**Miquel Guiot Cusidó**
(Barcelona, the 9th of April 1998)
Email: miquel.guiotc@gmail.com
Webpage : https://miquelguiot.github.io/

## PROFESSIONAL PROFILE

Interested in the research fields of **cryptography, high performance computing,** and **computational algebra.** Willingness to adhere to **research** and **investigation processes** involving **learning; dynamism; teamwork; interaction** and **challenges.** My main qualities are the **ability to learn; commitment; planning; organisation; coordination** and **initiative.**

## EDUCATION

### REGULATED EDUCATION

- 2024 - Now **Ph.D. Student in Cryptography**
  ***Better secret sharing schemes for general access structures***
  Universitat Rovira I Virgili, Computer Science and Mathematics Dept.
  Advisor: Oriol Farràs Ventura
  Expected date of graduation: Dec 2027.

- 2022 - 2023 **MSc in Advanced Mathematics**
  Universitat de Barcelona
  Expedient grade: 9.7/10

- 2016 - 2022 **Double Bachelor in Mathematics and Computer Science**
  Universitat de Barcelona
  Expedient grade: 8.9/10

### MAIN THESIS

- 2022 - 2023 **Master's Thesis**
  ***Large images for Galois representations attached to modular forms***
  Advisor: Luis Victor Dieulefait
  Expedient grade: 10/10
  Extraordinary Award for the Best Master's Thesis

- 2021 - 2022 **Bachelor's Thesis**
  ***NTRU Cryptosystem: A solution to the quantum threat***
  Advisor: Xavier Guitart Morales
  Expedient grade: 9.8/10

## PROFESSIONAL EXPERIENCE

- 2024 – Now **Ph.D. Student in Cryptography**
  ***Better secret sharing schemes for general access structures***
  Universitat Rovira I Virgili, Computer Science and Mathematics Dept.

  Optimization of secret sharing schemes for general access structures, with special attention to reducing the share size and the computational cost of share generation and secret reconstruction. Since starting my PhD, I have worked in three main topics: improving the efficiency of weighted threshold secret sharing, studying traceable secret sharing for general access structures, and improving side-channel attacks for AES.

  This work has resulted in four papers: one published at TCC 2024, one at CHES 2026, and two preprints.

- 2022 - 2023 **Research Engineer, Barcelona Supercomputing Center (BSC-CNS)**
  Memory Systems group, Computer Sciences Department.
  Research in memory systems for high-performance computing. Collaborating with *Micron Technologies US* on novel memory architectures, focusing in the areas of Processing in Memory (PIM), and Compute Express Link (CXL).

  During this period, my main tasks involved the study of algorithms on PIM devices via computational complexity theory and the development of analytical models for novel memory architectures such as CXL using queueing theory. perspectives.

  My work culminated in the publication of a paper at IEEE Transactions on Computers, where we presented a new processing in memory device for optimizing key-value sort algorithms.

- 2022 - 2023 **Associate Professor, Universitat de Barcelona**
  Teaching course: *Operating Systems*, Degree in Computer Science.
  Theoretical and practical classes, preparation of notes, activities and practices. Correction of exercises and exams. Assisting students in laboratory classes. Carrying out revision classes and resolving doubts. Individual assistance to students. Cooperation in the organisation of the course.

- 2019 - 2020 **Teaching Assistant, Universitat de Barcelona**
  Teaching course: *Software Design*, Degree in Computer Science.
  Preparation of notes, activities and practices. Correction of exercises. Assisting students in laboratory classes. Carrying out revision classes and resolving doubts. Individual assistance to students. Cooperation in the organisation of the course.

## TECHNICAL SKILLS AND COMPETENCIES

- **Programming Languages and Derivatives:**

  Python, R, Matlab, Shell scripting (Bash), Mathematica, Java, C, C++, Javascript, Kotlin, SageMath, HTML and SQL

- **Mathematics and Statistics:**

  Good background in undergraduate and graduate mathematics.
  Work and research experience in cryptography, cryptanalysis, complexity theory, queueing theory, probability and statistics.
  Deep understanding of number theory and algebra: computational algebra, category theory, algebraic topology, algebraic geometry, homological algebra, Langlands program.

- **Computer Architecture:**

  Good background in computer architecture and microarchitecture, especially in high performance computing and memory systems.
  Work and research experience with novel memory architectures, Processing in Memory (PIM) devices and Compute Express Link (CXL).

- **Analytical Modelling:**

  Work experience in the design and development of analytical models for predicting and estimating performance of novel memory architectures.
  Application of complexity theory, queueing theory, probability theory and statistics in the design of analytical models.

## PEER-REVIEWED PUBLICATIONS

- 2026 Oriol Farràs, Miquel Guiot. ***Traceable Secret Sharing Schemes for General Access Structures,*** Eurocrypt 2026. Full version available at ePrint.

- 2026 Oriol Farràs, Miquel Guiot. ***Revisiting Beimel-Weinreb Weighted Threshold Secret Sharing Schemes,*** IEEE Computer Security Foundations Symposium (CSF) 2026. Full version available at ePrint.

- 2025 Oriol Farràs, Vincent Grosso, Miquel Guiot, Carlos-Andrés Lara-Nino. ***Improving the Selection Rule of Correlation Attacks for Remote Power Analysis***, Conference on Cryptographic Hardware and Embedded Systems (CHES) 2026. Full version available at ePrint.

- 2024 Oriol Farràs, Miquel Guiot Cusidó. ***Reducing the Share Size of Weighted Threshold Secret Sharing Schemes via Chow Parameters Approximation***, Theory of Cryptography Conference (TCC) 2024. Full version available at ePrint.

- 2024 Pouya Esmaili-Dokht, Miquel Guiot Cusidó *et al.* ***O(n) Key-value Sort with Active Compute Memory***, IEEE Transactions on Computers.

## PREPRINTS

- 2026 Oriol Farràs, Miquel Guiot. ***Information-theoretic Strong Traceable Secret Sharing Schemes,*** Submitted. Full version available at ePrint.

## SCIENTIFIC TALKS

- 2026 ***Traceable Secret Sharing Schemes for General Access Structures***, Eurocrypt 2026, Roma.

- 2026 ***Traceable Secret Sharing Schemes for General Access Structures***, MAK Seminar UPC, Barcelona.

- 2025 ***Weighted Threshold Secret Sharing Schemes***, Primeras Jornadas Sobre criptografía aplicada a la seguridad y a la privacidad en ciencias de datos, Castro Urdiales.

- 2025 ***Weighted Threshold Secret Sharing Schemes***, Workshop on Secret Sharing Schemes, Tarragona.

- 2025 ***Weighted Threshold Secret Sharing Schemes***, CyberSec+ Doctoral Workshop, Lleida.

- 2025 ***Weighted Threshold Secret Sharing Schemes***, Congreso Jóvenes de la RSME, Bilbao.

- 2024 ***Reducing the Share Size of Weighted Threshold Secret Sharing Schemes via Chow Parameters Approximation***, Theory of Cryptography Conference (TCC), Milan

- 2024 ***Reducing the Share Size of Weighted Threshold Secret Sharing Schemes via Chow Parameters Approximation***, MAK Seminar UPC, Barcelona

- 2024 ***Reducing the Share Size of Weighted Threshold Secret Sharing Schemes via Chow Parameters Approximation***, Deiminari URV, Tarragona

## TEACHING

- 2022 ***Software Design***, BSc in Computer Science, Universitat de Barcelona
- 2023 ***Operating Systems***, BSc in Computer Science, Universitat de Barcelona
- 2024 ***Discrete Mathematics II***, BSc in Computer Science, Universitat Rovira I Virgili
- 2025 ***Discrete Mathematics II***, BSc in Computer Science, Universitat Rovira I Virgili

## LANGUAGES

- Catalan: native language and C2 level.
- Spanish: spoken, read and written perfectly, C2 level.
- English: *Advanced Certificate*, C1 level.
- German: B1 level.

## GRANTS

- 2024 **Grant for Development of Researchers**
  Beca del programa de formación de personal investigador – FPI
  Ministry of Science and Education, Spain
- 2024 **Young Researcher at 11th Heidelberg Laureate Forum**
  One of the 200 carefully selected young researchers in mathematics and computer science
  Klaus Tschira Stiftung, Germany
- 2019 **Grant for Teaching Assistants**
  Beca de col·laboració de la Universitat de Barcelona
  Universitat de Barcelona

## SERVICE

- **Scientific Papers Revision**

  I have reviewed papers for the following conferences:
  ACISP'24, CCS'24, EUROCRYPT'24, ICDE'25, ESORICS'25, TCC'26.

- **Scientific Informative Talks**

During 2024 and 2025 I have presented a scientific divulgative talk titled *Blockchain Technology: Far Beyond Cryptocurrencies* to more than 30 high schools in Spain.

During 2024 and 2025 I have presented a scientific divulgative talk titled *Privacy and Security on the Internet* to more than 10 high schools in Spain.

## AWARDS

- 2023 Extraordinary Award for the Best Master's Thesis

## OTHER INFORMATION OF INTEREST

Reference letters are available upon request.

Miquel Guiot Cusidó

Barcelona, the 19th of December 2025