Denis Firsov

Personal data

Birth date	28.05.1987
E-mail	denis.firsov@gmail.com
Degree	PhD
Homepage	`http://firsov.ee`

Brief Introduction

For my PhD, I studied under the supervision of Tarmo Uustalu at the Institute of Cybernetics of the Tallinn University of Technology (Taltech) where I studied constructive type theory and languages like **Agda** and **Coq**.

After that, I did my postdoctoral research with Aaron Stump at the Computational Logic Center of the University of Iowa where I studied impredicative type theory in **Cedille**.

Then I joined R&D department of GuardTime (2019-2023) where I was using **EasyCrypt** theorem prover to derive security of novel cryptographic constructions (digital signatures, commitment schemes, zero-knowledge systems).

Then I held a researcher position at the Matter Labs (2023-2024) where we were developing Rust DSL for correct-by-construction ZK-circuits; proving correctness of the low-level implementation of PLONK system in **EasyCrypt**; and modelling rollup system behaviour in tools like **TLA+** and **Alloy**.

I am also holding a researcher position at the Department of Software Science in Taltech.

My PhD thesis, entitled "Certified algorithms for context-free languages", was supervised by prof. Tarmo Uustalu and I defended it on 31st August 2016.

My interests include algorithms, cryptography, functional programming, formal verification, constructive mathematics, and software design.

Education

2016–2018 **Postdoc, Computer science**, *University of Iowa*.
2012–2016 **PhD, Computer science**, *Tallinn University of Technology*.
2010–2012 **MSc (Cum laude), Informatics**, *Tallinn University of Technology*.
2006–2010 **BSc, Software development**, *The Estonian Information Technology College*.
1994–2006 **Secondary education**, *Russian Gymnasium of Mustvee*.

Work Experience

2023–2024 **Research scientist**, Matter Labs, Remote.
2019–2023 **Research engineer**, GuardTime, Tallinn.
2019–present **Researcher**, Tallinn University of Technology, Tallinn.
2012–2016 **Lecturer**, Estonian Information Technology College, Tallinn.
2011–2016 **Junior researcher**, Institute of Cybernetics at TUT, Tallinn.
2010–2011 **Software architect**, Attitude OÜ, Tallinn.
2009–2010 **Software developer**, Majandustarkvara (Erply) OÜ, Tallinn.

Relevant Publications and Preprints

- M. Stronati, D. Firsov, A. Locascio, B. Livshits **Clap: a Rust eDSL for PlonKish Proof Systems with a Semantics-preserving Optimizing Compiler**
  submitted to NDSS'25, CoRR abs/2405.12115 (2024)
- S. Chaliasos, D. Firsov, B. Livshits **Towards a Formal Foundation for Blockchain Rollups**
  planned for FC'25, CoRR abs/2406.16219 (2024)
- D. Firsov, D. Unruh **Zero-Knowledge in EasyCrypt**
  In Proc. of 36th IEEE Computer Security Foundations Symposium, CSF '23 (Dubrovnik, Croatia), pages 226-241, 2023.
- D. Firsov, S. Laur, E. Zhuchko **Unsatisfiability of Comparison-Based Non-Malleability for Commitments**
  In: H. Seidl, Z. Liu, C. S. Pasareanu, eds., Proc. of 19th Int. Coll. on Theoretical Aspects of Computing, ICTAC 2022 (Tbilisi, Sept. 2022), v. 13572 of Lect. Notes in Comput. Sci., pp. 305-323. Springer, 2022.
- D. Firsov, D. Unruh **Reflection, Rewinding, and Coin-Toss in EasyCrypt**
  In Proc. of 11th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP '22 (Philadelphia, Pennsylvania, USA), pages 166-179.
- D. Firsov, H. Lakk, S. Laur, A. Truu **BLT+L: Efficient Signatures from Timestamping and Endorsements**
  In Proc. of the 18th International Conference on Security and Cryptography, SECRYPT '21 (Virtual Conference), pages 75-86.
- D. Firsov, H. Lakk, A. Truu **Verified Multiple-Time Signature Scheme from One-Time Signatures and Timestamping**
  In Proc. of 34th IEEE Computer Security Foundations Symposium, CSF '21 (Virtual Conference), pages 653-665.
- A. Buldas, D. Firsov, R. Laanoja, A. Truu. **Verified Security of BLT Signature Scheme**
  In Proc. of 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP

'20 (New Orleans, LA, USA).

- A. Buldas, D. Firsov, R. Laanoja, H. Lakk, A. Truu. **A New Approach to Constructing Digital Signature Schemes**
  In:Attrapadung N., Yagi T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. Springer, 2019
- D. Firsov, L. Diehl, C. Jenkins, A. Stump. **Course-of-Value Induction in Cedille**
  Manuscript, 2018
- L. Diehl, D. Firsov, A. Stump. **Generic Zero-Cost Reuse for Dependent Types**
  In Proc. of 23rd ACM SIGPLAN International Conference on Functional Programming, ICFP '18 (St. Louis, Missouri, United States, September 2018).
- D. Firsov, R. Blair, A. Stump. **Efficient Mendler-Style Lambda-Encodings in Cedille.**
  In Proc. of 9th International Conference on Interactive Theorem Proving, ITP '18 (Oxford, July 2018).
- D. Firsov, A. Stump. **Generic derivation of induction for impredicative encodings in Cedille.**
  In Proc. of 7th ACM SIGPLAN Conf. on Certified Programs and Proofs, CPP '18 (Los Angeles, Jan. 2018), pp. 215-227, ACM, 2018.
- D. Firsov. **Certified algorithms for context-free grammars.**
  PhD thesis, Institute of Cybernetics at TUT, 2016.
- D. Firsov, W. Jeltsch. **Purely functional incremental computing.**
  In F. Castor, Y. D. Liu, eds., Proc. of 20th Brazilian Symp. on Prog. Lang., SBLP 2016 (Maringá, Brazil), v. 9889 of Lect. Notes in Comput. Sci., pp. 62-77, Springer, 2016.
- D. Firsov, T. Uustalu, N. Veltri. **Variations on Noetherianness.**
  In R. Atkey, N. Krishnaswami, eds., Proc. of 6th Wksh. on Mathematically Structured Functional Programming, MSFP 2016 (Eindhoven, April 2016), v. 207 of Electron. Proc. in Theor. Comput. Sci., pp. 76-88. Open Publishing Assoc., 2016.
- D. Firsov, T. Uustalu. **Dependently typed programming with finite sets.**
  In Proc. of 11th ACM SIGPLAN Wksh. on Generic Programming, WGP '15 (Vancouver, BC, Aug. 2015), pp. 33-44. ACM Press, 2015.
- D. Firsov, T. Uustalu. **Certified normalization of context-free grammars.**
  In Proc. of 4th ACM SIGPLAN Conf. on Certified Programs and Proofs, CPP '15 (Mumbai, Jan. 2015), ACM Press, 2015
- D. Firsov, T. Uustalu. **Certified CYK parsing of context-free languages.**
  J. of Log. and Algebr. Meth. in Program., v. 83, n. 5-6, pp. 459-468, 2014.
- D. Firsov, T. Uustalu. **Certified parsing of regular languages.**
  In G. Gonthier, M. Norrish, eds., Proc. of 3rd Int. Conf. on Certified Programs and Proofs, CPP 2013 (Melbourne, Dec. 2013), v. 8307 of Lect. Notes in Comput. Sci., pp. 98-113. Springer, 2013.

Patents

- A. Truu, D. Firsov. **Delegated signatures for smart devices**
  US Patent 11,316,698 (granted)
- D. Firsov, H. Lakk. **Method and System for Generating Data Signatures Using an Unbounded, Stateless Private Key**
  US Patent App. 16/784,561 (granted)
- D. Firsov. **One-Time Data Signature System and Method with Untrusted Server Assistance**
  US Patent App. 16/784,561 (published)

Conferences/Talks/Workshops/Summerschools/Winterschools

22/05/24–24/05/24 **ZKProof 6**, Berlin, Germany
Talk: The Ouroboros of ZK (presented by Ben Livshits)

23/02/24–03/03/24 **ETHDenver**, Denver, USA
Talk: How do we use formal methods to harden ZK-rollups

10/04/24–11/04/24 **ZKSummit 11**, Athens, Greece

20/11/23–24/11/23 **Matter Labs offsite**, Istanbul, Turkey

09/07/23–13/07/23 **36th IEEE Computer Security Foundations Symposium**, Dubrovnik, Croatia
Talk: Zero-Knowledge in EasyCrypt

30/03/23–01/04/23 **High-Assurance Crypto Software meeting**, HACS 2023,

27/02/23–10/03/23 **Workshop at Reykjavik University**, Reykjavik, Iceland
Talk: EasyCrypt for working cryptographer

09/11/22–14/12/22 **Workshop at IOHK**, Virtual,
Talk: EasyCrypt for working cryptographer

27/09/22–30/09/22 **19th International Colloquium on Theoretical Aspects of Computing**, Tbilisi, Georgia

17/01/22–19/01/22 **The 11th ACM SIGPLAN International Conference on Certified Programs and Proofs**, Philadelphia, Pennsylvania, USA
Talk: Reflection, Rewinding, and Coin-Toss in EasyCrypt

04/11/21–06/11/21 **32nd Nordic Workshop on Programming Theory**, NWPT 2021,

09/09/21–11/09/21 **Logic and Semantics Group Outing Days**, Pillapalu, Estonia
Talk: Probabilistic Reflection in EasyCrypt

21/06/21–24/06/21 **34th IEEE Computer Security Foundations Symposium**, Virtual Conference,
Talk: Verified Multiple-Time Signature Scheme from One-Time Signatures and Timestamping

10/06/21 **Computer Science Theory Seminar at TUT**, Tallinn, Estonia
Talk: Verified Multiple-Time Signature Scheme from One-Time Signatures and Timestamping

23/02/19–24/02/19 **EUTypes Meeting**, Krakow, Poland
Talk: Efficient Mendler-Style Lambda-Encodings in Cedille

07/02/19–09/02/19 **DLT Notary Workshop**, Luxembourg City, Luxembourg

23/09/18–29/09/18 **23rd ACM SIGPLAN International Conference on Functional Programming**, St. Louis, Missouri, United States

6/07/18–14/07/18 **9th International Conference on Interactive Theorem Proving**, Oxford, UK
Talk: Efficient Mendler-Style Lambda-Encodings in Cedille

5/07/18 **Theory Lunch at TTÜ Software Lab**, Tallinn, Estonia
Talk: Generic Zero-Cost Reuse for Dependent Types

19/02/18–24/02/18 **Visiting the Reykjavik University**, Reykjavik, Iceland
Talk: Generic derivation of induction for impredicative encodings in Cedille

07/01/18–13/01/18 **The 7th ACM SIGPLAN International Conference on Certified Programs and Proofs (+ POPL + CoqPL)**, Los Angeles, CA, United States
Talk: Generic derivation of induction for impredicative encodings in Cedille

22/09/16–23/09/16 **XX Brazilian Symposium on Programming Languages**, Maringá, Brazil
Talk: Purely functional incremental computing

21/08/16–25/08/16 **15th Estonian Summer School on Computer Science**, Nelijärve, Estonia
Talk: Purely functional incremental computing

26/06/16–02/07/16 **Second International Summer School on Behavioural Types**, Limassol, Cyprus

01/04/16–09/04/16 **Sixth Workshop on Mathematically Structured Functional Programming (+ ETAPS)**, Eindhoven, Holland
Talk: Variations on Noetherianness

28/02/16–04/03/16 **21st Estonian Winter School in Computer Science**, Palmse, Estonia

29/01/16–31/01/16 **Theory Days at Käo**, Käo, Estonia
Talk: Noetherian sets

13/11/15–15/11/15 **Estonian-Finnish logic meeting**, Rakvere, Estonia
Talk: Dependently typed programming with finite sets

21/10/15–23/10/15 **27th Nordic Workshop on Programming Theory**, Reykjavik, Iceland
Talk: Acyclic attribute evaluation in dependently typed setting

02/10/15–04/10/15 **Theory Days at Jõeküla**, Jõeküla, Estonia

18/09/15–20/09/15 **Coinduction project working meeting**, Sääritsa, Estonia
Talk: Incremental Stable Sorting in Haskell

30/08/15–05/09/15 **11th ACM SIGPLAN Workshop on Generic Programming**, Vancouver, Canada
Talk: Dependently typed programming with finite sets

13/07/15–22/07/15 **Understanding Complexity and concurrency through topology of data**, Camerino, Italy

06/07/15–10/07/15 **Summer School on Generic and Effectful Programming**, Oxford, UK

01/03/15–06/03/15 **20th Estonian Winter School in Computer Science**, Palmse, Estonia

06/02/15–08/02/15 **Theory Days**, Rogosi, Estonia
Talk: Functional incremental computing

13/01/15–14/01/15 **The 4th ACM-SIGPLAN Conference on Certified Programs and Proofs**, Mumbai, India
Talk: Certified normalization of context-free grammars

05/12/14–06/12/14 **8th Annual Conference of the National Doctoral School in Information and Communication Technologies**, Rakvere, Estonia
Talk: Functional incremental computing

10/11/14–11/11/14 **Coinduction project working meeting**, Pillapalu, Estonia

02/10/14–05/10/14 **Joint Estonian-Latvian Theory Days at Ratnieki**, Ratnieki, Latvia

21/09/14–23/09/14 **Coinduction Meeting**, Kata, Estonia

16/05/14–18/05/14 **Theory Days**, Narva-Jõesuu, Estonia

20/04/14–27/04/14 **Midlands Graduate School 2014**, Nottingham, UK

02/03/14–07/03/14 **19th Estonian Winter School in Computer Science**, Palmse, Estonia

25/10/13–27/10/13 **Theory Days**, Saka, Estonia
Talk: Formalizing attribute grammars and circularity checking

17/10/13–18/10/13 **Rich Model Toolkit–Final COST Action Meeting**, Madrid, Spain
Talk: Certified attribute grammar validation

08/07/13–20/07/13 **Domain specific languages summer school 2013**, Cluj-Napoca, Romania

08/04/13–12/04/13 **Midlands Graduate School 2013**, Leicester, England

03/03/13–08/03/13 **18th Estonian Winter School in Computer Science**, Palmse, Estonia

01/02/13–03/02/13 **Theory Days**, Otepää, Estonia
Talk: Certified normalization of context-free grammars

20/01/13–21/01/13 **Workshop on Synthesis, Verification and Analysis of Rich Models**, Rome, Italy
Talk: Certified normalization of context-free grammars and CYK parsing

31/10/12–02/11/12 **24th Nordic Workshop on Programming Theory**, Bergen, Norway
Talk: Certified CYK parsing of context-free languages

03/10/12–09/10/12 **The XVI edition of the Agda Implementors' Meeting: Theory and implementation**, Copenhagen, Denmark

27/09/12–30/09/12 **Joint Estonian-Latvian Theory Days at Medzābaki**, Lilaste, Latvia
Talk: Certified parsing of context-free grammars

19/08/12–23/07/12 **11th Estonian Summer School on Computer Science**, Jäneda, Estonia

16/07/12–28/07/12 **Oregon Programming Languages Summer School**, Oregon, USA

26/02/12–02/03/12 **17th Estonian Winter School in Computer Science**, Palmse, Estonia
Talk: Certified parsing of regular languages

27/01/12–29/01/12 **Theory Days**, Kubija, Estonia
Talk: Certified parsing

07/10/11–09/10/11 **Theory Days**, Tõrve, Estonia

Organizing activity

I helped in organizing the following events: ETAPS 2012, EWSCS '12– EWSCS '16, NWPT '13, COST ARVI Tallinn meeting '15, Estonian-Finnish logic meeting '15, TYPES '15, CPP '23.

Peer Review

I reviewed papers for the following conferences and journals: ICALP, ICFP, JFR, LMCS, RTALCA, TYPES, CPP, FM, ICR.
I also reviewed multiple master, doctoral, and bachelor theses for TUT and UT.

Students

Margit Ool (BSc), Jaan Elken (BSc), Liisa Suurkaev (BSc), Richard Blair (PhD student), Ekaterina Zhuchko (MSc)

Teaching

I used to teach functional programming at the Estonian Information Technology College (years 2012-2015).

Background

My main interests include the following topics:

- type theory
- algorithms
- semantics of programming languages
- constructive logic
- cryptography
- compiler construction
- type systems
- functional programming

Languages

Russian	**Mothertongue**
English	**Fluent**
Estonian	**Fluent**
Italian	**Beginner**

Interests

- Skiing
- Piano
- Hiking
- Scuba diving
- Ice/Roller Skating
- Literature
- SUPing
- Spearfishing