Europass Curriculum Vitae

Personal information

Name / Surname	**Calderini, Marco**
Date of birth	

Position held

September 2017 - present	Senior Researcher (Forsker II, SKO 1109)
Name of employer	Department of Informatics, University of Bergen
Occupation or position held	Researcher
Main activities and responsibilities	Interdisciplinary research in mathematics and information theory, combining computational and mathematical methods, for constructing Boolean functions with optimal resistance to various cryptographic attacks. Co-supervision of the research of two Ph.D. students.
September 2016 - September 2017	Postdoctoral Fellow
Name of employer	Department of Mathematics, University of Trento
Occupation or position held	Postdoctoral researcher
Main activities and responsibilities	Mathematical analysis of existent cryptographic systems for protecting financial transactions; study of new algorithms for the management of Mobile Payment such that the communication with the BANCOMAT network and the e-payment server would be cryptographically secure; supervision of the research of a young researchers team.
June 2015 - June 2016	Postdoctoral Fellow
Name of employer	Department of Mathematics, University of Trento
Occupation or position held	Postdoctoral researcher
Main activities and responsibilities	Detailed evaluation of the safety system, based on elliptic curve cryptography (ECC), proposed by IDQ. In particular, to analyze from a mathematical point of view the cryptographic robustness of the curve chosen by IDQ.

Education and training

November 2011 - April 2015	Ph.D in Mathematics
Name of the University or institution, place	University of Trento
Main subjects, skills	Cryptography, Information theory, Coding theory. Graduation thesis title:“On Boolean functions, symmetric cryptography and algebraic coding theory”, supervisor: Massimiliano Sala
Status/certificate obtained	Doctor of Philosophy in Mathematics
October 2009 - July 2011	Master’s Degree in Mathematics (named: Corso di Laurea Magistrale in Matematica, indirizzo Applicato)
Name of the University or institution, place	University of Perugia
Main subjects, skills	Mathematical analysis, Numerical analysis, Differential geometry, Algebraic geometry, Combinatorial geometry, Algebra, Topology. Graduation thesis in Coding theory, title: “Generalized algebraic-geometry codes from maximal curves”, supervisor: Massimo Giulietti
Status/certificate obtained	Master’s Degree in Mathematics

Grade	110/110 cum laude
October 2004 - July 2009	Bachelor's Degree in Mathematics (named: Corso di Laurea Triennale in Matematica per le Applicazioni, indirizzo Matematica per le Applicazioni a Teoria delle Informazioni, Codici e Crittografia)
Name of the University or institution, place	University of Perugia
Main subjects, skills	Mathematical analysis, Numerical analysis, Algebraic geometry, Combinatorial geometry, Algebra, Informatics, Coding theory, Information theory, Cryptography. Graduation thesis in Topology, title: "Weakly continuous relations and representation theorems", supervisor: Alessandro Caterino
Status/certificate obtained	Bachelor's Degree in Mathematics

Research interest

My research activity is mainly in the field of finite permutation groups and discrete functions in relation to their applications to coding theory and cryptography.

Publications

Journals

[1] M. Calderini, R. Civino, M. Sala, "On properties of translation groups in the affine general linear group with applications to cryptography", J. Algebra, https://doi.org/10.1016/j.jalgebra.2020.10.034, 2021

[2] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter and I. Villa, "Generalized Isotopic Shift Construction for APN Functions", Designs Codes and Cryptography, https://doi.org/10.1007/s10623-020-00807-x, 2020

[3] M. Calderini, "Differentially low uniform permutations from known 4-uniform functions", Designs Codes and Cryptography, https://doi.org/10.1007/s10623-020-00807-x, 2020

[4] L. Budaghyan, M. Calderini and I. Villa, "On equivalence between known families of quadratic APN functions", Finite Fields and their Applications, 66, https://doi.org/10.1016/j.ffa.2020.101704, 2020.

[5] M. Calderini and I. Villa, "On the Boomerang Uniformity of some Permutation Polynomials", Cryptography and Communications, 12, 1161?1178 https://doi.org/10.1007/s12095-020-00439-x, 2020

[6] R. Aragona, M. Calderini, R. Civino, "Some group-theoretical results on Feistel Networks in a long-key scenario". Advances in Mathematics of Communications 14(4) : 727-743, doi: 10.3934/amc.2020093, 2020.

[7] M. Calderini, "On the EA-classes of known APN functions in small dimensions", Cryptography and Communications, 12(5), 821-840 https://doi.org/10.1007/s12095-020-00427-1, 2020.

[8] M. Calderini, "Primitivity of the group of a cipher involving the action of the key-schedule", Journal of Algebra and its Applications, DOI: 10.1142/S0219498821500845, 2020

[9] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter and I. Villa, "Constructing APN functions through isotopic shifts", IEEE Transactions on information theory, 66(8) pp. 5299 - 5309, DOI: 10.1109/TIT.2020.2974471, 2020

[10] L. Budaghyan, M. Calderini, and I. Villa, "On relations between CCZ- and EA-equivalences", Cryptography and Communications, doi:10.1007/s12095-019-00367-5, 2019

[11] R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, "Wave-Shaped Round Functions and Primitive Groups", Advances in Mathematics of Communications 13(1), 2019.

[12] C. Brunetta, M. Calderini, M. Sala, "On hidden sums compatible with a given block cipher diffusion layer", Discrete Mathematics 342(2), 373-386, 2018.

[13] M. Calderini, “A note on some algebraic trapdoors for block ciphers”, in Advances in Mathematics of Communications, Vol. 12, No. 3, pp. 515–524, doi:10.3934/amc.2018030, 2018.

[14] R. Aragona, M. Calderini, A. Tortora, M. Tota, “Primitivity of PRESENT and other lightweight ciphers”, Journal of Algebra and Its Applications, https://doi.org/10.1142/S0219498818501153 (arXiv:1611.01346), 2018.

[15] E. Byrne, and M. Calderini, “Bounding the optimal rate of the ICSI and ICCSI problem”, SIAM J. Discrete Math., 31(2), 1403–1427, 2017.

[16] M. Calderini, M. Sala, and I. Villa. "A note on APN permutations in even dimension." Finite Fields and Their Applications July 2017, Vol.46:1–16, 2017.

[17] E. Byrne, and M. Calderini, “Error Correction for Index Coding with Coded Side Information”,IEEE Transactions on Information Theory Volume: 63, Issue: 6, 3712 - 3728, 2017.

[18] R. Aragona, M. Calderini, D. Maccauro and M. Sala “On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion”, Applicable Algebra in Engineering, Communication and Computing, 27(5), 359-372, 2016.

[19] M. Calderini, and G. Faina. “Generalized Algebraic Geometric Codes From Maximal Curves” Information Theory, IEEE Transactions on 58.4 : 2386-2396, 2012.

Conference Proceedings (Refereed)

[20] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, “A note on the Walsh spectrum of Dobbertin APN functions”, proceedings SETA2020, Saint-Petersburg, Russia, 2020

[21] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, “On a Relationship between Gold and Kasami Functions and other Power APN Functions”, proceedings SETA2020, Saint-Petersburg, Russia, 2020

[22] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter and I. Villa, “On Isotopic Shift Construction for Planar Functions”, 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 2962-2966. doi: 10.1109/ISIT.2019.8849339

[23] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter and I. Villa, “Generalized Isotopic Shift of Gold Functions”, proceedings WCC2019, France

[24] L. Budaghyan, M. Calderini and I. Villa, “On equivalence between some families of APN functions”, proceedings WCC2019, France

[25] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter and I. Villa, “Constructing APN functions through isotopic shifts”, proceedings SETA2018, Hong Kong

[26] C. Brunetta, M. Calderini, M. Sala, “Hidden sums and their application on block ciphers", proceedings WCC 2017, Russia.

[27] M. Calderini, and M. Sala. "On Differential Uniformity of Maps that May Hide an Algebraic Trapdoor." In: Maletti A. (eds) Algebraic Informatics. CAI 2015. Lecture Notes in Computer Science, vol 9270. Springer, doi:10.1007/978-3-319-23021-4_7.

[28] M. Calderini, and M. Sala. “Generalized AG codes as evaluation codes.” In: Muntean T., Poulakis D., Rolland R. (eds) Algebraic Informatics. CAI 2013. Lecture Notes in Computer Science, vol 8080. Springer, doi:10.1007/978-3-642-40663-8_8.

Book chapters

[29] E. Byrne, and M. Calderini, “Index Coding, Network Coding and Broadcast with Side-Information”, in N.Silberstein, A. Vazquez-Castro, M. Pavcevic, and M. Greferath, “Network Coding and Subspace Designs”, Springer, 2018.

Preprints

[30] M. Calderini, L. Budaghyan, C. Carlet, “On known constructions of APN and AB functions and their relation to each other", ePrint Archive: Report 2020/1444, 2020

[31] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, “On two fundamental problems on APN power functions”, ePrint Archive: Report 2020/1359, submitted to IEEE Transactions on Information Theory, 2020

[32] D. Bartoli, M. Calderini, “On construction and (non)existence of c-(almost) perfect non-linear functions”, arXiv:2008.03953, submitted to Finite Fields and their Applications, 2020

Invited talks

10 October 2019 “On vectorial Boolean functions with low differential and boomerang uniformity” - 1st Workshop on Algebra for Cryptography (A4C 2019), L’Aquila (IT)

18 June 2019 “Investigating the EA-classes of known APN functions” - 4th International Workshop on Boolean Functions and their Applications (BFA), Florence (IT)

18 June 2018 “On relations between CCZ and EA-equivalence” - The 3rd International Workshop on Boolean Functions and their Applications (BFA), Loen (Norway)

4 July 2017 “APN permutations” - The 2nd International Workshop on Boolean Functions and their Applications (BFA), Os (Norway)

8 March 2017 “Curve ellittiche crittograficamente robuste per la generazione di moneta elettronica” - Applicazioni della crittografia nel mondo aziendale, Department of Mathematics and Computer Science, University of Perugia (Italy)

10 January 2017 “The Role of Boolean Functions in some Algebraic Trapdoors” - Department of Informatics, University of Bergen, Bergen (Norway)

14 October 2014 “Index coding” - Miniworkshop: CodingTheory and Cryptography, University of Torino, Torino (Italy)

21 October 2013 “Index Codes from t-designs” - Arbeitsgemeinschaft in Codierungstheorie und Kryptographie, University of Neuchatel, Neuchatel (Swiss)

22 May 2013 “Network coding problem - An introduction” - Workshop BunnyTN 4, University of Trento, Trento (Italy)

Contributed talks

17 September 2020 “Differentially low uniform permutations from the Gold and Bracken-Leander functions”, BFA 2020, Norway

2 April 2019 “Generalized Isotopic Shift of Gold Functions”, WCC 2019, France

2 April 2019 “On equivalence between some families of APN functions”, WCC 2019, France

20 September 2017 “Hidden sums and their application on block ciphers” - Tenth International Workshop on Coding and Cryptography 2017, Saint-Petersburg (Russia)

5 April 2016 “Bounding the optimal rate of the ICCSI problem” - Network Coding and Designs, Centre for Advanced Academic Studies, Dubrovnik (Croatia)

6 September 2015 “On differential uniformity of maps that may hide an algebraic trapdoor” - 6th International Conference on Algebraic Informatics, University of Stuttgart, Stuttgart (Germany)

4 June 2014 “Index codes and designs” - Combinatorics 2014, Gaeta (Italia)

18th September 2013 “Error Correction for Index Coding” - Conference on Random network codes and Designs over GF(q), Ghent (Belgium)

4th September 2013 “Generalized AG codes as Evaluation codes” - 5th International Conference on Algebraic Informatics, Porquerolles (France)

12th March 2012 “Generalized AG-codes from maximal curves” - Workshop on cryptography: BunnyTN 2012, University ofTrento, Trento (Italia)

Conferences and Workshops attended

15 - 17 September 2020 5th International Workshop on Boolean Functions and their Applications (BFA 2020), Loen (NO)

6 - 8 July 2020 International Workshop on the Arithmetic of Finite Fields (A4C 2019), Rennes (FR)

10 - 11 October 2019 1st Workshop on Algebra for Cryptography (WAIFI 2020), L’Aquila (IT)

16 - 21 June 2019 4th International Workshop on Boolean Functions and their Applications (BFA 2019), Florence (Italy)

31 March - 4 April 2019 11th International Workshop on Coding and Cryptography 2019, WCC 2019, France

17 - 22 June 2018	3rd International Workshop on Boolean Functions and their Applications (BFA), Loen (Norway)
14 - 16 June 2018	International Workshop on the Arithmetic of Finite Fields - WAIFI 2018, Bergen (Norway)
4 - 8 September 2017	Mathematical Methods for Cryptography, Svolvaer (Norway)
3 - 8 July 2017	The 2nd International Workshop on Boolean Functions and their Applications (BFA 2017), Os (Norway)
4 - 9 April 2016	"Network Coding and Designs", Centre for Advanced Academic Studies, Dubrovnik (Croatia)
2 - 6 September 2015	"6th International Conference on Algebraic Informatics", University of Stuttgart, Stuttgart (Germany)
15 - 19 June 2015	"MEGA 2015: Effective Methods in Algebraic Geometry", University of Trento, Trento (Italy)
13 - 17 April 2015	"The Ninth International Workshop on Coding and Cryptography 2015 ", Paris, (France)
13 - 14 October 2014	"Miniworkshop: CodingTheory and Cryptography", University of Torino, Torino (Italy)
2 - 6 june 2014	"Combinatorics 2014", Gaeta (Italy)
21 October 2013	Workshop:"Arbeitsgemeinschaft in Codierungstheorie und Kryptographie", University Neuchatel, Neuchatel (Swiss)
18 - 21 September 2013	"Conference on Random network codes and Designs over GF(q)", Ghent (Belgium)
3 - 6 September 2013	"5th International Conference on Algebraic Informatics", Porquerolles (France)
20 - 21 June 2013	"Zurich COST Meeting - Random Network Coding and Designs over GF(q)", University of Zurich, Zurich (Swiss)
4 - 8 February 2013	"First European Training School in Network Coding", Universidad autonoma de Barcelona, Barcelona (Spain)
9 -15 September 2012	"Combinatorics 2012", University of Perugia, Perugia (Italy))
30 July - 10 August 2012	"Ph.D. School: Groebner Bases, Curves, Codes and Cryptography", University of Trento, Trento (Italy)
28 May - 1st June 2012	"ECRYPT II Summer School on Tools", Mykonos (Greek)
19 - 30 March 2012	"Ph.D. School: Boolean functions and their applications to cryptography", University of Trento, Trento (Italy))
12 March 2012	"Workshop on cryptography: BunnyTN 2012", University of Trento, Trento (Italy)

Projects in which I have been involved

April 2015- September 2017	I was a member of the "Laboratorio di Matematica Industriale e Crittografia" of the University of Trento, supervised by Prof. Massimiliano Sala. The objectives of the laboratory were: (1) research activity in the field of Algebra applied to Cryptography and Coding Theory; (2) tutoring for the Master's students of the curricula "Coding Theory and Cryptography"; (3) consulting/analysis activities for project funded by private companies, such as evaluation of the security of protocols and cryptographic algorithms.
January 2013 - April 2016	I was involved in the COST Action IC1104 "Random Network Coding and Designs Over GF(q)". I have also spent 3 months at the University College Dublin for a Short-Term Scientific Missions (STSM) linked to the the COST Action.
September 2017 - present	I am currently a key member of the Selmer center (University of Bergen) in the 4-years project "Constructions of Optimal Boolean Functions", funded by the Bergen Research Foundation. PI: Dr. habil. Lilya Budaghyan. 23MNOK (∼ 2 million Euro), period 01/04/2017–31/03/2021.
February 2019 - present	I am involved in the project of Russia Program at Norwegian Center for International Cooperation in Education "Development of a new joint educational program in Information Security and Cryptography at the UiB and Novosibirsk State University" with N.Tokareva for period 02.2019–02.2021 (0.3 MNOK).

Grants

Travel grant from Meltzer Research Fund to maintain cooperation of scientific groups in Bergen and L'Aquila for period 06.2019–06.2020.

(Co-)Supervised Theses

February 2015	MSc thesis: Marco Iavernaro,“On some cryptographic properties of vectorial Boolean functions”, advisor: Massimiliano Sala.
October 2015	MSc thesis: Irene Villa, “On vectorial Boolean functions in even dimension”, advisor: Massimiliano Sala.
March 2016	MSc thesis: Francesco Devito,“An application of Edwards elliptic curves to Ripple protocol”, advisor: Massimiliano Sala.
July 2016	MSc thesis: Carlo Brunetta,“On some computational aspects for hidden sums in Boolean functions”, advisor: Massimiliano Sala.
October 2016	MSc thesis: Roberto Roscino,“XMSS^T , a post-quantum signature for the QKD’s public channel authentication”, advisor: Massimiliano Sala.
February 2017	MSc thesis: Ilaria Zappatore,“On the primitivity of generalized translation based ciphers”, advisor: Massimiliano Sala.
October 2017	MSc thesis: Marco Zaninelli,“On cryptographic properties of cubic Boolean functions”, advisor: Massimiliano Sala.

(Co-)Supervised Ph.D.

September 2017 - January 2021	Irene Villa: “On the construction and the analysis of families of optimal Boolean functions". Supervisor: Prof. Lilya Budaghyan
September 2017 - September 2021	Nikolay Stoyanov Kaleyski: “On the classification and construction of almost perfect linear functions". Supervisor: Prof. Lilya Budaghyan. To be defended in September 2021.

Organization of international conferences

September 2021	Member of the Program and Organizing Committee for the “6th International Workshop on Boolean Functions and their Applications (BFA)", Granada (Spain)
September 2020	Member of the Organizing Committee for the “5th International Workshop on Boolean Functions and their Applications (BFA)", Loen (Norway)
June 2019	Member of the Program and Organizing Committee for the “4th International Workshop on Boolean Functions and their Applications (BFA)", Florence (Italy)
June 2018	Member of the Program and Organizing Committee for the “International Workshop on the Arithmetic of Finite Fields - WAIFI 2018", Bergen (Norway
June 2018	Member of the Organizing Committee for the “3rd International Workshop on Boolean Functions and their Applications (BFA)", Loen (Norway)

Organization of Workshops

27th May 2015	Organizer for “Bitcoin and altcoins: applications and limitations", Milano (Italy)
22th December 2014	Organizer for “Cryptography Workshop BunnyTN 5", University of Trento (Italy)
22th May 2013	Organizer for “Cryptography Workshop BunnyTN 4", University of Trento (Italy)
12th March 2012	Organizer for “Cryptography Workshop BunnyTN 3", University of Trento (Italy)

Academic Teaching

between August 2018 and December 2018	Teaching for the course "Selected topics in Cryptography- INF347"
Occupation or position held	Teaching
Main activities and responsibilities	Classroom lessons/seminars
Name of employer	University of Bergen

between September 2016 and March 2017	Teaching assistant for the course "Analysis 1" of Bachelor's Degree in Information Engineering and Computer Science
Occupation or position held	Teaching assistant
Main activities and responsibilities	Lectures, classroom exercises
Name of employer	University of Trento
between March 2016 and June 2016	Teaching assistant for the course "Finite Fields" of Master's Degree in Mathematics
Occupation or position held	Teaching assistant
Main activities and responsibilities	Lectures, classroom exercises
Name of employer	University of Trento
between September 2015 and March 2016	Teaching assistant for the course "Analysis 1" of Bachelor's Degree in Information Engineering and Computer Science
Occupation or position held	Teaching assistant
Main activities and responsibilities	Lectures, classroom exercises
Name of employer	University of Trento
between March 2015 and June 2015	Teaching assistant for the course "Finite Fields" of Master's Degree in Mathematics
Occupation or position held	Teaching assistant
Main activities and responsibilities	Lectures, classroom exercises
Name of employer	University of Trento
between September 2014 and March 2015	Teaching assistant for the course "Analysis 1" of Bachelor's Degree in Information Engineering and Computer Science
Occupation or position held	Teaching assistant
Main activities and responsibilities	Lectures, classroom exercises
Name of employer	University of Trento
between March 2011 and June 2011	Teaching assistant for the course "Analysis of Numerical Methods" of Master's Degree in Mathematics
Occupation or position held	Teaching assistant
Main activities and responsibilities	Classroom exercises
Name of employer	University of Perugia

Workshops and courses for professionals

10-11 November 2016	Course: "Bitcoin, Blockchain and their new frontiers in Rome"
Occupation or position held	Assistant Lecturer
Main activities and responsibilities	Lectures
Name of employer	University of Trento
17-21 October 2016	Course: "Advance analysis of block cipher"
Occupation or position held	Assistant Lecturer
Main activities and responsibilities	Lectures
Name of employer	University of Trento

12-13 May 2016	Course: "Bitcoin, Blockchain and their new frontiers"
Occupation or position held	Assistant Lecturer
Main activities and responsibilities	Lectures
Name of employer	University of Trento
21-25 September 2015	Course: "Mathematical trapdoors in block ciphers: evaluation and attack exploitation"
Occupation or position held	Assistant Lecturer
Main activities and responsibilities	Lectures
Name of employer	University of Trento

Personal skills and competences

Mother tongue — **Italian**

Other language(s) — English, French

Self-assessment *European level*(*)	Understanding		Speaking		Writing
	Listening	Reading	Spoken interaction	Spoken production	
English	C1 Proficient user	C1 Proficient user	C1 Proficient user	C1 Proficient user	C1 Proficient user
French	A2 Basic user	A2 Basic user	A1 Basic user	A1 Basic user	A1 Basic user

(*) *Common European Framework of Reference* (CEF) level

Computer skills and competences

Operative system: OS X, MS Windows
Programming languages: C, C++
Computer Algebra System: MAGMA, Singular, Maple, MatLab, Mathematica, R
Professional typing/publication software: LaTex, Acrobat, MS Office

Qualifications

February 2020	Qualification as Maître de Conférences in Mathematics n. MFC-2020-25-20225334162
February 2020	Qualification as Maître de Conférences in Applied Mathematics n. MFC-2020-25-20226334162

Refereeing activity

Journals	IEEE Transactions on Information Theory - Applicable Algebra in Engineering, Communication and Computing - Cryptography and Communications - Journal of Cryptology - Finite Fields and their Applications - Designs Codes and Cryptography
Conferences	MEGA2015, WCC2017, SETA2018, WAFI2018, WCC2019
Others	Mathematical Reviews, Zentralblatt für Mathematik

Member of PhD Thesis Committees

22 June 2018	University of Bergen. Ph.D. candidate: Bo Sun; thesis: On Classification and Some Properties of APN Functions.

Le dichiarazioni rese nel presente curriculum sono da ritenersi rilasciate ai sensi degli artt. 46 e 47 del D.P.R. 445/2000. Il sottoscritto dichiara di aver ricevuto l'informativa sul trattamento dei dati personali.

F.to da Marco Calderini, Bergen, January 19, 2021