

# Thomas Debris-Alazard

BORN IN PARIS, FRANCE, MAY 1, 1991 · RESEARCHER SCIENTIST AT INRIA

✉ (+33) 631053595 | 📩 thomas.debris@inria.fr | 🌐 http://tdalazard.io/

## Research Interests

---

**Public-Key Cryptography with a focus on code- and lattice-based cryptography**

- **Cryptographic designs, cryptanalysis, reductions**
- **Algorithms** classical and quantum
- **Security estimates** study of generic decoding problems
- **Security proofs** in the classical or quantum model

## Employment

---

### École Polytechnique

Saclay, France

TEACHER ASSISTANT (CHARGÉ D'ENSEIGNEMENT)

Sept. 2022 - Present

Département d'Informatique de l'École Polytechnique (DIX)

### Inria Saclay

Saclay, France

RESEARCHER SCIENTIST (CHARGÉ DE RECHERCHE)

Sept. 2020 - Present

Project-Team: Grace

### Royal Holloway, University of London, UK

London, UK

POSTDOC IN THE INFORMATION SECURITY GROUP

Sept. 2019 - Sept. 2020

Hosted by Pr Martin R. Albrecht

## Education

---

### Inria Paris

Paris, France

PH.D., CODE-BASED CRYPTOGRAPHY: NEW APPROACHES FOR DESIGN AND PROOF ; CONTRIBUTION TO  
CRYPTANALYSIS

Sept. 2016 - Sept. 2019

Advisor: Pr Jean-Pierre Tillich

### École Normale Supérieure de Cachan (ENS)

Paris, France

THESIS, CODE-BASED CRYPTOGRAPHY: STUDY OF A GENERIC DECODING ALGORITHM, STATISTICAL DECODING

Mar. 2016 - Sept. 2016

Advisor: Pr Jean-Pierre Tillich

MASTER MPRI (PARISIAN MASTER OF RESEARCH IN COMPUTER SCIENCE).

Sept. 2015 - Sept. 2016

Main Topics: Cryptography, Complexity, Security reductions, Gröebner basis, Quantum algorithms

AGRÉGATION DE MATHÉMATIQUES OPTION INFORMATIQUE.

Sept. 2014 - Sept. 2015

## Honors and Awards

---

### 2026-2031 ERC Starting Grant

1.5M€

IQ-SCALE: IRONCLAD QUANTUM SECURITY OF CODE- AND LATTICE-BASED CRYPTOGRAPHY

### 2021-2025 ANR JCJ

200 k€

COLA: AN INTERFACE BETWEEN CODE AND LATTICE-BASED CRYPTOGRAPHY

### 2021 Finalist for the Cor Baayen Young Researcher Award

ERCIM

### 2020 Gilles Kahn Thesis Award

Société Informatique de  
France

THOMAS DEBRIS-ALAZARD UNDER THE SUPERVISION OF JEAN-PIERRE TILLICH

- 2019 **Best Paper Award, Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes**

*Asiacrypt '19*

THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILlich

## Scientific Publications

---

- 2025 **Worst and Average Case Hardness of Decoding via Smoothing Bounds** *PKC '25*  
THOMAS DEBRIS-ALAZARD AND NICOLAS RESCH
- 2024 **New Solutions to Delsarte's Dual Linear Programs** *IEEE Information Theory '24*  
ANDRÉ CHAILLOUX AND THOMAS DEBRIS-ALAZARD
- 2024 **Exploiting signature leakages: breaking Enhanced pqsigRM** *ISIT '24*  
THOMAS DEBRIS-ALAZARD, PIERRE LOISEL AND VALENTIN VASSEUR
- 2024 **Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs** *STOC '24*  
THOMAS DEBRIS-ALAZARD, POURIA FALLAHPOUR AND DAMIEN STEHLÉ
- 2024 **Reduction from sparse LPN to LPN, Dual Attack 3.0** *Eurocrypt '24*  
KEVIN CARRIER, THOMAS DEBRIS-ALAZARD, CHARLES MEYER-HILFIGER AND JEAN-PIERRE TILlich
- 2023 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem** *IEEE Information Theory '23*  
THOMAS DEBRIS-ALAZARD, MAXIME REMAUX AND JEAN-PIERRE TILlich
- 2023 **On the pseudorandomness of the decoding problem via the Oracle Comparison Problem** *Asiacrypt '23*  
MAXIME BOMBAR, ALAIN COUVREUR AND THOMAS DEBRIS-ALAZARD
- 2023 **Smoothing codes and lattices: systematic study and new bounds** *IEEE Information Theory '23*  
THOMAS DEBRIS-ALAZARD, LÉO DUCAS, NICOLAS RESCH AND JEAN-PIERRE TILlich
- 2022 **Statistical Decoding 2.0: Reducing Decoding to LPN** *Asiacrypt '22*  
KEVIN CARRIER, THOMAS DEBRIS-ALAZARD, CHARLES MEYER-HILFIGER AND JEAN-PIERRE TILlich
- 2022 **On Codes and Learning with Errors over Function Fields** *Crypto '22*  
MAXIME BOMBAR, ALAIN COUVREUR AND THOMAS DEBRIS-ALAZARD
- 2022 **An Algorithmic Reduction Theory for Binary Codes: LLL and more** *IEEE Information Theory '22*  
THOMAS DEBRIS-ALAZARD, LÉO DUCAS AND WESSEL P.J. VAN WOERDEN
- 2021 **Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric** *PQCrypto '21*  
ANDRÉ CHAILLOUX, THOMAS DEBRIS-ALAZARD AND SIMONA ETINSKI
- 2020 **Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures** *PKC '20*  
ANDRÉ CHAILLOUX AND THOMAS DEBRIS-ALAZARD
- 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes** *Asiacrypt '19*  
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILlich
- 2019 **Ternary syndrome decoding with large weights** *SAC '19*  
RÉMI BRICOUT, ANDRÉ CHAILLOUX, THOMAS DEBRIS-ALAZARD AND MATTHIEU LEQUESNE
- 2018 **Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme** *Asiacrypt '18*  
THOMAS DEBRIS-ALAZARD AND JEAN-PIERRE TILlich

## Preprints

---

- 2025 **Hardness of Problems with Hints in Code-Based Cryptography and Applications to Traitor Tracing** [iacr.org](https://iacr.org)  
 THOMAS DEBRIS-ALAZARD, VICTOR DYSERYN AND DUONG HIEU PHAN
- 2025 **A Minrank-based encryption scheme à la Alekhnovich-Regev** [iacr.org](https://iacr.org)  
 THOMAS DEBRIS-ALAZARD, PHILIPPE GABORIT, ROMARIC NEVEU AND OLIVIER RUATTA
- 2025 **MIRANDA: short signatures from a leakage-free full-domain-hash scheme** [iacr.org](https://iacr.org)  
 ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD, PHILIPPE GABORIT, AND ADRIEN VINCOTTE
- 2021 **Wavelet: Code-based postquantum signatures with fast verification on microcontrollers** [iacr.org](https://iacr.org)  
 GUSTAVO BANEGRAS, THOMAS DEBRIS-ALAZARD, MILENA NEDELJKOVIC AND BENJAMIN SMITH
- 2020 **On the Hardness of Code Equivalence Problems in Rank Metric** [arxiv.org](https://arxiv.org)  
 ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT
- 2019 **About Wave Implementation and its Leakage Immunity** [iacr.org](https://iacr.org)  
 THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH
- 2017 **The problem with the SURF scheme** [arxiv.org](https://arxiv.org)  
 THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH

## Teaching

---

### PhD. Supervision

- 2023- **Pierre Loisel** [with Alain Couvreur](#)  
 ON CODE ALGORITHMS AND CRYPTANALYSIS
- 2020-2023 **Maxime Bombar** [with Alain Couvreur](#)  
 ON STRUCTURES CODES IN CRYPTOGRAPHY (DEFENDED ON DECEMBER 15, 2023)

### Courses

- 2024- **Advanced topics in quantum information and computing ( CSC\_51002\_EP )**  
 ÉCOLE POLYTECHNIQUE
- 2023- **Introduction to information theory (INF563, CSC\_51063\_EP )**  
 ÉCOLE POLYTECHNIQUE
- 2022- **Introduction to quantum computing and quantum information (INF587, MDC\_51002\_EP )**  
 ÉCOLE POLYTECHNIQUE
- 2021- **Error-correcting codes and applications to cryptography**  
 MPRI, WITH ANNE CANTEAUT AND ALAIN COUVREUR
- 2021-2023 **Post-quantum cryptography, introduction to code-based cryptography**  
 ENS LYON, WITH DAMIEN STEHLÉ AND BENJAMIN WESOLOWSKI

### Tutorials

Sept. 2024 **Summer School IES Corsica, INTRODUCTION TO CODE-BASED CRYPTOGRAHY**

[Cargèse](#)

- June. 2024 **Introduction to Quantum-Safe Cryptography (IBM Zurich) INTRODUCTION TO CODE-BASED CRYPTOGRAHY**

[Zurich](#)

Oct. 2023 **CIMPA school: mathematical aspects of post-quantum cryptography**, INTRODUCTION TO CODE-BASED CRYPTOTGRAPHY

Rabat

Aug. 2022 **Summer school in post-quantum cryptography**, INTRODUCTION TO CODE-BASED CRYPTOTGRAPHY

Budapest

June. 2022 **CIMPA: SuSAAN Summer School of Applied Arithmetic**, INTRODUCTION TO RESEARCH VIA AN OPEN PROBLEM IN COMBINATORICS

Izmir

## Invited Talks

---

2024 **Mathematics for post-quantum cryptanalysis**

Budapest

2024 **Thirteenth in the series workshop Coding and Cryptography (WCC)**

Perugia

## Program Committees

---

2021- **Program committee member**

GILLES THESIS KAHN AWARD '21-23, EUROCRYPT '25, PKC '25, SAC '25, CRYPTO '25, PQCRYPTO '26

2025- **Editorial board member**

DESIGNS, CODES AND CRYPTOGRAPHY (DCC)

## Presentations

---

### Selected Talks at Seminars, Workshops and Conferences

Dec, 2024 **Codes and Lattices in Cryptography: real twins or distant cousins?** CAIPI WORKSHOP

Limoges

Feb, 2024 **Codes and Lattices in Cryptography: real twins or distant cousins?** ATTACC WORKSHOP

Munich

Sept, 2023 **Wave: a Code-based Hash and Sign Signature Scheme**, OXFORD POST-QUANTUM CRYPTOGRAPHY SUMMIT (PQCS)

Oxford

Oct, 2021 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem**, DAGSTUHL SEMINAR, QUANTUM CRYPTANALYSIS

Dagstuhl

Dec, 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes**, ASIACRYPT 19'

Kobe

Sept, 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes**, LONDON-ish LATTICE CODING AND CRYPTO MEETINGS

Imperial College, London

May, 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes**, CRYPTO MEETING

ENS, Lyon

Feb, 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes**, CRYPTOGRAPHY SEMINAR

PQShield, Oxford

Dec, 2018 **Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme**, ASIACRYPT 18'

Brisbane

June, 2017 **Statistical Decoding**, ISIT 17'

Aachen

## Workshops

2020-2024 **Organization of the team Grace Seminar**,

Inria Saclay

PRESENTATIONS: HERE

PRESENTATION: SMOOTHING BOUNDS FOR CODES AND LATTICES

PRESENTATION: WORST-CASE HARDNESS FOR LPN AND CRYPTOGRAPHIC HASHING VIA CODE SMOOTHING

PRESENTATIONS: QUANTUM OBLIVIOUS LWE SAMPLING, ON THE PSEUDORANDOMNESS OF THE DECODING PROBLEM VIA THE ORACLE COMPARISON PROBLEM, STATISTICAL DECODING, SURF : A NEW CODE-BASED SIGNATURE SCHEME, TWO ATTACKS AGAINST SCHEMES BASED ON RANK METRIC, NEW RESULTS ABOUT SIGNATURES BASED ON CODES, WAVE, WORST-CASE HARDNESS FOR LPN AND CRYPTOGRAPHIC HASHING VIA CODE SMOOTHING, AN ALGORITHMIC REDUCTION THEORY FOR BINARY CODES: LLL AND MORE, QUANTUM REDUCTION OF FINDING SHORT CODE VECTORS TO THE DECODING PROBLEM, SMOOTHING BOUNDS: FROM LATTICES TO CODES AND BACK TO LATTICES

## Scientific Popularization

---

2021	<b>Rendez-vous des Jeunes Mathématiciennes et Informaticiennes, Fête de la science à l'école Polytechnique, Olympiades de Mathématiques de l'Académie de Crétteil</b>
2018	<b>International Tournament of Young Mathematicians (Jury Member)</b>
2018	<b>Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)</b>
2018	<b>Rendez-vous des Jeunes Mathématiciennes et Informaticiennes</b>