

Mohamed Amine NAJAH

Ph.D. Student in Computer Science



Info

Born **February 28th, 1987.**
in La Marsa Tunisia.
Citizenship **Tunisian, French.**
Marital status **Single.**

Contact

Email amine.najahi@univ-perp.fr.
Phone **(+33) (0)6 80 14 14 34.**
Address **Log 8D003, Résidence Canigou.**
18 bis avenue Alfred Sauvy.
66100 Perpignan - France.
Homepage <http://perso.univ-perp.fr/mohamedamine.najahi>.

Education

- 2011–present **Ph.D. student in Computer Science**, *Université de Perpignan Via Domitia*, Perpignan, *Supervised by [Matthieu Martel](#) and [Guillaume Revy](#) in the [DALI team \(UPVD-LIRMM\)](#).*
Title : *Synthesis of programs in the fixed-point arithmetic*
Topics : Fixed-point arithmetic ◊ Code synthesis for arithmetic expressions ◊ Linear algebra basic blocks in fixed-point arithmetic ◊ Numerical certification of fixed-point codes
- 2009–2011 **M.Sc. in Computer Science**, *Université Pierre et Marie Curie*, Paris, *[Parisian Master of Research in Computer Science](#)*.
Selection of courses followed : Cryptanalysis ◊ Arithmetic algorithms for cryptology ◊ Polynomial systems, computer algebra and applications ◊ Error correcting codes and applications to cryptography ◊ Efficient algorithms in computer algebra ◊ Cryptographic protocols : computational and symbolic proofs ◊ Number theory ◊ Advanced cryptology
- 2005–2009 **B.Sc. in Mathematics and Computer Science**, *Université Pierre et Marie Curie*, Paris, *cum laude*.
Selection of courses followed : Recursive programming ◊ Data structures and C programming ◊ Algorithmic ◊ Types and data structures ◊ Object-oriented programming ◊ Functions ◊ Sequences and integrals ◊ Arithmetic ◊ Algebra ◊ Group theory

PhD thesis

Title ***Synthesis of programs in the fixed-point arithmetic***

Supervisors [Matthieu Martel](#) and [Guillaume Revy](#)

Timeline Started **November 2011** / Thesis defense planned for **November 2014**.

Abstract In constrained environments like embedded systems, designs that rely on the fixed-point arithmetic are more efficient and consume less resources than floating-point ones. However, since the programmer is in charge of every arithmetical detail, writing fixed-point programs is a tedious and time consuming process. The goal of this thesis is to suggest and implement techniques in order to synthesize fixed-point programs. This synthesis process must achieve trade-offs between multiple conflicting goals such as the compactness of the design and its numerical quality. A second goal is to study the trade-offs involved in the fixed-point code generation of basic linear algebra routines such as dot-products, matrix-vector and matrix-matrix multiplication, as well as matrix inversion. *The thesis is supported by the [ANR DEFIS](#) project.*

Publications

International conferences with review committees and proceedings

- [1] **Toward the synthesis of fixed-point code for matrix inversion based on Cholesky decomposition**, joint work with Matthieu Martel and Guillaume Revy. Accepted for presentation at the Conference on Design and Architectures for Signal and Image Processing (DASIP 2014), Madrid, Spain, 8-10 October 2014..
- [2] **Automated Synthesis of Target-Dependent Programs for Polynomial Evaluation in Fixed-Point Arithmetic**, joint work with Christophe Moulleron and Guillaume Revy. Presented at the 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2014), Timisoara, Romania, 22-25 September 2014. .
- [3] **Code Size and Accuracy-Aware Synthesis of Fixed-Point Programs for Matrix Multiplication**, joint work with Matthieu Martel and Guillaume Revy. In A. Ahrens, C. Benavente-Peces , and J. Filipethe, editors, 4th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014) p. 204-214. Lisbon, Portugal, 7-9 January 2014.
- [4] **Design of Fixed-point Embedded Systems (DEFIS) French ANR Project**, joint work with Daniel Ménard, Romuald Rocher, Olivier Sentieys, Nicolas Simon, Laurent-Stéphane Didier, Thibault Hilaire, Benoît Lopez, Éric Goubault, Sylvie Putot, Franck Védrine, Guillaume Revy, Laurent Fangain, Christian Samoyeau, Fabrice Lemonnier, and Christophe Clienti. Demo Night of the Conference on Design and Architectures for Signal and Image Processing (DASIP 2012). Karlsruhe, Germany, 23-25 October 2012.

Abstract only conferences

- [5] **Approach based on instruction selection for fast and certified code generation**, joint work with Christophe Moulleron and Guillaume Revy. In 15th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics (SCAN'2012). Novosibirsk, Russia. 23-29 September 2012.

Research reports

- [6] **Automated Synthesis of Target-Dependent Programs for Polynomial Evaluation in Fixed-Point Arithmetic**, joint work with Christophe Moulleron and Guillaume Revy. Research report indexed at LIRMM-13006, 2013. Available at <http://hal-lirmm.ccsd.cnrs.fr/lirmm-00814338>.

Recent talks

- [1] **Automated Synthesis of Target-Dependent Programs for Polynomial Evaluation in Fixed-Point Arithmetic**, SYNASC 2014, Timisoara, Romania, September 22nd, 2014.
- [2] **Code Size and Accuracy-Aware Synthesis of Fixed-Point Programs for Matrix Multiplication**, PECCS 2014, Lisbon, Portugal, January 8th, 2014.
- [3] **Synthesis of fixed point programs : the case of matrix multiplication**, EJCIM 2013, Perpignan, France, April 12th, 2013.
- [4] **Synthesis of fixed-point programs based on instruction selection : the case of polynomial evaluation**, RAIM 2012, Dijon, France, June 22th, 2012.
- [5] **Mieux calculer avec un ordinateur (Improving computations' quality)**, Perpignan's doctoral seminar, Perpignan, France, June 7th, 2012.

Experience

- 2011 **5 months internship**, *LIP6 and INRIA laboratories*, Paris, supervised by [Jean-Charles Faugère](#), [Ludovic Perret](#), [Jean-Pierre Tillich](#), and [Ayoub Otmani](#).
This internship's goal is to work on the master's thesis.
- 2010 **1 month internship**, *LIP6 laboratory*, Paris, supervised by [Ludovic Perret](#).
« Algebraic cryptanalysis of a multivariate signature scheme »
- 2010 **4 months research project**, Paris, supervised by [Ludovic Perret](#) and [Guénaél Renault](#).
« Algebraic cryptanalysis of a symmetric family of ciphers : Katan & Ktantan »

Computer skills

Programming languages	C/C++, JAVA, Python, Lisp, ML	Computer arithmetic tools	GMP, MPFR, MPFI, Gappa, Sollya
Numerical computing environments	Matlab, Scilab, Octave	Computer algebra systems	Magma, Maple, Pari/GP, Sage Mathematica
Operating systems	UNIX, GNU/Linux, Windows, (POSIX systems)	Other	ΛT_EX, Gnuplot, Office Subversion, Emacs

Software development

[FPLA](#) (<http://perso.univ-perp.fr/mohamedamine.najahi/fpla/>)

- [1] *FPLA (Fixed-Point Linear Algebra) is a tool that synthesizes fixed-point codes for matrix multiplications and inversions. Its main goal is to find trade-offs between the accuracy of the generated code and its size. FPLA relies on the CGPE library for the synthesis of arithmetic expressions.*

[CGPE](#) (<http://cgpe.gforge.inria.fr>)

- [2] *CGPE (Code Generation for Polynomial Evaluation) is a synthesis tool (and library) of fast and certified codes for the evaluation of univariate and bivariate polynomials, in fixed-point arithmetic. So far it has been extended to handle sums, dot-products and fully parenthesized arithmetic expressions.*

Languages

Arabic	Mother tongue
French	Very fluent
English	Fluent
Chinese	Beginner level

participated to a high school exchange program in Virginia, USA

Interests

Reading
Traveling
Sports