

Gabrielle De Micheli

Personal Information

- Date and place of birth: 11th February 1993, Palo Alto, CA, USA
- Citizenship: Swiss, French, Italian, American
- Email: gdemicheli@ucsd.edu
- Web page: <https://gmicheli.github.io/>
- OrCID: 0000-0002-2617-6878

Employment

- May 2023- current **Consulting**, *Beyond Aerospace Ltd.*
- Sept 2021- current **Postdoctoral scholar**, *University of California, San Diego (UCSD)*.
Funded by Early Postdoc.Mobility Fellowship (18 months) and by the UCSD CSE Fellows Program.

Education

- May 2021 **PhD in Computer Science**, *University of Lorraine*, Nancy, France.
Advisors: Pierrick Gaudry, Cécile Pierrot
- May 2018 **Masters in Computer Science**, *University of Pennsylvania*, Philadelphia, USA.
- Oct 2016 **Masters in Mathematics**, *EPFL, Swiss Institute of Technology*, Lausanne, Switzerland.
- July 2014 **Bachelor in Mathematics**, *EPFL, Swiss Institute of Technology*, Lausanne, Switzerland.

Academic distinctions and Fellowships

- March 2023 **UCSD CSE Fellowship**, *from the CSE Fellows Program.*
- October 2022 **Finalist**, *ERCIM Cor Baayen Young Researcher Award*, Nominated by Inria.
- January 2022 **Thesis prize Gilles Kahn 2021**, *from Société Informatique de France (SIF) for an excellent thesis in Computer Science.*
- December 2021 **Award paper**, *Asiacrypt 2021*, for *Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation.*
- October 2021 **Young Talent for Women in Science prize 2021**, *from the Foundation l'Oréal-UNESCO.*
- September 2021 **Early Postdoc.Mobility Fellowship**, *from the Swiss National Science Foundation.*

Publications

- Nam, Zhou, Gupta, De Micheli, Cammarota, Wilkerson, Micciancio, Rosing **Efficient Machine Learning on Encrypted Data using Hyperdimensional Computing**, *ISLPED*, to appear in the proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design , 2023.

- De Micheli, Micciancio, Pellet-Mary, Tran **Reductions from module lattices to free module lattices, and application to dequantizing module-LLL**, *Crypto*, to appear in Advances in Cryptology – Crypto, 2023.
- De Micheli, Gaudry, Pierrot **Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation**, *Asiacrypt*, published in Advances in Cryptology – Asiacrypt, 2021.
- De Micheli, Gaudry, Pierrot **Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields**, *Crypto*, published in Advances in Cryptology – Crypto, 2020.
- De Micheli, Piau, Pierrot **A Tale of Three Signatures: practical attack of ECDSA with wNAF**, *Africacrypt*, published in Progress in Cryptology – Africacrypt, 2020.
- De Micheli, Shani, Heninger **Characterizing Overstretched NTRU Attacks**, *Mathcrypt*, published 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 (2), 2018.

Unpublished work

- De Micheli, Kim, Micciancio, Suhl **Faster Amortized FHEW bootstrapping using Ring Automorphisms**, *Cryptology ePrint Archive: Report 2023/112*, 2023, In submission.
- De Micheli, Micciancio **A fully classical LLL algorithm for modules**, *Cryptology ePrint Archive: Report 2022/1356*, 2022, Merged with Crypto 2023 accepted paper.
- De Micheli, Heninger **Recovering cryptographic keys from partial information, by example**, *Cryptology ePrint Archive: Report 2020/1506*, 2021.

Invited talks and presentations

- May 2023 **Algebraically structured lattices in Cryptography**, *Theory seminar*, UCSD.
- February 2023 **Faster Amortized FHEW Bootstrapping using Ring Automorphisms**, *FHE.org*, Virtual seminar.
- October 2022 **Faster amortized FHEW bootstrapping**, *Intel Frontier Workshop*, Portland, USA.
- June 2022 **Cryptanalyses de logarithmes discrets (in French)**, *Journées nationales du GDR Sécurité Informatique*, Paris, France.
- April 2022 **Énumération de réseaux pour Tower NFS : un calcul de logarithme discret de 521 bits (in French)**, *ECO seminar*, Montpellier, France.
- April 2022 **Discrete logarithm cryptanalysis**, *Stanford University*, Palo Alto, USA.
- March 2022 **Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation**, *AWM seminar*, UC San Diego, USA.
- February 2022 **Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation**, *Number Theory seminar*, UC San Diego, USA.
- December 2021 **Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation**, *Asiacrypt 2021*, Virtual conference.
- November 2021 **Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation**, *Theory seminar*, UC San Diego, USA.
- October 2021 **Key recovery from partial information**, *Cryptography seminar*, Rennes, France.
- November 2020 **Discrete logarithm algorithms in pairing-relevant finite fields**, *Journées Codage et Cryptographie C2 2020*, Virtual conference.
- August 2020 **Discrete logarithm algorithms in pairing-relevant finite fields**, *Crypto 2020*, Virtual conference.

- July 2020 **A Tale of Three Signatures: practical attack of ECDSA with wNAF**, *Africacrypt 2020*, Virtual conference.
- February 2020 **Pairings and security of the discrete logarithm problem in finite fields**, *Security seminar*, Boston University, Boston, USA.
- February 2020 **Pairings and security of the discrete logarithm problem in finite fields**, *Theory seminar*, University of Northeastern, Boston, USA.
- Décembre 2019 **A Tale of Three Signatures: practical attack of ECDSA with wNAF**, *IMA International Conference on Cryptography and Coding*, Oxford, UK.
- September 2018 **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *Conference on Cryptographic Hardware and Embedded Systems (CHES) 2018*, Amsterdam, Netherlands.
- September 2018 **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *Security seminar*, MIT, Boston, USA.
- Septembre 2018 **CacheQuote: Efficiently Recovering Long-term Secrets of SGX EPID via Cache Attacks**, *Security seminar*, University of Pennsylvania, Philadelphia, USA.
- August 2018 **Characterizing overstretched NTRU Attacks**, *Mathcrypt*, Santa Barbara, USA.

Major scientific achievements

Record computations

- February 2021 **Discrete logarithm computation in $GF(p^6)$ of 521 bit with Tower NFS**, with Pierrick Gaudry and Cécile Pierrot, Record announced in the mailing list NMBRTHRY of number theory.

Common Vulnerabilities Exposures (CVE)

- May 2018 **CVE-2018-3691**, for the CacheQuote attack.

Scientific activities

- Co-Organizer **Workshop on Attacks in Cryptography (WAC5)**, affiliated with *Crypto 2022*, with Shaanan Cohney.
- Program committees **ACM CCS 22',23' Crypto 23', Eurocrypt 24'**.
- External reviewing **Crypto 17'/22', Asiacrypt 18'/19'/22', CHES 18', Designs, Codes and Cryptography (journal), Eurocrypt 20'/22'/23'**.
- Translation **Exercises and solutions for Calculus I and II**, translation from French to English, EPFL, Lausanne, Sep 2014 - June 2015.
- Outreach **Television report, Arte journal**, *Cybersécurité: la science des codes secrets*, July 26 2021.
- Panel on Women in CS**, École Polytechnique (France) - Université de Yaoundé I (Cameroon), December 20 2022.

Teaching activities

Supervision of students

- May-July 2019 **Co-advising undergraduate internship for a student from ENS Rennes, INRIA, Nancy, France**, student name: Rémi Piau.
Project: The student implemented and improved an attack designed by myself which allowed to break the signature algorithm ECDSA using partial information collected from a side-channel attack. This collaborative work led to the paper *A Tale of Three Signatures: practical attack of ECDSA with wNAF* accepted at Africacrypt 2020 and published in its proceedings.

Courses

- Dec 2020 - Jan 2021 **Introduction à l'apprentissage automatique (in French), exercise sessions**, *École des Mines, second year*, Nancy, France.
- Oct - Dec 2020 **Python (in French), exercise sessions**, *École des Mines, first year*, Nancy, France.
- Jan - March 2020 **Cryptography and Authentication (in English), Lectures and exercise sessions**, *Télécom Nancy (ESIAL), second year ISS*, Nancy, France.
- Jan - March 2020 **Introduction to Cryptography (in English), Lectures and exercise sessions**, *Télécom Nancy (ESIAL), second year Formation par Apprentissage*, Nancy, France.
- Feb -June 2013 **General Physics II (in English), exercise sessions**, *EPFL*, Lausanne, Switerland.

Other

- July 2013 **Humanitarian project EMaHP (EPFL Mathematic Humanitarian Project)**, *workshops and vulgarisation of mathematics for students from middle school and highschool*, South Africa.