Curriculum vitae

Personal information

Name	**Irene Villa**
E-mail	irene1villa@gmail.com Irene.Villa@uib.no
Nationality	Italian
Date of birth	28/02/1990 – Milano (Italy)

Education

2013-2015
University of Trento – Department of Mathematics – Master Degree in Mathematics, specialization in computational algebra, cryptography and error correcting codes
Master degree awarded 23rd of October 2015 with a mark of 110/110 with honors (magna cum laude).
Graduation thesis title: “Vectorial Boolean Functions in even dimension”

2009-2013
University of Milano-Bicocca – Department of Mathematic – Bachelor Degree in Mathematics
Bachelor degree awarded 27th of March 2013 with a mark of 102/110.
Graduation thesis title: “Burnside Theorem”

Current Position

From 15th of September 2016 (4 years position)

Research Fellow at the Department of Informatics, University of Bergen (Norway)
Project title: “Optimal Boolean Functions”
Main supervisor: Prof. Lilya Budaghyan
Co-supervisors: Prof. Tor Helleseth, Dr. Marco Calderini

Activities

Teaching assistant at the Department of Informatics (University of Bergen) for the following courses:
“Information theory”, spring-semester 2017 and spring-semester 2018
“Algorithms, data structures and programming languages”, autumn-semester 2017 and autumn-semester 2018

Member of Organizing Committee of the 3rd International Conference on Boolean Functions and their Applications (BFA 2018)

Member of Organizing Committee of the 4th International Conference on Boolean Functions and their Applications (BFA 2019)

Member of Organizing Committee of the 5th International Conference on Boolean Functions and their Applications (BFA 2020)

April 2019: One month visit to Prof. Robert Coulter, University of Delaware (USA)
May 2019: One month visit to Prof. Claude Carlet, University of Paris VIII (France)

September 2019: Organiser of the Boolean function group meeting & team-building activity

Research Interests

Boolean Functions, Finite Fields, Discrete Mathematics, Algebra, Coding Theory

Languages

Italian, English and Spanish
Basic level of Norwegian

Publications

Marco Calderini, Massimiliano Sala, Irene Villa:
A note on APN permutations in even dimension (2017)
Finite Fields and Their Applications 46: 1-16

Irene Villa:
On APN functions $L_1(x^3)+L_2(x^9)$ with linear L_1 and L_2 (2018)
Cryptography and Communications. 1-18. 10.1007/s12095-018-0283-8

Lilya Budaghyan, Marco Calderini, Irene Villa:
On relations between CCZ- and EA-equivalences (2018)
Cryptography and Communications. 1-16. 10.1007/s12095-019-00367-5

Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, Irene Villa:
Constructing APN functions through isotopic shifts (2018)
Submitted to: IEEE Transaction on Information Theory

Marco Calderini, Irene Villa:
On the Boomerang Uniformity of some Permutation Polynomials (2019)
Submitted to: Cryptography and Communications

Conference proceedings

Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, Irene Villa:
On Isotopic Construction of APN Functions (2018)
Proceedings : SETA 2018 – The 10th International Conference on Sequences and their Applications

Lilya Budaghyan, Marco Calderini, Irene Villa:
On the equivalence between some families of APN functions (2018)
Proceedings: WCC 2019 – The 11th International Workshop on Coding and Cryptography

Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, Irene Villa:
Generalized Isotopic Shift of Gold Functions (2018)
Proceedings: WCC 2019 – The 11th International Workshop on Coding and Cryptography

Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, Irene Villa:
On Isotopic Shift Construction for Planar Functions (2019)
Proceedings: ISIT 2019 – IEEE International Symposium on Information Theory

Presentations at Workshops and Conferences

December 2015 – Workshop BunnyTN 6 (Trento-Italy): “Vectorial Boolean Permutations in even dimension: anti-crookedness and APN”

April 2017 – 20th FRUCT ISPIT 2017 Seminar (Saint-Petersburg, Russia): “Some Properties of APN Functions of the Form $L_1(x^3)+L_2(x^9)$, Where L_1 and L_2 Are Linear”

July 2017 – The 2nd International Workshop on Boolean Functions and their Applications (BFA) (Os, Norway): “On some properties of quadratic APN functions of a special form”

June 2018 – The 3rd International Workshop on Boolean Functions and their Applications (BFA) (Loen, Norway): “On isotopic construction of APN functions”

October 2018 – The 10th International Conference on Sequences and their Applications (SETA 2018) (Hong Kong): “On isotopic construction of APN functions”

June 2018 – The 4th International Workshop on Boolean Functions and their Applications (BFA) (Firenze, Italy): “On the boomerang uniformity of some permutation polynomials”

June 2018 – ISIT 2019 – IEEE International Symposium on Information Theory (Paris, France): “On isotopic shift construction for planar functions”

Support and Grants

Conferences and Workshops attended with funding from “*COINS Research School of Computer and Information Security*":

- Codes, Cryptology and Information Security, Second International Conference, Rabat, Morocco, 2017
- BFA 2017 workshop, Os, Norway,2017
- Mathematical Methods for Cryptography, Svolvær, Norway, 2017
- COINS Finse winter school, Finse, Norway, 2018
- Emil Artin International Conference, Yerevan, the Republic of Armenia, 2018
- BFA 2018 workshop, Loen, Norway, 2018
- COINS Ph.D. student seminar, Longyearbyen, Svalbard, Norway, 2018
- NISK 2018, Longyearbyen, Svalbard, Norway, 2018
- ECRYPT-NET School on Applied Cryptography and its Impact on Society, Innovation and Entrepreneurship, Malaga, Spain, 2019
- COINS Finse winter school, Finse, Norway, 2019
- BFA 2019 workshop, Florence, Italy, 2019

Meltzer Project Grant received: kr. 8 000 for project “*Investigation of properties for newly constructed cryptographically significant functions*”

Student Travel Grant sponsored by Région Île-de-France and Université de Cergy-Pontoise: 290 € for attending the conference ISIT 2019 in Paris, France