

# Luca De Feo's *Curriculum Vitae*

last updated February 13, 2012

Laboratoire PRiSM  
Université de Versailles  
45 Avenue des États-Unis  
78035 Versailles Cedex  
France

Tel.: +33 1 39 25 40 17  
Fax: +33 1 39 25 40 57  
e-mail: [luca.de-feo@uvsq.fr](mailto:luca.de-feo@uvsq.fr)  
web: <http://www.prism.uvsq.fr/~df1>

Born May 26, 1983  
Sex: male  
Citizenship: Italian  
Status: single

## Research interests

---

Algorithmic number theory, computer algebra, cryptology, automated deduction.

## Employment

---

Sep 2011 – present	Laboratoire PRiSM, Université de Versailles	<b>Maitre de Conférences.</b>
Jul 2011 – Aug 2011	Combinatorics & Optimization, University of Waterloo	<b>Postdoctoral researcher.</b>
Dec 2010 – May 2011	IRMAR, Université de Rennes 1	<b>Postdoctoral researcher.</b>

## Education

---

2007–2010	École Polytechnique	<b>PhD</b> <i>Fast Algorithms for Towers of Finite Fields and Isogenies.</i> Defended December 13, 2010.
2004–2007	ENS Ulm (Paris)	<b>Diplôme de l'École Normale Supérieure</b> <i>Spécialité Informatique, Spécialité secondaire Mathématiques.</i>
2005–2007	ENS Ulm (Paris) – Département d'Informatique	<b>Master Parisien de Recherche en Informatique</b> <i>Mention: Bien.</i>
2004–2005	ENS Ulm (Paris) – Département de Mathématiques	<b>L3 (Bachelor) de Mathématiques.</b>
2001–2004	Università di Pisa – Dipartimento di Informatica	<b>Laurea triennale in Informatica (Bachelor)</b> <i>110/110 cum laude.</i>

## Research Papers

---

- David Jao and Luca De Feo. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies Post-Quantum Cryptography”. In: *Post-Quantum Cryptography*. Ed. by Bo-Yin Yang. Vol. 7071. Lecture Notes in Computer Science. Taipei, Taiwan: Springer Berlin / Heidelberg, 2011. Chap. 2, pp. 19–34. DOI: 10.1007/978-3-642-25405-5\_2.
- Luca De Feo. “Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies”. PhD thesis. Ecole Polytechnique X, Dec. 2010.
- Luca De Feo and Éric Schost. “Fast arithmetics in Artin-Schreier towers over finite fields”. In: *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*. Seoul, Republic of Korea: ACM, 2009, pp. 127–134. DOI: 10.1145/1576702.1576722.
- Luca De Feo. “Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic”. In: *Journal of Number Theory* 131.5 (May 2011), pp. 873–893. DOI: 10.1016/j.jnt.2010.07.003.
- Luca De Feo and Éric Schost. “transalpyne: a language for automatic transposition”. In: *SIGSAM Bulletin* 44.1/2 (2010), pp. 59–71. DOI: 10.1145/1838599.1838624.

- Luca De Feo and Éric Schost. “Fast Arithmetics in Artin-Schreier Towers over Finite Fields”. In: *Journal of Symbolic Computation* (Feb. 2011. Accepted). eprint: 1002.2594

## Software

---

- Sage implementation of “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies Post-Quantum Cryptography”. Available at <http://www.prism.uvsq.fr/~df1/>
- Contributor to Sage, the free open-source mathematics software system. <http://www.sagemath.com/>
- **FAAST. A library for Fast arithmetics in Artin-Schreier towers.** C++ library. <http://www.lix.polytechnique.fr/~defeo/FAAST/>
- **transalpyne. An implementation of the Transposable Algebraic Language.** Python program (compiler, interpreter). <http://transalpyne.gforge.inria.fr/>

## Awards

---

- **SIGSAM ISSAC 2009 Distinguished Student Author Award** for *Fast arithmetics in Artin-Schreier towers over Finite Fields*.

## Research Visits

---

Nov 2009–Jan 2010,	
Nov–Dec 2008,	
Mar 2008	University of Western Ontario, London (Ontario) – Computer Science Department, Symbolic Computation Lab <b>collaboration with E. Schost</b>
May 2009	University of Waterloo, Waterloo (Ontario) – Department of Combinatorics and Optimization, CACR
Mar–Sep 2006	McGill University, Montréal – School of Computer Science, Laboratoire de Crypto et Info Quantique <b>stage de M1: Simulation de fonctions booléennes non-inversibles under the direction of Claude Crépeau</b>
Jun–Sep 2005	Universitat Politècnica de Catalunya, Barcelona – Departament de Llenguatges i Sistemes Informàtics, ALBCOM team <b>stage de licence: Contrôle d’équivalence par approximation de fonctions under the direction of Jordi Cortadella</b>
Mar–Jul 2004	ASH, Pisa – Sezione Sviluppo Sistemi Informatici <b>stage della laurea triennale: Piattaforma embedded per il controllo remoto</b>

## Teaching

---

2011–present	Maître de Conférences <b>Licence et Master d’Informatique</b> <i>Univesité de Versailles</i> .
2009–2010	TA (moniteur) for the undergraduate course <b>IO2, Internet and Tools</b> at <i>Université Paris Diderot (Paris 7)</i>
2008–2009	TA (chargé de TDs) for the graduate course <b>INF568, Cryptology</b> at <i>École Polytechnique</i>
2008–2009	TA (chargé de TDs) for the undergraduate course <b>Modex Web</b> at <i>École Polytechnique</i>
2007–2008	TA (chargé de TDs) for the undergraduate course <b>INF311, Introduction to Computer Science</b> at <i>École Polytechnique</i>
2004–2006	Teacher of <b>Italian</b> and <b>Computer Science</b> at <i>Fresnes prison for the association Génèpi</i>

## Selected talks

---

### Peer-reviewed conferences and invited talks

- July 2010      **transalpyne: a language for automatic transposition**  
PLMMS (CNAM, Paris, France)
- August 2009    **Computing isogenies in small characteristic**  
ECC (University of Calgary, Canada)
- October 2009   **Fast Arithmetics for Artin-Schreier Extensions**  
RAIM (ENS Lyon, France)
- July 2009      **ISSAC (KIAS, Seoul, South Korea)**

### Other conferences and summer schools

- June 2011      **Explict isogenies and implementations**  
Géocrypt (Bastia, France)
- April 2011     **Explict isogenies: recent progress and implementations**  
C2 (CAES CNRS, Saint-Pierre d'Oléron, France)
- July 2009      **Computing isogenies in small characteristic**  
Journées Arithmétiques (Univestité Jean Monnet, Saint-Étienne, France)
- December 2008 **Fast Arithmetics for Artin-Schreier Extensions**  
CMS Winter Meeting (Ottawa, Canada)
- May 2008      **Dualities and Transposition principle**  
C4 (École Polytechnique, Palaiseau, France)
- October 2008   **JNCF (Luminy, France)**

## Various knowledges & experiences

---

- **Spoken languages:** *Italian* (native), *French* (bilingual), *English* (fluent), *Spanish* (good), *Sardinian* (basic).
- **Programming languages:** bash, C, C++, Haskell, Java, Javascript, Perl, PHP, Python, OCaml, SQL.
- **Markup languages:** CSS, HTML, L<sup>A</sup>T<sub>E</sub>X, XHTML, XML.
- **Mathematical software:** Magma, Maple, Sage.

## Hobbies

---

- DJing, sound and light engineering (head of the BOUM team for the *Association des Elèves de l'ENS* from 2006 to 2008).
- Basketball.