Curriculum vitae with track record

Personal information

First name, Surname:	Lilya Budaghyan		
Date of birth:	29.01.1976	Sex:	F
Nationality:	Norway and Armenia		
URL for personal website:	https://org.uib.no/selmer/people/lbu061/		

Education

Year	Faculty/department - University/institution - Country
2013	Habilitation (professorial) degree in Mathematics from University of Paris 8, France
2005	Ph.D. Degree in Mathematics from Otto-von-Guericke University Magdeburg, Germany (magna cum laude)
2002	Postgraduate degree from Higher Algebra and Geometry Chair, Department of Mathematics, Yerevan State University (cumulative GPA: 5.0 out of 5.0)
1998	Diploma with Honors in Mathematics of Yerevan State University (YSU), Yerevan, Armenia (summa cum laude, cumulative GPA: 4.92 out of 5.0)

Positions - current and previous

Year	Job title – Employer - Country
2019 —	Professor at Department of Informatics, University of Bergen (UoB), Norway
2012-2013	Postdoc at Department of Mathematics, Universities of Paris 8 and 13, France
2011	Sabbatical at Telecom ParisTech, Paris, France
2007-2019	Postdoc/Researcher/TMS fellow at Department of Informatics, UoB
2005-2007	Postdoc at Department of Mathematics, University of Trento, Italy
2003-2005	PhD student at Dept. of Mathematics, Otto-von-Guericke University Magdeburg
1998-2003	Research Assistant at Higher Algebra and Geometry Chair, YSU, Armenia

Project management experience

Year	Project owner - Project - Role - Funder
2021-2025	UoB - “Boolean functions and threshold implementations” - PI - Norwegian Research Council (11 MNOK); other key members: V. Rijmen and C. Carlet
2017-2021	UoB - “Optimal Boolean Functions” - PI - *Trond Mohn Foundation Recruitment Program Grant* (23.5 MNOK); other key member: C. Carlet
2019-2021	UoB - “Development of a new joint educational program in Information Security and Cryptography at the UiB and Novosibirsk State University”- PI - *Russia Program at Norwegian Center for International Cooperation in Education* (0.3 MNOK)

2014-2018	UoB - “Discrete Functions and There Applications in Cryptography and Mathematics” - PI - *“Young research talent grant” from FRITEK of Norwegian Research Council* (7 MNOK)
2017	UoB - “Development of Education in Computer Science and Applied Mathematics in Armenia” - PI - *Eurasia 2017 Project Development Funding Grant* (50 KNOK)
2012-2013	UoB - Cooperation of scientific groups in Bergen and Paris - PI - *Travel grant from Meltzer Research Fund*
2010-2014	UoB - Secure Boolean Function for Coding and Cryptography - Co-initiator and key member - *FRITEK of Norwegian Research Council* (10.1 MNOK)

Supervision

Master's students	Ph.D. students	Postdocs/Researchers	University/institution - Country
5	9 (two currently hold associate prof position; one vice-head of institute, two postdocs)	5 (all currently in academia; two hold associate prof position)	University of Bergen/ Department of Informatics - Norway

Other relevant professional experiences

Year	Description - Role
2022 —	Member of the Department of Informatics Council (Instituttsråd)
2021 —	Member of a steering group of GenderAct project at MatNat Faculty, UoB
2017 —	Leader of *the Selmer Center in Secure Communication*, Dept. of Informatics, UoB
2017 —	Leader of *Boolean Functions Research Team* at the Selmer Center
2019 —	Co-founder and member of a steering committee of *George Boole Int. Prize*
2018 —	Member of a steering committee of *WAIFI* - the Int. Workshop on the Arithmetic of Finite Fields.
2018 —	Assoc. editor of the Int. Journal *“Cryptography and Communications”* (Springer)
2017—	Elected member of *Armenian Mathematical Union*
2014 —	Co-founder and general chair of annual int. workshops in Boolean functions and Their Applications (BFA 2014, 2017, 2018, 2019, 2020, 2021, 2022)
2018	Member of Strategy Planning Commit. of Dept of Informatics (UoB) for 2019-2024
2018	General and PC co-chair of *WAIFI* 2018
2018	Co-organizer of *Emil Artin* International Conference
2017	General chair of Int. Workshop on Mathematical Methods for Cryptography *MMC*
2013	Co-chair of PC of Int. Workshop on Coding and Cryptography *WCC*
2010	Co-organizer of Workshop of *Cryptography and Security*
2009 —	Member of program committees of 14 international workshops and conferences
2016—	23 invited talks in international conferences, including Alcocrypt 2023 (France), Fq’15 (France, 2023), Africacrypt 2022 (Morocco), CECC 2020 (Croatia), etc.

Track record

- **Fellowships, awards and prizes**
  - Member of *Norwegian Academy of Technological Sciences* since 2019
  - Laureate of *2012 Postdoctoral Fellowship Award of the Foundation Sciences Mathematiques de Paris* (a network of excellence in fundamental and applied mathematics and fundamental computer science), for period 09.2012–09.2013
  - *2011 Emil Artin Junior Prize in Mathematics* for outstanding contributions in algebra, geometry and number theory
  - *Ph.D. Fellowship of the State of Saxony Anhalt*, Germany, for period 03.2003–12.2005
  - *Honorary Student Scholarship* at Yerevan State University for period 02.1994–06.1998
- **Number of citations:** 1675, **H-index in google scholar:** 21; **h-index in scopus:** 13
- **A list of 8 publications out of 70**

1. E. Piccione, S. Andreoli, L. Budaghyan, C. Carlet, S. Dhooghe, S. Nikova, G. Petrides, V. Rijmen. An Optimal Universal Construction for the Threshold Implementation of Bijective S-boxes. Submitted to *IEEE Trans. Inf. Theory*, 2022.

2. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, N. Kaleyski. "On two fundamental problems on APN power functions", *IEEE Trans. Inf. Theory,* 2022.

3. [**Award Winning**] D. Davidova, L. Budaghyan, C. Carlet, T. Helleseth, F. Ihringer, T. Penttila. Relation between o-equivalence and EA-equivalence for Niho bent functions. *Finite Fields Their Appl.*, 2021.

4. L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa. Constructing APN Functions Through Isotopic Shifts. *IEEE Trans. Inf. Theory,* 2020.

5. L. Budaghyan, C. Carlet, T. Helleseth, N. Kaleyski. On the distance between APN functions. *IEEE Trans. Inf. Theory,* 2020.

6. L. Budaghyan, T. Helleseth, N. Kaleyski. A new family of APN quadrinomials. *IEEE Trans. Inf. Theory,* 2020.

7. L. Budaghyan, C. Carlet, T. Helleseth. N. Li, B. Sun. On upper bounds for algebraic degrees of APN functions. *IEEE Trans. on Inform. Theory* 64(6), pp. 4399-4411, 2018.

8. [**Award Winning**] L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. *Crypt. and Communications*, 3 (1), pp. 1-16, 2011.

- **Books (2)**
  - L. Budaghyan. Construction and Analysis of Cryptographic Functions. *Springer*, 168 pages, 2015.
  - L. Budaghyan. The Equivalence of AB and APN Functions and Their Generalizations. *VDM Verlag*, 92 pages, 2008 (Second edition in 2018).
- **Co-editor of Special Issues** 10

- **Leadership education**
  - Research Leadership Programme organised at University of Oslo (12 month) 2019
  - Career kick-of meetings organized by Trond Mohn Foundation, 2019-2022
  - Research Leadership Course by Norwegian Research Council for PIs of Young Research Talent grants, 2017