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 *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

2021-2024 **ANR JCJ** *200 000 €*
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

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

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** *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 Tillich	
2017	**The problem with the SURF scheme**	*arxiv.org*
	Thomas Debris-Alazard, Nicolas Sendrier and Jean-Pierre Tillich	

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

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 Wesolowski

Tutorials

Sept. 2024	**Summer School IES Corsica,** INTRODUCTION TO CODE-BASED CRYPOTGRAPHY	*Cargèse*
Oct. 2023	**CIMPA school: mathematical aspects of post-quantum cryptography,** INTRODUCTION TO CODE-BASED CRYPOTGRAPHY	*Rabat*
Aug. 2022	**Summer school in post-quantum cryptography,** INTRODUCTION TO CODE-BASED CRYPOTGRAPHY	*Budapest*
June. 2022	**CIMPA: SuSAAN Summer School of Applied Arithmetic,** INTRODUCTION TO RESEARCH VIA AN OPEN PROBLEM IN COMBINATORICS	*Izmir*

Invited Talks

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

Program Committees

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 and Conferences

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	
Mar. 2016 -	**Workshop ''code-based cryptography''**, organized by Jean-Pierre Tillich	*Inria Paris*
	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, jjkiloMagma, 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**