

Arman Kolozyan

Research Interests: Applied Cryptography
Email: arman@kolozyan.com
Portfolio: <https://armankolozyan.com>

I am a recent graduate in Computer Science with research experience in applied cryptography, currently interning at the Max Planck Institute for Security and Privacy (MPI-SP) under the excellent guidance of Prof. Carmela Troncoso. For my master's thesis, I investigated vulnerabilities in zero-knowledge proofs in collaboration with Nokia Bell Labs and zkSecurity. Before that, I completed a research internship at KU Leuven's COSIC group under the supervision of Prof. Bart Preneel and Prof. Dave Singelée, where I analyzed the security of the Matter standard for smart home devices. These experiences have helped me better understand where things can go wrong in cryptographic applications, while equipping me with deeper knowledge of cryptography, programming languages, and program analysis. Building on this foundation, I am now expanding my focus beyond analyzing systems toward addressing real-world security problems more broadly. This includes developing cryptographic techniques and privacy-preserving systems that address challenges in industry and society.

RESEARCH EXPERIENCE

January 2026 -
Present

Security Research Intern

Max Planck Institute for Security and Privacy, Bochum

Collaborating with the European Broadcasting Union (EBU) on designing a lightweight media encryption system.

October 2025 -
November 2025

Security Research Intern

Self, San Francisco

- Invited for the [Self Zero-Knowledge Proofs \(ZKPs\)](#) Residency.
- Worked on post-quantum cryptography.
- Presented my Master's thesis research.
- Collaborated with builders on improving real-world ZKP applications.
- Fully funded by the organizers.

July 2025

Summer School Participant

EPFL & ETH Zurich, Lausanne

- Participated in the [EPFL-ETH Summer School on Lattice-based Cryptography](#), held at EPFL.
- Received lectures from experts including [Vadim Lyubashevsky](#) and [Jonathan Bootle](#), covering both the theory and applications of lattice-based cryptography.
- Worked on a small research project focused on the Lattice Isomorphism Problem (LIP), where I explored the problem and identified directions for further research.
- Registration fee and accommodation were fully covered by the organizers.

September 2024
- September
2025

Security Research Intern

Nokia Bell Labs, Antwerp

- Conducted research focused on the security analysis of zero-knowledge proofs (ZKPs), under the supervision of [Prof. Coen De Roover](#), [Prof. Janwillem Swaenens](#), and [Prof. Stefanos Chaliasos](#).
- Part of my Master's thesis.
- Developed a language-agnostic approach for detecting inconsistencies between computations and constraints in ZKP programs.

July 2024 -
September 2024

Security Research Intern

COSIC (KU Leuven), Leuven

- COSIC is a leading research institution in cryptography and software/hardware security.
- Conducted an in-depth security analysis of the Matter standard for smart home communication, with the aim of identifying potential security weaknesses and vulnerabilities.
- Performed formal verification of Matter's protocols using automated tools, which involved modeling and verifying the protocols.
- Worked under the supervision of [Prof. Dave Singelée](#) and [Prof. Bart Preneel](#).

September 2024

Summer School Participant

Technische Universität Darmstadt, Darmstadt

- Attended the ACM Europe Summer School on Distributed and Replicated Environments (DARE) 2024.
- The summer school was focused on advanced topics in distributed systems.
- It offered me both theoretical and practical knowledge, with lectures focusing on CRDTs, Byzantine fault-tolerance, distributed systems, verification techniques for consistency, and programming/debugging/testing distributed applications.
- Participated in hands-on sessions and conducted a small research project on enhancing decentralized access control algorithms with a focus on security.
- Took classes from esteemed experts in this field, including [Prof. Martin Kleppmann](#), [Prof. Carlos Baquero](#), [Prof. Mira Mezini](#), and [Prof. Elisa Gonzalez Boix](#).
- Fully funded by the [Erasmus+ grant](#).

September 2022
- June 2023

Bachelor's Thesis

Vrije Universiteit Brussel, Brussels

- Conducted research on enhancing the speed of modular static analyses, under the supervision of [Prof. Coen De Roover](#).
- Identified limitations in existing worklist heuristics.
- Designed more efficient ones.
- Benchmarked all new and existing worklist heuristics.

PUBLICATIONS

November 2025

Language-Agnostic Detection of Computation-Constraint Inconsistencies in ZKP Programs

[Arman Kolozyan](#), [Bram Vandenbogaerde](#), [Janwillem Swalens](#), [Lode Hoste](#), [Stefanos Chaliasos](#), and [Coen De Roover](#)

This [paper](#) (S&P 2026) presents a language-agnostic formalization and a corresponding prototype implementation for detecting inconsistencies between computations and constraints in zero-knowledge proof programs. This work was carried out as part of my Master's thesis in collaboration with Nokia Bell Labs.

July 2025

What's the Matter? An In-Depth Security Analysis of the Matter Protocol

[Sayon Duttagupta](#), [Arman Kolozyan](#) (co-first author), [Georgio Nicolas](#), [Bart Preneel](#), and [Dave Singelée](#)

This [paper](#) (ePrint) is based on the work I conducted, together with my supervisors, during my internship at COSIC. It presents the first formal and practical security analysis of the Matter protocol, an IoT standard adopted by Apple, Google, Amazon, and others. Our work identifies design and implementation vulnerabilities in its key-establishment protocols (PASE and CASE), and proposes improvements to strengthen the protocol. We responsibly disclosed these [issues](#), some of which led to patches in the official codebase.

July 2020

How to Become a Memory Champion?

Arman Kolozyan

EOS Wetenschap is a renowned Belgian monthly magazine that reports on recent developments in science for a general audience. While not a peer-reviewed academic journal, it has a professional editorial board and often features articles from professors. In this article (written in Dutch), I explored whether anyone can develop a great memory by using techniques such as the memory palace. As part of the research, I interviewed world memory champions, including [Nelson Dellis](#). Quoting from the journal: "Arman Kolozyan is 19 years old. He graduated in Science-Mathematics from GO! Atheneum Emanuel Hiel and has always dreamed of having a fantastic memory. Can anyone become a memory champion? He researched this question and wrote an article on his findings." You can read the article [here](#) (in Dutch).

RESEARCH TALKS

Securing Live Media Streams in Broadcast Production (ongoing work)

- University of Bern (Christian Cachin's group), June 2026 (Bern, Switzerland)
- EBU Network Technology Seminar (NTS), June 2026 (Geneva, Switzerland)
- Cambridge Security Seminar Series, Upcoming in July 2026 (Cambridge, UK)
- Stanford Security Lunch, Upcoming in July 2026 (San Francisco, USA)

Language-Agnostic Detection of Computation-Constraint Inconsistencies in ZKP Programs

- The Science of Blockchain Conference (SBC), Upcoming in July 2026 (San Francisco, USA)
- MPI-SP Retreat Poster Session, May 2026 (Meschede, Germany)
- Stanford Security Seminar, May 2026 (San Francisco, USA)
- IEEE S&P, May 2026 (San Francisco, USA)
- ZKProof, May 2026 (Rome, Italy)
- MPI-SP (Carmela Troncoso's group), May 2026 (Bochum, Germany)
- Microsoft Research, April 2026 (Online) *
- MPI-SP (Marcel Böhme's group), April 2026 (Bochum, Germany)
- Self, November 2025 (San Francisco, USA)
- Veridise, October 2025 (Online)
- zkSecurity, October 2025 (Online)
- Nokia Bell Labs, September 2025 (Antwerp, Belgium)

TEACHING EXPERIENCE

December 2021 –
June 2025

Teaching Volunteer

Infogroep Student Association

- Infogroep is the student association dedicated to supporting Computer Science students at the Vrije Universiteit Brussel.
- Organized and taught classes on various subjects, including a preparation workshop for my university's Capture the Flag (CTF) security competition.
- Taught an introductory session on using LaTeX (Overleaf) for writing academic essays and reports.

November 2021 –
November 2024

Programming Lecturer

Vrije Universiteit Brussel

- Lecturer for additional programming classes (in the programming language Scheme), organized for first-year Computer Science students at my university.
- Always prepared slides to help the students refresh the necessary theory. Then we solved exercises in preparation for the exam.
- During the coronavirus period, I gave a session online and an on-campus session every other week.
- If the session went online, I had the students share their code via a code-sharing website where I provided comments to help them make progress.

September 2022
- September
2023

Lecturer of Mathematics

Vrije Universiteit Brussel

- Taught the following topics of mathematics for both mathematics and non-mathematics background students: Linear Algebra, Analysis, Functions, Plane Geometry, Three-Dimensional Geometry.
- This was my first experience teaching a class of more than 40 students.

August 2021 -
September 2021

Teaching Assistant of Preparation/Bridge Course in Mathematics

Vrije Universiteit Brussel

- During the coronavirus pandemic.
- Organized live question sessions.
- Answered students' questions on discussion fora.
- Corrected mathematics tests.
- Updated the solutions of exercises on the website of the mathematics book [Wiskundige basisvaardigheden](#).

WORK EXPERIENCE

April 2022 -
September 2022

Web Developer

Vrije Universiteit Brussel, Brussels

- Helped with the development of the new website of the Vrije Universiteit Brussel (VUB).
- Regularly made small adjustments to the site, created new events, etc.
- Followed up a ticketing system and resolved tickets from VUB staff and external people.

August 2022

IT Intern

Argenta, Antwerp

- Argenta is a bank and insurance group offering financial services in Belgium, the Netherlands, and Luxembourg.
- Spent a month in their IT Shared Service Integration department, assisting with the identification of available APIs.
- Created a comprehensive list of technical and functional descriptions of APIs and researched optimal tools for inventory setup and maintenance.
- This role brought me a first business experience in IT, improved my skills in conveying information clearly, enhanced my ability to ask targeted questions to colleagues, and introduced me to Agile/Scrum methodologies.

July 2022

Integration of Usolv-it Exercises into the Canvas Learning Platform

Vrije Universiteit Brussel, Brussels

- Wrote mathematics problems in LaTeX format.
- Managed mathematics assignments in Usolv-it.
- Converted Usolv-it assignments into tests and then migrated these to the Canvas learning platform.

September 2021

Organization of Pretests in Mathematics, Chemistry and Physics

Vrije Universiteit Brussel, Brussels

- Corrected pretests (which test the prior knowledge of first-year university students).
- Supervised when the students took their tests.

July 2020 -
September 2020

Logistics and Outlet Employee

ZEB, Merchtem

RFID, Sorter, Optical Scanning.

March 2019

IT Help Desk Assistant

Famiris, Brussels

- Famiris is the federal agency responsible for managing child benefits in Belgium.
- Assisted its staff with technical problems.

EDUCATION

September 2023
- September
2025

Vrije Universiteit Brussel

Master's degree in Computer Science

Greatest Distinction (summa cum laude), ranking first in Computer Science out of 350+ graduates in the last 10 academic years. Best Master's Thesis in Computer Science Award. Most Outstanding Science Student Award (out of 300+ graduating students in the Science Faculty).

September 2020
- September
2023

Vrije Universiteit Brussel

Bachelor's degree in Computer Science

Greatest Distinction (summa cum laude).

September 2014
- September
2020

GO! Atheneum Emanuel Hiel

Science-Mathematics (8h math/week)

Ranked first in class.

HONORS

March 2026

IEEE S&P Student Stipend

Received a student stipend to present my Master's thesis work at IEEE S&P 2026.

February 2026

BAEF Graduate Study Fellowship

Awarded the [Belgian American Educational Foundation \(BAEF\)](#) Graduate Study Fellowship for one academic year. BAEF supports the exchange of scientists and scholars between the United States and Belgium.

January 2026

RWC Student Stipend

Awarded a student stipend to attend [Real World Crypto \(RWC\) 2026](#) in Taipei, Taiwan.

November 2025

1st Place National ie-net Master's Thesis Award

The national [ie-net Thesis Competition](#) recognizes outstanding Master's theses in Belgium, with eligibility limited to students in the top 20% of their faculty. After reaching the finals, I defended my thesis in front of a five-member jury from different backgrounds. I won first place (€1000) in the engineering track.

November 2025

Longlist National mtech+ Technology Thesis Award

The national [mtech+ Technology Thesis Award](#) recognizes the most innovative technology-focused Master's theses submitted to the Flemish Thesis Award (Vlaamse Scriptieprijs), which received over 600 submissions this year. My thesis was selected for the longlist (top 10).

November 2025	National ie-net Master's Thesis Audience Award The national ie-net Thesis Competition recognizes outstanding Master's theses in Belgium, with eligibility limited to students in the top 20% of their faculty. Finalists can also compete for the audience award (€250) by creating a two-minute video explaining their thesis to a broad audience. My video received 700+ likes on LinkedIn and was awarded this prize.
October 2025	Most Outstanding Science Student Award Awarded annually to the most outstanding student of the Faculty of Sciences based on academic excellence across the full study track. Selected among 345 graduating students.
October 2025	Best Master's Thesis in Computer Science Award Awarded annually to the student with the best Master's thesis in Computer Science. Selected for my thesis on improving the security of Zero-Knowledge Proofs, conducted in collaboration with Nokia Bell Labs.
September 2025	Master's Degree Summa Cum Laude (Greatest Distinction) Graduated with the highest distinction (summa cum laude) for my Master's degree in Computer Science. I ranked first in Computer Science at my university in the last decade.
July 2025	Grant for EPFL-ETH Summer School on Lattice-based Cryptography Awarded a grant to attend the EPFL-ETH Summer School on Lattice-based Cryptography, covering both the registration fee and accommodation.
March 2025	4th Place Finals Cyber Security Challenge Belgium 2025 National team competition for students about cyber security. Our team secured the 4th place out of 359 teams. My main contributions were to the cryptography category.
September 2024	Erasmus+ Grant for ACM Europe Summer School (DARE 2024) Received an Erasmus+ grant to attend the ACM Europe Summer School on Distributed and Replicated Environments (DARE) 2024 at Technische Universität Darmstadt, Germany.
March 2024	Winner of Qualifiers in Cyber Security Challenge Belgium 2024 National team competition for students about cyber security. We advanced through the qualifiers, securing first place out of 286 teams. We later finished 8th in the finals. My main contributions were to the cryptography category.
September 2023	Bachelor's Degree Summa Cum Laude (Greatest Distinction) Graduated with the highest distinction (summa cum laude) for my Bachelor's degree in Computer Science.
March 2023	Finalist Cyber Security Challenge Belgium 2023 National team competition for students about cyber security. We successfully advanced through the qualifiers and secured 7th place out of 289 teams in the finals. My main contributions were to the cryptography and forensics categories.
March 2022	Pre-Finalist Cyber Security Challenge Belgium 2022 National team competition for students about cyber security. We successfully advanced through the qualifiers and secured 43rd place out of 253 teams in the pre-finals. Unfortunately, we did not progress to the finals. My main contributions were to the cryptography and forensics categories.

November 2021

Winner Vrije Universiteit Brussel (VUB) CTF 2021

Capture The Flag (CTF) is a competition in which teams solve tasks related to cyber security. [This competition](#) was organized by the Vrije Universiteit Brussel. My contribution was mainly on the cryptography category, where I successfully solved all of the cryptography challenges.

September 2021

Interview in BRUZZ (Belgian magazine)

After I successfully completed my first academic year, I was interviewed in [this Belgian news article](#) about the Computer Science major and my academic achievements. I was later also invited for a radio interview.

March 2020

Finalist Wiskunnend Wiske Wedstrijd 2020

[Competition](#) where hard mathematics questions must be solved by students in their final years of secondary school. I solved the three challenges on my own and, upon hearing that my submission qualified for the finals, gathered a team to compete in the next stage.

VOLUNTEERING

September 2024
- September
2025

Co-organizer of Capture The Flag (CTF) Competition Infogroep Student Association

[Infogroep](#) is the student association dedicated to supporting Computer Science students at the Vrije Universiteit Brussel. At Infogroep, we organize activities such as seminars, cyber security competitions, a gaming tournament, a job fair, etc. I co-organized the annual [Capture The Flag \(CTF\) competition](#) at our university, a cybersecurity event where students solve real-world hacking challenges in areas such as web exploitation, cryptography, and reverse engineering. The competition aims to promote security awareness and hands-on learning among students.

September 2021
- June 2025

Student Representative in Study Program Committee Vrije Universiteit Brussel

Worked with faculty, staff, and fellow students to improve our academic programs and student life. I helped bring forward student concerns, suggest changes, and support initiatives that make a positive difference.

February 2025

Volunteer at FOSDEM FOSDEM

Assisted visitors at the info desk and sold [FOSDEM](#) merchandise.

September 2023
- September
2024

Corporate Relations, Lectures & Seminars Infogroep Student Association

[Infogroep](#) is the student association dedicated to supporting Computer Science students at the Vrije Universiteit Brussel. At Infogroep, we organize activities such as seminars, cyber security competitions, a gaming tournament, a job fair, etc. I managed our corporate relations with companies such as Deloitte and PwC. I also organized and taught several seminars on topics such as using LaTeX (Overleaf) for academic writing.

March 2024

Student Volunteer at Computer Science Workshop Brussels Workshop on Real-Time Scheduling and Operating System Synergies

Assisted attendees in navigating the university campus.

December 2021 -
September 2023

Job Fair Organizer

Infogroep

I served as the head of the annual [job fair](#) organized by our student association. To make the job fair a success, I ensured extensive promotion, which included announcements at the beginning of lectures, paid Facebook advertisements, and more. My goal was to also attract a diverse range of appealing companies to participate. Ultimately, the job fair proved to be a great success, with over 100 attendees, 15+ participating companies, and with more than 150 student resumes submitted.

October 2022

Student Volunteer at Gaming Event

GameForce

[GameForce](#) is the largest gaming event in the Benelux. I had the responsibility to stand at various booths, attract visitors, and provide the necessary assistance to them.

September 2022

Student Volunteer at Computer Science Conference

International Conference on Managed Programming Languages & Runtimes

I provided room support by assisting presenters in the [conference](#) room, troubleshooting technical issues, and passing the microphone for audience questions. Additionally, I offered outside support in the main hall, where I helped at the registration desk.