

Nikita Frolov's CV

2012-01-02

Contacts

- email/jabber/gtalk: nf@mkmks.org
- homepage: <http://mkmks.org>
- GitHub: <https://github.com/mkmks>
- LinkedIn: <http://se.linkedin.com/in/nickfrolov>
- PGP key id: 3FAD8754

Education

2012–now Ph.D. in Computer Science, Chalmers TH (Gothenburg, Sweden)

I'm part of the [RAWFP](#) project that aims to bridge the semantic gap between application domains and functional programming and between functional programming and hardware.

2009–2011 M.Sc. in Computer Engineering, Chalmers TH (Gothenburg, Sweden)

In my master's thesis I was researching an approach to the phase sequencing problem based on expressing the scheduling problem as a set of mutually independent constraints and solving them with a SAT solver. The approach is evaluated by creating a retargetable compiler for the FlexCore processor¹.

2003–2008 B.Sc. in Computer Engineering, Bauman TU (Moscow, Russia)

My bachelor's thesis was about design and evaluation of a simple VLIW processor and a GCC backend targeting it.

Employment

09/2011–12/2011 Research assistant at Chalmers TH (Gothenburg, Sweden)

As part of [MOLTO](#), I was improving the Russian resource grammar for [Grammatical Framework](#).

¹FlexCore — a computing architecture developed by the VLSI group at Chalmers that is highly reconfigurable both at design- and run-time and encourages hardware-software codesign by inclusion of application-specific accelerator blocks. (<http://flexsoc.org>)

2005–2009 Developer at Demos Co. (Moscow, Russia)

Some significant projects include:

- a platform for SIM/USIM-cards lifecycle management (I co-authored the system specification and the security policy and implemented SEE² components of access control and key storage subsystems);
- a GOST³ implementation for [nCipher HSMs](#), including PKCS11 wrapper;
- a library for implementation of RSA CTKIP protocol servers and clients;
- adding support for GOST algorithms to RSA MobileID authentication server and software implementations of RSA SecurID tokens.

Publications

- N. Frolov, M. Sjölander, P. Larsson-Edefors, S.A. McKee, “A SAT-Based Compiler for Flex-Core”, Technical report - Department of Computer Science and Engineering, Chalmers University of Technology and Göteborg University, ISSN 1652-926x; nr 1652, 2011 ([link](#))
- N. Frolov, M. Sjölander, P. Larsson-Edefors, S.A. McKee, “Declarative, SAT-solver-based Scheduling for an Embedded Architecture with a Flexible Datapath”, 2011 Swedish System-on-Chip Conference (not a peer-reviewed conference)
- N.V. Frolov, “Timestamping Services and Trusted Sources of Time”, [Journal of Networks and Services](#) №17, 2006 (in Russian)

Invited talks

- “A DSL for compiler construction”, Functional Programming Group, Chalmers University of Technology, October 2010
- A series of guest lectures on timestamping and trusted sources of time, [Russian Association of Networks and Services](#), 2007–2009

Open source

- [Haskell bindings for LLVM](#)
 - Support for bytecode traversal

²SEE — Secure Execution Engine, a proprietary trusted computing technology developed by nCipher

³GOST (ГОСТ) 28147-89, 34.11-94, 34.10-2001 — Soviet/Russian symmetric block cipher, hash function and digital signature algorithms

Other

Natural languages

- Russian: native
- English: fluent/C2 (IELTS 8.5 (out of 9))
- German: intermediate/B2 (TestDaF Niveaustufe 4 (out of 5))
- Swedish: pre-intermediate/B1