Alexander (Sasha) Frolov

Updated December 11, 2023

Email: sashafrolov@meta.com **GitHub**: github.com/sashafrolov **Website**: sasha.place

Research interests

Cryptography, Security & Privacy, Theory

Education

Cornell University Ithaca, NY
M. Eng. in Computer Science August 2020 – May 2021
GPA: 3.953.

Cornell University Ithaca, NY
BA in Computer Science and Mathematics August 2017 – December 2020
GPA: 4.055. Cumme Laude in Mathematics, With Distinction in all subjects.

Selected coursework

- Cryptography: Introduction to Cryptography (CS 4830), Pseudorandomness (CS 6815), Number Theory (MATH 3320)
- Systems Design: Distributed Computing Principles (CS 5414), Advanced Programming Languages (CS 6110), Cloud Computing (CS 5412), Operating Systems (CS 4410)
- Quantum Computing: Quantum Information Processing (CS 4812), Introduction to Quantum Mechanics (PHYS 3316), Applications of Quantum Mechanics (PHYS 3317)
- Math/Theory: Analysis of Algorithms (CS 6820), Special Topics in Algorithms (CS 7822), Honors Analysis I (Math 4130), Combinatorics I/II (MATH 4410/4420)

Honors and scholarships

Dean's List Fall 2017, Spring 2018, Spring 2019, Fall 2019, Fall 2020
Admitted to Phi Beta Kappa 2020
Juniper Networks Engineering Scholarship 2017

Publications

Purple Llama CyberSecEval: A Secure Coding Benchmark for Language Models
Manish Bhatt, Sahana Chennabasappa, Cyrus Nikolaidis, Shengye Wan, Ivan Evtimov, Dominik Gabi, Daniel Song, Faizan Ahmad, Cornelius Aschermann, Lorenzo Fontana, **Sasha Frolov**, Ravi Prakash Giri, Dhaval Kapil, Yiannis Kozyrakis, David LeBlanc, James Milazzo, Aleksandar Straumann, Gabriel Synnaeve, Varun Vontimitta, Spencer Whitman, Joshua Saxe.
Was presented at a workshop at NeurIPS 2023.
https://arxiv.org/abs/2312.04724.

CanDID: Bootstrapping Decentralized Identity from Legacy Providers
Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, **Alexander Frolov**, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller.
Appeared in IEEE S&P 2021.
https://eprint.iacr.org/2020/934

Statistical Properties of Soft X-ray emission of Solar Flares
Viacheslav M Sadykov, Alexander G Kosovichev, Irina N Kitiashvili, **Alexander Frolov**.
The Astrophysical Journal.
https://arxiv.org/abs/1810.05610

Other contributions

Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts
Kushal Babel, Philip Daian, Mahimna Kelkar, Ari Juels (I have a "thanks to" at the bottom of the paper).
Appeared in IEEE S&P 2023.
https://arxiv.org/abs/2109.04347

Mastering Ethereum: Building Smart Contracts and DApps
Andreas Antonopoulos. (I contributed to the book on GitHub and am credited in the front of the book).
O'Reilly, 2018.
https://www.oreilly.com/library/view/mastering-ethereum/9781491971932/

Editing Wikipedia
User A40585. (100+ edits to cryptography/computer science related articles).
https://en.wikipedia.org/wiki/Special:Contributions/A40585

Industry experience

Meta — New York City and Seattle
Software Engineer, IC4 — October 2021 – Present
Member of Cryptography Infrastructure team (team working on basic cryptographic primitives).
Wrote code for key management systems/internal cryptography libraries.
Wrote/reviewed designs and worked on auditing various internal systems that used cryptographic technologies like Multi-Party Computation, Trusted Execution Environments and Post-Quantum Cryptography.
Received "Redefines Expectations" performance rating in 2022 (highest rating given to top 1-5% of engineers).
Notable projects:
– Implemented and tuned the assembly for a new mode of operation for the AES block cipher with extended nonces, authentication and key commitment.
– Worked on project to find and eradicate use cases of encryption with high likelihood of nonce collisions occurring.
– Helped design and implement systems to encrypt storage in Meta data centers.

Facebook — Menlo Park, CA
Software Engineering Intern — Summer 2020
Working on language support/advanced library tooling for Oculus projects.
Worked on implementing data binding features for a systems programming library to enable efficient future AR/VR development.

Facebook Menlo Park, CA
Software Engineering Intern Summer 2019
Optimized part of WhatsApp Business API backend, decreasing database load and latency by 10-20%, while also increasing reliability/decreasing lost revenue.
Fixed bugs and increased testing coverage/stability for WhatsApp Business backend.
Designed/implemented system for API to hot-swap business logic from external configs.

Cornell Tech New York City
Research Intern Summer 2018
Reverse engineered contracts on Ethereum blockchain to analyze wealth distributions of token sales, security/cryptographic properties, and dynamics of exchanges.
Analyzed data and created visualizations to showcase inequality and team's results.

Teaching experience

Teaching assistant, Cornell University January 2018 – May 2021
Teaching Assistant for:
– Discrete Mathematics (CS 2800) in Spring 2018
– Introduction to Algorithms (CS 4820) in Fall 2018, Spring 2019, Fall 2019, Fall 2020, Spring 2021
– Introduction to Computational Complexity (CS 4814) in Spring 2020.
Held weekly office hours, contributed to testing/developing homeworks and exams, and graded homework as well as exams.
Received recognition for continued service as a TA (7 semesters) in the CS department.
Due to Computational Complexity not being offered for 4 years, I was trusted to self-study the material for the class and be a teaching assistant without having formally taken the class.

Talks

Migrating to Nonce Misuse Resistant Ciphers August 2023
Gave a talk to the entire Meta Security organization about my team's efforts to migrate users to nonce misuse resistant cryptography.

Quantum and Post-Quantum Cryptography December 2022
Gave a talk to the Meta Cryptography Infrastructure team about the current state of Post-Quantum Cryptography.

Outreach

Was a Cornell Alumni Admissions Ambassador Network (CAAAN) Ambassador for the 2022 and 2023 application cycles.
Talked to multiple Meta interviewees with similar disabilities/medical issues to mine about working at the company through Disability@ program.

Skills

C++, Java, Python, Rust, Erlang, OCaml, LaTeX, Intel SGX, AMD SNP, Tuning x86 assembly

Miscellaneous

Fluent in Russian, Amateur Standup Comedian, Eagle Scout.