Gabrielle De Micheli, PhD

gdemicheli@ucsd.edu · gmicheli.github.io · +1 (760) 208 8039

Scientific Interests

Researcher with expertise in **Mathematics and Applied Cryptography**, with particular research interests in post-quantum cryptography, lattice-based cryptography, fully homomorphic encryption and computational number theory. Experience in both cryptographic attacks and defenses, and using mathematical techniques to obtain a better understanding of the security properties of commonly-used cryptographic primitives in real-world applications.

Experience

Oct 2023- current **Visiting Scholar**, *University of California, San Diego*, Department of Electrical and Computer Engineering, with Prof. Farinaz Koushanfar.

- **Applied Cryptography**: Working on 3 research projects in Electrical Engineering (Prof. Farinaz Koushanfar) and Computer Science (Prof. Tajana Rosing) on lattice-based cryptography, fully homomorphic encryption, and zero-knowledge proofs with specific focus on applications
- **Working on an industry collaboration** with Intel Labs
- Presented 5 talks at international conferences (4 invited) and invited speaker on 2 panels
- **CIC Journal editorial board**, serving as a reviewer
- **Program committees of 2 international conferences**, serving as a reviewer
- Published 2 academic papers in Journals (Communications in Cryptology and Journal of Cryptology)

Oct 2023- May 2024 **Senior Cryptographer**, *Beyond Aerospace Ltd.*

- **Applied Post-Quantum Cryptography**: Created a post-quantum transition roadmap and implementation plan. Incorporated post-quantum protocols in company's software platform. The task included developing and integrating C and Go code to enhance the existing software platform with post-quantum cryptographic capabilities through a flexible API
- Assisted marketing efforts with **post-quantum technical proposals and feasibility studies**
- Researched evolving quantum-secure cryptographic algorithms and their applications

May 2023- Oct 2023 **Consultant**, *Beyond Aerospace Ltd.*

- **Post-quantum vulnerability assessment** of company's existing software platform
- Identification of suitable post-quantum replacement cryptographic algorithms
- Developing post-quantum transition roadmap and implementation plan
- Writing grant proposal for post-quantum development in software platform

Sept 2021- Oct 2023 **Postdoctoral scholar**, *University of California, San Diego (UCSD) with Prof. Daniele Micciancio*, funding awarded by Early Postdoc Mobility Fellowship from the Swiss National Science Foundation (18 months) and by the UCSD CSE Fellows Program.

- Led research project in **lattice-based cryptography** analysing algebraic hardness assumptions used in the new post-quantum algorithms to be standardized by NIST. Publication at top-tier conference (IACR Crypto 2023)
- Led research project and advised PhD student on **fully homomorphic encryption**. Publication at top-tier conference (IACR PKC 2024)
- Participated in collaboration with **industry partner**, Intel Labs
- Initiated and developed collaboration with reasearch group within UCSD to develop **practical application of fully homomorphic encryption**. Collaboration led to one publication (ISLPED 2023) and is still on-going
- Promoted research work through 10 invited talks and 2 conference presentations
- Reviewed academic work by being in program commitees of 2 top-tier conferences in the field

Education

May 2021 **PhD in Computer Science**, *University of Lorraine*, Nancy, France.
Thesis: Discrete Logarithm Cryptanalyses: Number Field Sieve and Lattice Tools for Side-Channel Attacks.

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 best PhD thesis in all Computer Science in France*.

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*.

Grants

June 2024 **AWM Travel Grant**, *to travel to Eurocrypt 2024 in Zurich, Switzerland*, 3.5K.

Publications

De Micheli, Kim, Micciancio, Suhl **Faster Amortized FHEW bootstrapping using Ring Automorphisms**, *PKC*, published in Lecture Notes in Computer Science, 2024.

De Micheli, Gaudry, Pierrot **Lattice Enumeration and Automorphisms for Tower NFS: a 521-bit Discrete Logarithm Computation**, *Journal of Cryptology*, 2024.

De Micheli, Heninger **Survey: Recovering cryptographic keys from partial information, by example**, *Communications in Cryptology*, 2024.

Nam, Zhou, Gupta, De Micheli, Cammarota, Wilkerson, Micciancio, Rosing **Efficient Machine Learning on Encrypted Data using Hyperdimensional Computing**, *ISLPED*, published 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*, published 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.

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

De Micheli, Shani, Heninger **Characterizing Overstretched NTRU Attacks**, *Mathcrypt*, published in Journal of Mathematical Cryptology, 2018.

Unpublished work

De Micheli, Micciancio **A fully classical LLL algorithm for modules**, *Cryptology ePrint Archive: Report 2022/1356*, 2022, Merged with Crypto 2023 accepted paper.

Major scientific achievements

Record computations

February 2021 **Discrete logarithm computation in $GF(p^6)$ of 521 bit with Tower NFS**, *with Dr. Pierrick Gaudry and Dr. 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*.

Invited talks and presentations

April 2024 **Algebraically structured lattices in Cryptography**, *Cyber Group seminar series*, Melbourne University, Australia.

April 2024 **Faster Amortized FHEW bootstrapping using Ring Automorphisms**, *PKC*, Sydney, Australia.

January 2024 **Reductions from module lattices to free module lattices, and applications to dequantizing module-LLL**, *Joint Mathematics Meetings*, San Francisco, USA.

December 2023 **Algebraically structured lattices in Cryptography**, KEYNOTE *at WoCC'23-Women in Computer Science Cameroon*, Polytech School of Yaounde Cameroon, Cameroon.

October 2023 **Algebraically structured lattices in Cryptography**, *AWM Research Symposium*, Atlanta, USA.

August 2023 **Reductions from module lattices to free module lattices, and application to dequantizing module-LLL**, *Crypto 2023*, Santa Barbara, USA.

May 2023 **Algebraically structured lattices in Cryptography**, *Theory seminar*, UC San Diego, USA.

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 discret logarithm problem in finite fields**, *Security seminar*, Boston University, Boston, USA.

February 2020 **Pairings and security of the discret logarithm problem in finite fields**, *Theory seminar*, University of Northeastern, Boston, USA.

Decembre 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.

Scientific activities

Co-Organizer **Workshop on Attacks in Cryptography (WAC5)**, *affiliated with Crypto 2022*, with Shaanan Cohney.

Program committees **ACM CCS 22',23', Thesis prize Gilles Kahn 22', 23', IACR Crypto 23', IACR Eurocrypt 24'**.

External reviewing **Crypto 17'/22'/24', Asiacrypt 18'/19'/22', CHES 18', Designs, Codes and Cryptography (journal), Eurocrypt 20'/22'/23'**.

Editorial Board **IACR Communications in Cryptology**, *2024-*.

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)*, 2022-2023.

Panel and discussion, *Quantum Algorithms for lattice problems*, PKC, Sydney, April, 2024.

Teaching activities

Supervision of master and undergraduate internships

June-Aug 2024 **Advising master student internship for a student from ENS Rennes (France)**, *at UC San Diego*, USA, student name: Guilhem Repetto.
Project: The student will focus on zero-knowledge proofs and applications to security and privacy.

May-July 2019 **Co-advising undergraduate internship for a student from ENS Rennes (France)**, *at 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 lead 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.