



# Gabrielle De Micheli

---

## General Information

- Address: Distributed Systems Lab, 3300 Walnut St, Philadelphia, PA, 19104, USA
- Email: gmicheli@seas.upenn.edu
- <https://www.seas.upenn.edu/~gmicheli/>
- Nationality: American, French, Italian, Swiss

## 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 lattice-based cryptography, computational number theory, and the Number Field Sieve algorithm. 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

Oct 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.

## 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

- De Micheli, Shani, Heninger **Characterizing Overstretched NTRU Attacks**, to appear at *Mathcrypt*, 2018.  
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.

---

## Talks and presentations

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

---

## Teaching Experience

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

---

## Editorial tasks

- Reviewer **Crypto 17', Asiacrypt 18'.**  
Translator **Exercises and solutions for Analysis I and II, translation from French to English**, *EPFL*, Lausanne, Sep 2014 - June 2015.

---

## Computer skills

Matlab, HTML,  $\text{\LaTeX}$ , Python, Sage

---

## Languages

- Fluent **English, French, Italian**  
Basic **German**