, Cham. (2021)
(DOI:10.1007/978-3-030-68869-1_8)

15. M. Borello, F. Dalla Volta and G. Zini, *The Möbius function of* $\mathrm{PSL}(3, 2^p)$ *for any prime* p, **International Journal of Algebra and Computation**, 31(6): 9871011 (2021)
(DOI:10.1142/S0218196721400014)
16. M. Borello, J. de la Cruz and W. Willems, *On checkable codes in group algebras*, **Journal of Algebra and its Applications**, 21(6): 2250125 (2022)
(DOI:10.1142/S0219498822501250)
17. M. Borello, C. Güneri, E. Saçıkara and P. Solé, *The concatenated structure of quasi-abelian codes*, **Designs, Codes and Cryptography** 90(11): 2647–2661 (2022)
(DOI:10.1007/s10623-021-00921-4)
18. M. Borello and P. Solé, *The uncertainty principle over finite fields*, **Discrete Mathematics** 345: 112670 (2022)
(DOI:10.1016/j.disc.2021.112670)
19. G.N. Alfarano, M. Borello and A. Neri, *A geometric characterization of minimal codes and their asymptotic performance*, **Advances in Mathematics of Communications**, 16(1): 115133 (2022)
(DOI:10.3934/amc.2020104)
20. G.N. Alfarano, M. Borello, A. Neri and A. Ravagnani, *Three combinatorial perspectives on minimal codes*, **SIAM Journal on Discrete Mathematics** 36(1): 461–489 (2022)
(DOI:10.1137/21M1391493)
21. M. Borello, F. Dalla Volta and G. Zini, *The Möbius function for finite groups and some related topics*, in **Algebra for Cryptography**, Collectio Ciphrarum (2021).
22. G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani, *Linear cutting blocking sets and minimal codes in the rank metric*, **Journal of Combinatorial Theory, Series A** 192: 105658 (2022)
(DOI:10.1016/j.jcta.2022.105658)
23. M. Borello and W. Willems, *On the algebraic structure of quasi group codes*, **Journal of Algebra and its Applications**, 2350222 (2022)
(DOI:10.1142/S0219498823502225)
24. M. Borello, W. Willems and G. Zini, *On ideals in group algebras: an uncertainty principle and the Schur product*, **Forum Mathematicum** 34(5): 1345–1354 (2022)
(DOI:10.1515/forum-2022-0064)
25. D. Bartoli and M. Borello, *Small strong blocking sets by concatenation*, **SIAM Journal on Discrete Mathematics** 37(1): 65–82 (2023)
(DOI:10.1137/21M145032)

Preprints:

1. M. Bonini, M. Borello and E. Byrne, *Saturating systems and rank covering radius*, preprint (`https://arxiv.org/pdf/2206.14740.pdf`)
2. M. Borello, P. Santonastaso and F. Zullo, *Left ideal LRPC codes and a ROLLO-type cryptosystem based on group algebras*, preprint, (`https://arxiv.org/pdf/2210.11774.pdf`)
3. A. Behajaina, M. Borello, J. de la Cruz and W. Willems, *Twisted skew G-codes*, preprint (`https://arxiv.org/pdf/2212.13190.pdf`)
4. G.N. Alfarano, M. Borello and A. Neri, *Outer strong blocking sets*, preprint (`https://arxiv.org/pdf/2301.09590.pdf`)

5. M. Borello and F. Zullo, *Geometric dual and sum-rank minimal codes*, preprint (`https://arxiv.org/pdf/2303.07288.pdf`)

Informative papers:

- M. Borello, *Medaglie Fields 2014 - Storie di matematici esemplari*, EMMECI-quadro 55, December 2014

REVIEWER

Reviewer for: Advances in Mathematics of Communication – Applicable Algebra in Engineering, Communication and Computing – Ars Mathematica Contemporanea – Designs, Codes and Cryptography – Discrete Mathematics – Finite Fields and Their Applications – IEEE Transactions on Information Theory – International Journal of Algebra and Computation – Journal of Algebra – Journal of Algebra and its Applications – Journal of Combinatorial Theory, Series A – Journal of Number Theory – **MathSciNet (8 reviews)**

Reviewer of an application for the **National Research Foundation of South Africa** (2019) and for the **Estonian Research Council** (2021).

Member of the examining committee of the PhD thesis defense of

- E. Saçıkara (Sabancı University - July 2018)
- M. Bonini (University of Trento - February 2019)

Referee for the PhD thesis of M. Bonini.

ORGANIZATION

Organizer of the session **Algebraic coding theory and cryptography** within the 29th Nordic Congress of Mathematicians with EMS — July 2023
`https://www.math.univ-paris13.fr/~borello/NCM29-actc`

Member of the **local organizing committee** of Fq15 — June 2023
`https://org.uib.no/selmer/fq15/`

Member of the program committee of

- WCC 2019, `www.lebesgue.fr/en/content/sem2019-WCC-Presentation`
- WCC 2022, `www.wcc2022.uni-rostock.de/home/`
- IWSDA 2022, `https://iwsda2022.github.io/`
- C2SI-2023, `http://www.c2si-conference.org/`

Organizer of the "Séminaire Mathématiques Discrètes, Codes et Cryptographie" — 2018 - present
`www.math.univ-paris13.fr/laga/index.php/fr/agc3/seminaires`
Université de Paris 8, Saint-Denis, France

Organizer of the "Séminaire Protection de l'information" — 2017 - 2018
Université de Paris 8, Saint-Denis, France

Co–organizer of a working seminar on Bruhat-Tits buildings — 2015 - 2016
EPFL, Lausanne, Switerland

Co–organizer of the "Séminaire d'Algèbre et de Théorie des Nombres" — 2015-2016
EPFL, Lausanne, Switerland

EDITORSHIP

Guest Editor of the Special Issue *Algebraic and Geometric Perspectives on Coding Theory* of **Advances in Mathematics of Communications**

ADMINISTRATIVE EXPERIENCE

Chairman of the selection board for a *maître de conférences* position in Mathematics for cryptography, at Université de Paris 8, Saint-Denis, France — 2020

Member of the *Conseil de perfectionnement de la Licence* — 2019 - present
Department of Mathematics, Université de Paris 8, Saint-Denis, France

Responsible for the 2nd year of the **Bachelor of Mathematics** — 2019 - present
Department of Mathematics, Université de Paris 8, Saint-Denis, France

Member of the *commission d'examen des voeux de la licence Mathématiques* — 2019
Department of Mathematics, Université de Paris 8, Saint-Denis, France

Member of the Bachelor Committee (*Jury de la Licence*) — 2018 - present
Department of Mathematics, Université de Paris 8, Saint-Denis, France

Member of the Advisory Committee (*Comité Consultatif*) — 2018 - present
Department of Mathematics, Université de Paris 8, Saint-Denis, France

INVITED LECTURES

At conferences:

1. *On the Euclidean minimum of number fields*, XMaths 2015, Bari, Italy
2. *Symmetries of weight enumerators*, BunnyTN 2016, Trento, Italy
3. *Actions de groupes en thorie des codes*, Journe du LAGA 2017, Villetaneuse, France
4. *L'erreur dans la transmission d'informations numériques, comment la corriger?*, Colloque CLI 2017, Saint-Denis, France
5. *Représenter pour mieux comprendre : exemples en mathématiques*, Colloque CLI 2018, Saint-Denis, France
6. *Codes with symmetries*, The Second Colombian Workshop on Coding Theory (CWC 2019), Barranquilla, Colombia
7. *Algebraic properties of codes with symmetries*, Minisymposium in Coding Theory and Cryptography within the SIAM AG 2019, Bern, Switzerland
8. *On short Minimal Codes and related Combinatorial Structures*, Special session "Finite Groups and Combinatorial Structures" in the 64th congress of the South African Mathematical Society (SAMS), 2021, South Africa
9. *Geometric Dual and Sum-Rank Minimal Codes*, Minisymposium in Coding theory and Galois geometries within the SIAM AG 2023, Eindhoven, Netherlands

Seminars:

1. *On the search of extremal self-dual codes of length* 72, Magdeburg, Germany, December 6^{th} 2011
2. *The automorphism group of an extremal* $[72, 36, 16]$ *code does not contain elements of order* 6, Magdeburg, Germany, May 8^{th} 2012
3. *On the automorphism group of an extremal self-dual code of length* 72, Trento, Italy, August 10^{th} 2012
4. *On the automorphism group of extremal self-dual codes*, Trento, Italy, August 1^{st} 2013

5. *Automorphisms of self-dual binary linear codes*, EPFL Lausanne, Switzerland, November 14^{th} 2013
6. *Automorphisms of self-dual binary linear codes*, Leibniz Universität Hannover, Germany, November 20^{th} 2013
7. *New bounds for semi self-dual codes*, Milano-Bicocca, Milan, December 19^{th} 2013
8. *Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length* 72, Université de Neuchâtel, Switzerland, April 7^{th} 2014
9. *On the stabilizer of weight enumerators of linear codes*, Université de Neuchâtel, Switzerland, December 2^{nd} 2015
10. *Symmetries of weight enumerators*, Università degli Studi di Milano–Bicocca, Italy, January 13^{th} 2017
11. *Symétries de polynômes énumérateurs*, Université de Paris 8, France, April 6^{th} 2017
12. *New perspective on group codes*, Séminaire Géométrie et algèbre effectives, IRMAR Rennes, France, November 29^{th} 2019
13. *Asymptotic Performance of G-codes and Uncertainty Principle*, GT Equipe GRACE, École Polytechnique, France, November 24^{th} 2020
14. *Asymptotic Performance of G-codes and Uncertainty Principle*, Arbeitsgemeinschaft in Codierungstheorie und Kryptographie, University of Zurich, Switzerland, December 16^{th} 2020
15. *Small strong blocking sets and their coding theoretical counterparts*, Galois Geometries and their Applications, Università degli Studi della Campania "Luigi Vanvitelli", Italy, February 1^{st} 2022
16. *Il principio di indeterminazione dal punto di vista della teoria dei codici*, Seminario congiunto UMI, Gruppo Crittografia e Codici, Italy, March 2^{nd} 2022
17. *Le principe d'incertitude du point de vue la théorie des codes*, Séminaire de Théorie des Nombres, Institut de Mathématiques de Toulouse, France, March 17^{th} 2022
18. *Codes et combinatoire additive*, Retraite de l'ANR Barracuda, Métabief, France, June 27^{th} 2022

TALKS & POSTERS

1. *Ricerca di codici estremali autoduali di lunghezza* 72, Terzo workshop di crittografia BunnyTn 2011, Trento, Italy, March 12^{th} 2012
2. Poster *The automorphism group of an extremal* $[72, 36, 16]$ *code does not contain elements of order* 6, Ischia group Theory 2012, Ischia, Italy, 26-29 March 2012
3. *On the automorphisms of order* $2p$ *in binary self-dual extremal codes with an application to the remarkable case of length* 72, Trends in coding theory, Ascona, Switzerland, October 29^{th} 2012
4. *Automorphisms of extremal codes*, GTG-Gruppen und Topologische Gruppen 2012, Milan, Italy, January 26^{th} 2013
5. *Automorphisms of extremal self-dual codes*, Advances in Group Theory and Applications 2013, Porto Cesareo, Italy, June 6^{th} 2013

6. *Automorphisms of extremal self-dual binary linear codes*, The 11th International Conference on Finite Fields and their Applications, Magdeburg, Germany, July 22^{nd} 2013
7. *Symmetries of weight enumerators*, The 13th International Conference on Finite Fields and their Applications, Gaeta, Italy, June 6^{th} 2017
8. *An analogue of Gleasons theorem for binary Reed-Muller codes*, Combinatorics 2018, Arco, Italy, June 4^{th} 2018
9. *Checkable codes and their asymptotic performance*, NCRA VI, Lens, France, June 25^{th} 2019
10. *Dihedral codes with prescribed minimum distance*, WAIFI 2020, Rennes, France, July 7^{th} 2020
11. *On short minimal codes and related combinatorial structures*, Cryptography and Coding Theory (1st conference UMI), Italy, September 21^{st} 2021
12. *Small strong blocking sets by concatenation*, Combinatorics 2022, Italy, June 2^{nd} 2022

TEACHING EXPERIENCE

Invited lecturer June 2021
Algebraic Coding Theory e-Summer School - ACT21
University of Zurich, Switzerland
- Course of "A coding theoretical perspective on ideals in group algebras" (3 hours - **PhD and junior researchers**)

Associate professor September 2016 - present
Université de Paris 8, Saint-Denis, France
AY 2022-2023 (165 hours)
- Course of "Coding theory 1" (30 hours - **grad**)
- Course of "Graph theory and combinatorics" (30 hours - undergrad)
- Course of "Interactions codes/cryptography" (30 hours - **grad**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Linear Algebra II" (30 hours - undergrad)
- Course of "Tremplin Master" (15 hours - undergrad)

AY 2021-2022 (165 hours)
- Course of "Coding theory 1" (30 hours - **grad**)
- Course of "Graph theory and combinatorics" (30 hours - undergrad)
- Course of "Interactions codes/cryptography" (30 hours - **grad**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Linear Algebra II" (30 hours - undergrad)
- Course of "Tremplin Master" (15 hours - undergrad)

AY 2020-2021 (165 hours)
- Course of "Coding theory 1" (30 hours - **grad**)
- Course of "Graph theory and combinatorics" (30 hours - undergrad)
- Course of "Interactions codes/cryptography" (30 hours - **grad**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Linear Algebra II" (30 hours - undergrad)
- Course of "Tremplin Master" (15 hours - undergrad)

AY 2019-2020 (165 hours)

- Course of "Interactions codes/cryptography" (30 hours - **grad**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Algebra II" (30 hours - undergrad)
- Course of "Combinatorics" (30 hours - undergrad)
- Course of "Coding theory 1" (30 hours - **grad**)
- Cours of "Algebra III" (15 hours - undergrad)

AY 2018-2019 (165 hours)

- Course of "Information Theory" (30 hours - **grad**)
- Course of "Interactions codes/cryptography" (30 hours - **grad**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Combinatorics" (15 hours - undergrad)
- Course of "Coding theory 1" (30 hours - **grad**)
- Cours of "Algebra III" (30 hours - undergrad)

AY 2017-2018 (150 hours)

- Course of "Information Theory" (30 hours - **grad**)
- Course of "Interactions codes/cryptography" (30 hours - **grad and Ph.D.**)
- Course of "Introduction to coding theory" (30 hours - undergrad)
- Course of "Combinatorics" (30 hours - undergrad)
- Course of "Coding theory 1" (30 hours - **grad**)

AY 2016-2017 (120 hours)

- Course of "Information Theory" (30 hours - **grad**)
- Course of "Algorithms for cryptography" (30 hours - **grad**)
- Course of "Geometry" (30 hours - undergrad)
- Course of "Combinatorics" (30 hours - undergrad)

Teaching Assistant September 2014 - August 2016
EPFL, Lausanne, Switzerland
AY 2015-2016

- Exercises of "Group Theory" (24 hours - undergrad)
- Exercises of "Rings and Fields" (24 hours - undergrad)

AY 2014-2015

- Exercises of "Algebra I and II" (48 hours - undergrad)

Teaching Assistant January 2011 - August 2014
Università degli studi di Milano-Bicocca, Milan, MI, Italy
AY 2013-2014

- Exercises of "Principles of Mathematics" (16 hours - undergrad)
- Tutoring of "Recalls of Mathematics"(45 hours - undergrad)

AY 2012-2013

- Exercises of "Algebraic methods for computer science" (24 hours - undergrad)
- Tutoring of "Recalls of Mathematics"(30 hours - undergrad)

AY 2011-2012

- Tutoring of "Fundamentals of Mathematics" (20 hours - undergrad)

Tutor – Laboratory of Cryptography March 2014
Istituto Santa Dorotea, Arcore
Basic lectures of cryptography and elementary number theory (10 hours)

Tutor of Mathematics June 2010 - February 2014
Camplus (University College), Milan
Tutoring to freshmen of engineering and architecture (more than 40 hours)

Tutor – Laboratory of Cryptography March 2013
I.I.S. Greppi, Monticello
Basic lectures of cryptography and elementary number theory (6 hours)

Tutor – Laboratory of Cryptography February 2013
Liceo Scientifico Cremona, Milan
Basic lectures of cryptography (6 hours)

Teacher of Mathematics Summer 2009
Liceo Scientifico Donatelli-Pascal, Milan
Remedial courses for high school students (20 hours)

SUPERVISIONS Supervisions of **1 Ph.D. thesis**, **10 Master projects** and **15 semester projects**:

Ph.D. thesis of M. Scotti October 2022-present
Interactions between coding theory and additive combinatorics
with W. Schmid

Master project of M. Scotti Spring 2022
Interactions between coding theory and additive combinatorics
with W. Schmid

Master project of Salvatore Caruso Spring 2021
Codici LCD: struttura e applicazioni
with F. Dalla Volta and I. Cascudo (at Università degli Studi di Milano-Bicocca)

Semester Project (Master) of O. El-Ouahhaj Spring 2021
Le principe d'incertitude des corps finis

Semester Project (Master) of D.-Q. Nguyen Spring 2021
Codes sur $\mathbb{Z}/4\mathbb{Z}$

Semester Project (Master) of B. Cissokho Spring 2021
Quadratic residue codes

Master Project of C. Halima Spring 2021
Secure implementation of designing a public key cryptosystem based on quasi-cyclic subspace subcodes of Reed-Solomon codes
with G.N. Dione (at Université Cheikh Anta Diop, Dakar)

Master Project of K. Lairedj Spring 2021
Interpolation d'Hermite et codes correcteurs
with E. Guerrini and R. Lebreton (at LIRMM, Montpellier)

Master Project of S. Majbour — Spring 2021
Etude des conséquences des biais des statistiques sur la sécurité du schéma dauthentification Fuzzy vault
with M. Barbier and J.-M. Le Bars (at GREYC, Caen)

Semester Project (Master) of O. Perrin — Spring 2020
Raptor codes

Master Project of S. Grib — Spring 2020
La biométrie basée sur la théorie des codes
with M. Barbier and J.-M. Le Bars (at GREYC, Caen)

Master Project of L. Demange — Spring 2020
Implémentation optimisée de schémas de signature post-quantiques
with T. Ricosset (at Thales)

Master Project of Y. Ameur — Spring 2019
Side channel attack sur un cryptosystème post-quantique
with A. Heuser (at IRISA Rennes)

Master Project of S. Azzoug — Spring 2019
Délivrance de certificat numérique et authentification
with L. Saidat (at BNP Paribas)

Semester Project (Master) of S. Grib and H. Tazaïrt — Spring 2019
Les bornes des codes correcteurs

Semester Project (Master) of O. Diankha — Spring 2018
Les codes en métrique rang

Semester Project (Master) of A. Ouhadj — Spring 2018
Protocole d'authentification de Schnorr

Semester Project (Master) of Z. Haddad and T. Benbouabdellah — Spring 2017
Fonctions de hachage

Semester Project (Master) of I. Benabed and M.H. Benyahia — Spring 2017
Algorithmes de signature numérique

Semester Project (Master) of A. Kerfi and T. Messous — Spring 2017
Attaques contre le cryptosystème RSA

Semester Project (Master) of S. Dehl and S. Hamel — Spring 2017
Chaînes de blocs et bitcoins

Semester Project (Master) of R. Issaad — Spring 2017
Entropie de la langue française

Semester Project (Bachelor) of Quentin Levêque, — Spring 2016
Sur les groupes simples
with Prof. Eva Bayer-Fluckiger

Semester Project (Bachelor) of Filip Fifka, — Autumn 2015
Ideal Class Group
with Prof. Eva Bayer-Fluckiger

Master project of Olivier Mila, — Spring 2015
Invariance for weight enumerators of evaluation codes and counting $\mathbb{F}_q$-rational points on hypersurfaces

with Prof. Eva Bayer-Fluckiger

Semester Project (Master) of Alessandro Slamitz, Autumn 2014
Inverse Galois Problem: Intersective Polynomials
with Prof. Eva Bayer-Fluckiger

LANGUAGE SKILLS

Italian: mother tongue
English: fluent, written and spoken
French: fluent, written and spoken
German: elementary (A1)