Contact information

E-mail: polubelovam@gmail.com
Personal website: https://polubelova.github.io/

Research interests

Software verification, cryptographic implementation, dependent type systems, functional programming, static program analysis.

Education

École Normale Supérieure Paris and **INRIA Paris**, Paris, France.

Ph.D in computer science, **Prosecco team**, September 2017 – May 2021.

- Thesis title: *Building a formally verified high-performance multi-platform cryptographic library in F**
- Advisor: Karthikeyan Bhargavan

Saint Petersburg State University, Saint Petersburg, Russia.

M.Sc. in mathematics and computer science, Dept. of Mathematics and Mechanics, GPA 4.8/5.0, 2015 – 2017.

- Thesis title: *Compiling verified F* programs to robust Web applications*
- Advisor: Karthikeyan Bhargavan, Semyon Grigorev

B.Sc. in mathematics and computer science, Dept. of Mathematics and Mechanics, GPA 4.5/5.0, 2011 – 2015.

- Thesis title: *Lexical analysis of dynamically generated string expressions*
- Advisor: Semyon Grigorev

Employment

Nomadic Labs, Paris, France

Software Engineer, Privacy team. October 2021 – now.

- Formal verification of standard signatures using F* (ECDSA over the P256 and K256 elliptic curves);
- Implementation of standard signatures in Zero-Knowledge circuits (Ed25519).

INRIA Paris, Paris, France

Doctorant, Prosecco team. September 2017 – May 2021.

- Thesis title: *Building a formally verified high-performance multi-platform cryptographic library in F**
- Advisor: Karthikeyan Bhargavan

Microsoft Research, Cambridge, United Kingdom

Research Intern, Programming Principles and Tools team. June 2018 – September 2018.

- Project title: *Verified Implementation of Post-Quantum Cryptography in F**
- Supervisor: Santiago Zanella-Béguelin

JetBrains Inc., Saint Petersburg, Russia

Software Developer, Programming Languages and Tools Lab team. January 2016 – July 2017.

Researcher, Programming Languages and Tools Lab team. June 2014 – July 2017.

- Development and implementation of lexical analysis for dynamically generated string-embedded languages;
- Program verification using F*;

Intern, Programming Languages and Tools Lab team. June 2015 – July 2015.

- Optimization of lexical analysis for dynamically generated string-embedded languages;
- Evaluation of lexical analysis implementation;

Intern, Programming Languages and Tools Lab team. June 2014 – September 2014.

- Development and implementation of lexical analysis for dynamically generated string-embedded languages;

INRIA Paris, Paris, France

Intern, Prosecco team. September 2016 – November 2016.

- Project title: *Verified backends for the F* programming language*
- Supervisor: Karthikeyan Bhargavan

YaccConstructor project, Saint Petersburg State University, Saint Petersburg, Russia

Student Researcher, YaccConstructor team. June 2013 – May 2014.

- Development of Transact SQL parser;
- Comparison tools for statical analysis of dynamically generated string-embedded languages;

LANIT-TERCOM Inc., Saint Petersburg, Russia

Software Engineer, Reengineering team. February 2014 – April 2014.

- Development of Sybase SQL parser;
- Estimation of structural program complexity (count of embedding operators in queries);

Publications and manuscripts

1. **HACLxN: Verified Generic SIMD Crypto (for all your favorite platforms)**
   Marina Polubelova, Karthikeyan Bhargavan, Jonathan Protzenko, Benjamin Beurdouche, Aymeric Fromherz, Natalia Kulatova, Santiago Zanella-Béguelin
   ACM Conference on Computer and Communications Security (CCS), 2020.
2. **EverCrypt: A Fast, Verified, Cross-Platform Cryptographic Provider**
   Jonathan Protzenko, Bryan Parno, Aymeric Fromherz, Chris Hawblitzel, Marina Polubelova, Karthikeyan Bhargavan, Benjamin Beurdouche, Joonwon Choi, Antoine Delignat-Lavaud, Cedric Fournet, Natalia Kulatova, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, Christoph Wintersteiger, Santiago Zanella-Béguelin
   IEEE Symposium on Security and Privacy (Oakland), 2020.
3. **Lexical analysis of dynamically generated string expressions**
   Marina Polubelova and Semyon Grigorev
   Scientific journal "Systems and Means of Informatics", volume 26, issue 2, pages 43–62, 2016.
4. **Lexical analysis of dynamically generated string expressions**
   Marina Polubelova and Semyon Grigorev
   Tools and Methods of Program Analysis Conference 2015 (TMPA-2015).

5. **Generator of abstract lexical analyzers**
   Marina Polubelova and Semyon Grigorev
   Young Researchers Conference on Microsoft Technologies in Theory and Practice of Programming 2014.
6. **String-embedded Language Support in Integrated Development Environment**
   Semyon Grigorev, Ekaterina Verbitskaia, Marina Polubelova, Andrey Ivanov and Ekaterina Mavchun
   10th Central and Eastern European Software Engineering Conference in Russia (SECR-2014).
7. **IDE Support of String-Embedded Languages**
   Semyon Grigorev, Ekaterina Verbitskaia, Marina Polubelova, Andrey Ivanov and Ekaterina Mavchun
   Workshop on Science Intensive Applied Software (PSI-2014).

Software contributions

- **HACL*** github repository
  - Verified Bignum Library
    - Custom Bignum Library (modulo-specific optimizations)
    - Generic Bignum Library
    - Examples: **curve25519**, **ed25519**, **RSA-PSS**
  - Verified Vectorized Crypto
    - Multiple Input Parallelism
    - Polynomial Evaluation
    - Counter Mode Encryption
    - Examples: **SHA2-mb**, **poly1305**, **chacha20**, **GMAC**
  - Verified Post-Quantum Crypto
    - Lattice-Based Crypto
    - Example: **FrodoKEM** (+**SHA3**)
- **F*** github repository
  Implementation of JavaScript backend for the F* programming language
- **YaccConstructor** github repository
  Implementation of lexical analysis for dynamically generated string-embedded languages

Technical skills

- Verification tools: F*
- Programming languages: OCaml, F#, C, C++, R, JavaScript

Language skills

English (C1) and Russian (mother tongue)