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

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

May 2018 **Master of Computer Science**, *University of Pennsylvania*, Philadelphia, PA, USA.

Under the supervision of Nadia Heninger: Lattice-based cryptography

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**, *Mathcrypt, to appear in Journal of Mathematical Cryptology*, 2018.

Dall, De Micheli, Eisenbarth, Genkin, Heninger, Moghimi, Yarom **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *CHES, published in IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(2)*, 2018.

Invited Talks and Workshops

September 2018 **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *Security Seminar*, MIT, Boston, USA.
Talk

September 2018 **CacheQuote attack and Hidden Number Problem performance analysis**, *Security Seminar*, University of Pennsylvania, USA.
Talk

August 2018 **Characterizing overstretched NTRU Attacks**, *Mathcrypt*, Santa Barbara, USA.
Talk

Avril 2018 **Hidden Number Problem: Performance Analysis**, *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', CHES 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, LaTeX, Python, Sage

Languages

Fluent	English, French, Italian
Basic	German