

Thomas Debris-Alazard

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

58 rue du ruisseau, Paris 75018

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

Research Interests

Research Area: *Public-Key Cryptography (theory, designs, cryptanalysis, standardization) with a focus on code and lattice-based cryptography*

- **Cryptographic Designs,**
- **Cryptanalysis,**
- **Security estimates,** study of the generic decoding problem
- **Security proof,** in the classical or quantum model
- **Algorithms, Reduction** classical and quantum

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

Paris, France

Mar. 2016 - Sept. 2016

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

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

Sept. 2015 - Sept. 2016

AGRÉGATION DE MATHÉMATIQUES OPTION INFORMATIQUE.

Sept. 2014 - Sept. 2015

Honors and Awards

2021-2024 **ANR JCJ**

COLA: AN INTERFACE BETWEEN CODE AND LATTICE-BASED CRYPTOGRAPHY

200 000 €

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

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

Asiacrypt '19

Scientific Publications

- 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
- 2017 **Statistical Decoding** *ISIT '17*
THOMAS DEBRIS-ALAZARD AND JEAN-PIERRE TILLICH

Preprints

- 2024 **New Solutions to Delsarte's Dual Linear Programs** *arxiv.org*
ANDRÉ CHAILLOUX AND THOMAS DEBRIS-ALAZARD
- 2022 **Worst and Average Case Hardness of Decoding via Smoothing Bounds** *iacr.org*
THOMAS DEBRIS-ALAZARD AND NICOLAS RESCH

2021	Wavelet: Code-based postquantum signatures with fast verification on microcontrollers GUSTAVO BANEGAS, THOMAS DEBRIS-ALAZARD, MILENA NEDELJKOVIĆ AND BENJAMIN SMITH	iacr.org
2020	On the Hardness of Code Equivalence Problems in Rank Metric ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT	arxiv.org
2019	About Wave Implementation and its Leakage Immunity THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH	iacr.org
2017	The problem with the SURF scheme THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH	arxiv.org

Teaching

PhD. Supervision

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

Courses

2023-	Introduction to information theory (INF563) ÉCOLE POLYTECHNIQUE
2022-	Introduction to quantum computing and quantum information (INF587) 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 WESOŁOWSKI

Tutorials

Sept. 2024	Summer School IES Corsica, INTRODUCTION TO CODE-BASED CRYPTOTGRAPHY	Cargèse
June. 2024	Introduction to Quantum-Safe Cryptography (IBM Zurich) INTRODUCTION TO CODE-BASED CRYPTOTGRAPHY	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

- 2024 **Program committee**
EUROCRYPT '25, PKC '25
- 2024 **Guest Editor**
SPECIAL ISSUE ON CODE-BASED CRYPTOGRAPHY IN *Designs, Codes and Cryptography*
- 2021-2023 **Gilles Kahn Award**
SOCIÉTÉ INFORMATIQUE DE FRANCE
- 2022 **Journées Codage & Cryptographie (JC2)**

Presentations

Selected Talks at Seminars, Workshops and Conferences

- 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

- Sept. 2020 **Organization of the team Grace Seminar,** *Inria Saclay*
PRESENTATIONS: [HERE](#)
- Sept. 2020 **Workshop on Transference,** ORGANIZED BY LÉO DUCAS *CWI*
PRESENTATION: [SMOOTHING BOUNDS FOR CODES AND LATTICES](#)
- Sept. 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](#)

PRESENTATIONS: 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	Rendez-vous des Jeunes Mathématiciennes et Informaticiennes, Fête de la science à l'école Polytechnique, Olympiades de Mathématiques de l'Académie de Créteil
2018	International Tournament of Young Mathematicians (Jury Member)
2018	Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)
2018	Rendez-vous des Jeunes Mathématiciennes et Informaticiennes

Skills

Programming	C, Java, Python, jkiloMagma, SageMath
Languages	French (native), English (fluent)

Reviews

2023	DCC, IEEE IT
2022	Asiacrypt, DCC, AMC, PQCrypto, JoC, ANR
2021	Eurocrypt, Crypto, CTRSA, DCC, ISIT, PQCrypto, ANR, IMACC, AMC, Latincrypt
2020	AMC, ITW, IEEE
2019	Eurocrypt, ISIT, DCC, PKC
2018	PQCrypto, WCC
2017	C2SI