

**Date of Birth:** 10/12/1986 (Tbilisi, Georgian SSR)

**Nationality:** Armenian

**Citizenship:** Armenia

**Email Address:** [diana.davidova@uib.no](mailto:diana.davidova@uib.no), [davidovadiana210@gmail.com](mailto:davidovadiana210@gmail.com)

## Education and Degrees

01/10/2017 –

**Ph.D. Candidate**, Department of Informatics, University of Bergen

07/2009

**MSc. in Mathematics** (grades 19.95 out of 20.0)

*Thesis Title:* Superproduct of algebras

*Supervisor:* Prof. Yu. M. Movsisyan

09/2007 - 06/2009

MS. Student of Applied Mathematics, dept. of Higher Algebra and Geometry, faculty of Mathematics and Mechanic, Yerevan State University, Armenia

07/2007

**BSc. in Mathematics and bachelor's degree in Pedagogics** (grades 5.0 out of 5.0), diploma with honor

*Thesis Title:* Distributive lattices with additional operation

*Supervisor:* Prof. Yu. M. Movsisyan

09/2003-06/2007

Bachelor Student, faculty of Mathematics, Yerevan State University, Armenia

## Work Experience

10/2020 – 12/2021

**Researcher**

University of Bergen, Norway

2015 - 2017

**Lecturer**

Armenian-Russian University, dept. of Mathematical Cybernetics, Yerevan, Armenia

2014 – 2017

**Lecturer**

European Educational Regional Academy, dept. of Applied Mathematics and Informational Technologies, Yerevan, Armenia

2011-2013

**Researcher**

Yerevan State University, Armenia

2009-2010

**Research Assistant**

Yerevan State University, Armenia

## Projects

2017- 2021

Role: member  
Grant: Optimal Boolean Functions (23,5 MNOK)  
University of Bergen (sponsored by the Trond Mohn Foundation)

2019-2021

Role: researcher  
Grant: Development of a new joint educational program in Information Security and Cryptography at the UIB and Novosibirsk State University (0.3 MNOK)  
University of Bergen

10/2020 – 12/2021

Role: member  
Grant: Modern Methods and Tools for Theoretical and Applied Cryptology  
University of Bergen (sponsored by the Norwegian Research Council)

2020

*Individual travel grant: Female visiting collaboration in cryptology (18.000 NOK)*  
University of Bergen (sponsored by the Meltzer fund)

2019

*Individual travel grant: Investigation of equivalence relation for cryptographical tools (8.000 NOK)*  
University of Bergen (sponsored by the Meltzer fund)

2011-2013

Role: researcher  
Grant: Structures with Identities and Hyperidentities  
Yerevan State University (sponsored by the Ministry of Education of the RA)

2009-2010

Role: research assistant  
Grant: Structures Defined by Identities and Hyperidentities and their Applications  
Yerevan State University (sponsored by Ministry of Education of RA)

**Travel grants** by “COINS Research School of Computer and Information Security” for attending the following workshops and conferences:

- COAST Training school on Symmetric Cryptography and Blockchain, Torremolinos, Spain, 2018
- 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
- COINS Finse winter school, Finse, Norway, 2019
- BFA 2019 workshop, Florence, Italy, 2019

## ACTIVITIES

### Research visits

2019

One month research visit to Prof. Claude Carlet at the University of Paris VIII, France

### Organization of workshops/conferences/events

2021

*member of the organizing committee of the 7<sup>th</sup> international workshop on Boolean Functions and Their Applications (BFA)<sup>1</sup>, Granada, Spain*

2020

*member of the organizing committee of the 6<sup>th</sup> international workshop on Boolean Functions and Their Applications (BFA)<sup>1</sup>, Loen, Norway (hybrid conference)*

2020

*member of the organizing committee of the Ernst Selmer national event<sup>2</sup>, University of Bergen, Norway*

2019

*member of the organizing committee of the 5<sup>th</sup> international workshop on Boolean Functions and Their Applications (BFA)<sup>1</sup>, Florence, Italy*

2018

*organization of the Emil Artin International conference<sup>3</sup>, Yerevan State University*

### Membership

2017-

*Scientific secretary & member of the Armenian Mathematical Union<sup>4</sup>*

---

<sup>1</sup> **BFA** is an annual workshop organized by the Selmer centre of the University of Bergen. The abstracts of the conference are peer-reviewed. The location of the workshop is different every year.

<sup>2</sup> **The Ernst Selmer national event** was organized by the Selmer Centre of UIB and Simula UIB at UIB on the 11<sup>th</sup> of February 2020. The event was dedicated to the 100<sup>th</sup> anniversary of one of the most prominent Norwegian cryptographers of the XX century, Ernst Selmer.

<sup>3</sup> **The Emil Artin International conference** is a workshop dedicated to the 120<sup>th</sup> anniversary of one of the most prominent mathematicians of the XX century, Emil Artin. The conference was organized by the Armenian Mathematical Union. Around 100 scientists from all over the world took part in the conference (Brazil, AMU, South Africa, Norway, Russia, Poland etc.) The abstracts of the conference were peer-reviewed.

<sup>4</sup> One of the duties of secretary is organization of annual conferences

## Teaching

- Teaching assistant, University of Bergen  
**Subjects:** **Computer network** (Spring semester, 2020), **Applied Cryptography A** (Autumn semester, 2020), **Information Theory** (Spring semester, 2019), **Applied Cryptography** (Autumn semester, 2019), **Discrete Structures** (Spring semester, 2018)
- Lecturer, European Regional Academy<sup>5</sup> & Russian Armenian University<sup>6</sup>  
**Subjects:** **Linear algebra** (4 semesters), **Number theory** (4 semesters), **Abstract Algebra** (4 semesters) **Analytical geometry** (4 semesters), **Discrete mathematics** (2 semesters), **Boolean algebras** (master course, 2 semesters)

## Research Interests

Boolean functions, Discrete Mathematics, Cryptography, Lattice theory, Universal algebra, Bilattices, Hyperidentities, Second-Ordered Formulas, Ordered Structures, Mathematical Logic

## Languages

Armenian (native), Russian (native), English

## Computer practice

Magma

## List of Publications:

### *Articles in refereed journals*

1. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, "On two fundamental problems on APN functions", submitted to IEEE Trans. On Inform. Theory, 2020.
2. D. Davidova and N. Kaleyski, "Generalization of a class of APN binomials to Gold-like functions", *Lecture Notes in Computer Science*, Springer (to appear in Volume 12542).
3. D. Davidova, L. Budaghyan, C. Carlet, T. Helleseht, F. Ihringer, T. Penttila, "Relation between o-equivalence and EA-equivalence for Niho bent functions", *Finite Fields and their Applications* (submitted July 2019, to appear).
4. D. S. Davidova, Yu. M. Movsisyan, "A set-theoretical representation for weakly idempotent lattices and interlaced weakly idempotent bilattices", *European Journal of Mathematics*, 2(2), 2016, p. 3-23.
5. Yu. M. Movsisyan, D.S. Davidova, "A complete characterization of hyperidentities of the variety of weakly idempotent lattices", *Proceedings of the International Conference CSIT, IEEE Trans. on Inform. Theory*, Yerevan 2015, p.41-43.
6. D. S. Davidova, Yu. M. Movsisyan, "Hyperidentities of weakly idempotent lattices", *Journal of Contemporary Mathematical Analysis*, 50(6), 2015, p. 259-264.

---

<sup>5</sup> Teaching was in Armenian & English

<sup>6</sup> Teaching was in Armenian & Russian

7. D. S. Davidova, Yu. M. Movsisyan, "Weakly idempotent lattices and bilattices, Non-idempotent Plonka functions", *Demonstratio Mathematica*, XLVIII(4), 2015, p. 509-535.
8. D. S. Davidova, Yu. M. Movsisyan, "Fixed point theorems for quantum lattices", *Vestnik of Kazan State Energy University*, 4(19), 2013, p.78-86.
9. Yu. M. Movsisyan, D. S. Davidova, "A fixed point theorem for q-lattices", *Mathematical Problems of Computer Science*, Yerevan, 38, 2012, p.80-82.
10. Yu. M. Movsisyan, D. S. Davidova, "q-Bilattices", *Journal of Mathematical Sciences*, Springer, 186(5), 2012, p. 798-801.
11. Yu. M. Movsisyan, D. S. Davidova, "Representation theorem for interlaced q-bilattices", *Logic, Algebra and Truth degrees*, Kanazawa, Ishikawa, Japan, JAIST, Kurt G ó del society, 2012, September 10-14, 2012, p. 110-113.
12. D. S. Davidova, "q-Lattices representation", *Mathematics in High School*, 8(1), 2012, p. 9-16 (Russian).
13. D. S. Davidova, "On q-bilattices", *Proceedings of the Yerevan State University Physical and Mathematical Sciences*, 3, 2011, p.9-16.
14. Yu. M. Movsisyan, D. S. Davidova, "q-Bilattices structure", *Proceedings of the International Conference Modern Algebra and its Applications*, Georgia, Batumi 2010, p.124-127.
15. Yu. M. Movsisyan, D. S. Davidova, "On the structure of interlaced q-bilattices", *Proceedings of the International Conference CSIT*, Yerevan 2009, p.57-58.
16. D. S. Davidova, "Interlaced bilattices", *Proceedings of Yerevan State University, Natural Sciences*, 3, 2008, p. 34-38 (Russian).

### **Abstracts of conferences**

1. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, "On a Relationship between Gold and Kasami Functions and other Power APN Functions", *SETA 2020*, St. Petersburg, Russia (online conference).
2. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova and N. Kaleyski, "A note on the Walsh spectrum of Dobbertin APN functions", *SETA 2020*, St. Petersburg, Russia (online conference).
3. D. Davidova and N. Kaleyski, "Generalization of a class of APN binomials to Gold like function", *WAIFI 2020*, Rennes, France (online conference).
4. L. Budaghyan, C. Carlet, D. Davidova, T. Helleseth, F. Ihringer, T. Penttila, "Relation between o-equivalence and EA-equivalence for Niho bent functions", *BFA*, June, 2018, Florence, Italy.
5. D. S. Davidova, "Magic action of o-polynomial and EA-equivalence of Niho bent functions", *BFA*, June, 2018, Loen, Norway.
6. D.S. Davidova, "Magic action and EA-equivalence of Niho bent functions", *Emil Artin International Conference*, May, 2018, Yerevan, Armenia
7. D. S. Davidova, Yu. M. Movsisyan, "Weakly idempotent lattices", *Abstracts of Armenian Mathematical Union Annual Session*, 2014, p.15.
8. D. S. Davidova, "Non-idempotent Plonka functions and hyperidentities", *Abstract Booklet for 88<sup>th</sup> Workshop on General Algebra*, Warsaw, Poland, June 19-22, 2014, p.10.

9. Yu. M. Movsisyan, D. S. Davidova, “Stone type theorems for  $q$ -lattices and interlaced  $q$ -Bilattice”, *Mal'tzev Meetings*, 12 – 15 November, 2013, Novosibirsk, Russia.
10. Yu. M. Movsisyan, D. S. Davidova, “A fixed point theorem for quantum-lattices”, *Abstracts of Second International Conference “Mathematics in Armenia. Advances and perspectives”*, 24-31 August 2013, Tzaghkadzor, Armenia.
11. Yu. M. Movsisyan, D. S. Davidova, “Interlaced  $q$ -bilattices”, *Armenian Mathematical Union Annual Session 2012 Dedicated to 1400 Anniversary of Anania Shirakatsy*, 2012, p. 82-86.