Gabrielle De Micheli

General Information

- Adress: Distributed Systems Lab, 3300 Walnut St, Philadelphie, PA, 19104, USA
- Email: gmicheli@seas.upenn.edu
- https://www.seas.upenn.edu/∼gmicheli/

- Nationality: American, French, Italian, Swiss
- Place and Date of Birth: Palo Alto, CA, February 11^{th}, 1993

Scientific Interests

Cryptography, Security, Computational Number Theory, Lattices, Algebra (Group Theory, Representation Theory), Geometry (Riemannian Geometry), General Relativity.

Education

Current Work

Sep 2016 - current **PhD in Computer Science**, *University of Pennsylvania*, Philadelphia, USA.

My work lies at the intersection of Mathematics and Cryptography, with particular research interests in the Number Field Sieve (NFS) algorithm, Zero-knowledge proofs and ideal lattices. I am interested in both attacks and defenses with a particular interest in using mathematical techniques for obtaining a better understanding of the security properties of commonly used cryptographic primitives in real-world applications.

Past Degrees

Sept 2016 **Master of Mathematics**, *EPFL, Ecole Polytechnique Fédérale de Lausanne*, Lausanne, Switzerland.

Master Thesis

Title *The Riemannian Penrose Inequality*

Supervisors Prof. Marc Troyanov & Prof. Spyros Alexakis

July 2014 **Bachelor of Mathematics**, *EPFL, Ecole Polytechnique Fédérale de Lausanne*, Lausanne, Switzerland.

International experience

Sep 2015-Jan 2016 **Semester abroad (Master thesis)**, *Imperial College*, London, UK.

Sep 2013-June 2014 **Erasmus year**, *Heriot-Watt University*, Edinburgh, Scotland, UK.

Seminars

Mai 2017 **GREPSEC Workshop**, *Seminar in computer security research*, San Jose, CA, USA.

Sept 2015 **School on Geometric Aspects of General Relativity**, *Université de Montpellier*, Montpellier, France.

Projects in mathematics

December 2014 **Understanding gravitational multi-instantons**.

June 2014 **Braid Group, Hecke and Temperley-Lieb algebras**.

December 2013 **Galois Theory**.

June 2013 **Discrete Logarithm Problem on Elliptic Curves**.

Publications

Dall, De Micheli, Eisenbarth, Genkin, Heninger, Moghimi, Yarom **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *Cryptographic Hardware and Embedded Systems (CHES)*, 2018.

De Micheli, Shani, Heninger **Characterizing Overstretched NTRU Attacks**, *In submission*, 2018.

Talks and presentations

Avril 2018 **Computational Challenges in the Theory of Lattices**, *Brown University*, Providence, USA.
Poster presentation

Teaching Experience

Feb -June 2013 **Teaching assistant for General Physics II**, *EPFL*, Lausanne.

Editorial tasks

Crypto 2017 **Subreviewer**.

Sep 2014 - June 2015 **Translator**, *Exercises and solutions for Analysis I and II, translation from French to English*, EPFL, Lausanne.

Computer skills

Basic Matlab, HTML

Intermediate Python, Sage, LaTeX

Languages

French **Mothertongue**

English **Fluent**

Italian **Fluent**

German **Basic**

Additional Interests

Sailing	**Club de voile Morges**	*Several international competitions*
	Club de voile EPFL	*Vice-president and treasurer, 2012-2013*
	Sailing instructor	*Glénans, France, summers 2011-2014*
Skiing	**Ski-Club Villars**	*2008-2010*
Basketball	**Heriot-Watt Ladies team**	*Sep 2013 - June 2014*
Piano	**Ecole Sociale de Musique, Lausanne**	*2004-2015*
Humanitarian	**Project EMahP**	*Teaching math in South Africa, July 2013*
Other	Alpinism, Climbing, Traveling	