

# 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

TEACHER ASSISTANT (CHARGÉ D'ENSEIGNEMENT)

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

*Saclay, France*

*Sept. 2022 - Present*

### Inria Saclay

RESEARCHER SCIENTIST (CHARGÉ DE RECHERCHE)

Project-Team: Grace

*Saclay, France*

*Sept. 2020 - Present*

### Royal Holloway, University of London, UK

POSTDOC IN THE INFORMATION SECURITY GROUP

Hosted by Pr Martin R. Albrecht

*London, UK*

*Sept. 2019 - Sept. 2020*

## Education

### Inria Paris

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

Advisor: Pr Jean-Pierre Tillich

*Paris, France*

*Sept. 2016 - Sept. 2019*

### École Normale Supérieure de Cachan (ENS)

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

Advisor: Pr Jean-Pierre Tillich

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

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

AGRÉGATION DE MATHÉMATIQUES OPTION INFORMATIQUE.

*Paris, France*

*Mar. 2016 - Sept. 2016*

*Sept. 2015 - Sept. 2016*

*Sept. 2014 - Sept. 2015*

## Honors and Awards

2026-2031 **ERC Starting Grant**

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

*1.5M€*

2021-2025 **ANR JCJ**

COLA: AN INTERFACE BETWEEN CODE AND LATTICE-BASED CRYPTOGRAPHY

*200 k€*

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

*ERCIM*

2020 **Gilles Kahn Thesis Award**

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

*Société Informatique de France*

2019	<b>Best Paper Award, Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes</b>	<i>Asiacrypt '19</i>
	THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH	

## Scientific Publications

---

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

## Preprints

---

- 2025 **Hardness of Problems with Hints in Code-Based Cryptography and Applications to Traitor Tracing** [iacr.org](#)  
THOMAS DEBRIS-ALAZARD, VICTOR DYSERYN AND DUONG HIEU PHAN
- 2025 **A Minrank-based encryption scheme à la Alekhnovich-Regev** [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](#)  
ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD, PHILIPPE GABORIT, AND ADRIEN VINCOTTE
- 2021 **Wavelet: Code-based postquantum signatures with fast verification on microcontrollers** [iacr.org](#)  
GUSTAVO BANEGAS, THOMAS DEBRIS-ALAZARD, MILENA NEDELJKOVIĆ AND BENJAMIN SMITH
- 2020 **On the Hardness of Code Equivalence Problems in Rank Metric** [arxiv.org](#)  
ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT
- 2019 **About Wave Implementation and its Leakage Immunity** [iacr.org](#)  
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH
- 2017 **The problem with the SURF scheme** [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 CRYPTOGRAPHY [Cargèse](#)
- June. 2024 **Introduction to Quantum-Safe Cryptography (IBM Zurich)** INTRODUCTION TO CODE-BASED CRYPTOGRAPHY [Zurich](#)

Oct. 2023	<b>CIMPA school: mathematical aspects of post-quantum cryptography,</b> INTRODUCTION TO CODE-BASED CRYPTOGRAPHY	<i>Rabat</i>
Aug. 2022	<b>Summer school in post-quantum cryptography,</b> INTRODUCTION TO CODE-BASED CRYPTOGRAPHY	<i>Budapest</i>
June. 2022	<b>CIMPA: SuSAAN Summer School of Applied Arithmetic,</b> INTRODUCTION TO RESEARCH VIA AN OPEN PROBLEM IN COMBINATORICS	<i>Izmir</i>

## Invited Talks

---

2024	<b>Mathematics for post-quantum cryptanalysis</b>	<i>Budapest</i>
2024	<b>Thirteenth in the series workshop Coding and Cryptography (WCC)</b>	<i>Perugia</i>

## Program Committees

---

2021-	<b>Program committee member</b> GILLES THESIS KAHN AWARD '21-23, EUROCRYPT '25, PKC '25, SAC '25, CRYPTO '25, PQCRYPTO '26
2025-	<b>Editorial board member</b> DESIGNS, CODES AND CRYPTOGRAPHY (DCC)

## Presentations

---

### Selected Talks at Seminars, Workshops and Conferences

Dec, 2024	<b>Codes and Lattices in Cryptography: real twins or distant cousins?</b> CAIPI WORKSHOP	<i>Limoges</i>
Feb, 2024	<b>Codes and Lattices in Cryptography: real twins or distant cousins?</b> ATTACC WORKSHOP	<i>Munich</i>
Sept, 2023	<b>Wave: a Code-based Hash and Sign Signature Scheme,</b> OXFORD POST-QUANTUM CRYPTOGRAPHY SUMMIT (PQCS)	<i>Oxford</i>
Oct, 2021	<b>Quantum Reduction of Finding Short Code Vectors to the Decoding Problem,</b> DAGSTUHL SEMINAR, QUANTUM CRYPTANALYSIS	<i>Dagstuhl</i>
Dec, 2019	<b>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,</b> ASIACRYPT 19'	<i>Kobe</i>
Sept, 2019	<b>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,</b> LONDON-ISH LATTICE CODING AND CRYPTO MEETINGS	<i>Imperial College, London</i>
May, 2019	<b>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,</b> CRYPTO MEETING	<i>ENS, Lyon</i>
Feb, 2019	<b>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,</b> CRYPTOGRAPHY SEMINAR	<i>PQShield, Oxford</i>
Dec, 2018	<b>Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme,</b> ASIACRYPT 18'	<i>Brisbane</i>
June, 2017	<b>Statistical Decoding,</b> ISIT 17'	<i>Aachen</i>

## Workshops

2020-2024	<b>Organization of the team Grace Seminar,</b> PRESENTATIONS: HERE	<i>Inria Saclay</i>
-----------	---	---------------------

2020-2022 **Workshop on Transference**, ORGANIZED BY LÉO DUCAS  
PRESENTATION: SMOOTHING BOUNDS FOR CODES AND LATTICES

*CWI*

2019-2020 **Workshop “yet another crypto reading group”**, ORGANIZED BY MARTIN R. ALBRECHT

*Royal Holloway  
University of London*

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

2016 - **Workshop “code-based cryptography”**, ORGANIZED BY JEAN-PIERRE TILlich

*Inria Paris*

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 Créteil</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>