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

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 **Statistical Decoding 2.0: Reducing Decoding to LPN** *iacr.org*

Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger and Jean-Pierre Tillich

2022 **Smoothing codes and lattices: systematic study and new bounds** *iacr.org*

Thomas Debris-Alazard, Léo Ducas, Nicolas Resch and Jean-Pierre Tillich

2021 **Wavelet: Code-based postquantum signatures with fast verification on microcontrollers** *iacr.org*

Gustavo Banegas, Thomas Debris-Alazard, Milena Nedeljković and Benjamin Smith

2021 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem** *arxiv.org*

Thomas Debris-Alazard, Maxime Remaux and Jean-Pierre Tillich

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

MPRI (2021-2022)

- **Error-correcting codes and applications to cryptography (with Anne Canteaut and Alain Couvreur),** introduction to code-based cryptography

ENS Lyon (2021-2022)

- **Post-quantum cryptography (with Damien Stehlé and Benjamin Wesolowski),** introduction to code-based cryptography

Polytechnique (2020-2022)

- **Introduction à l'informatique (INF361),** under the supervision of François Morain
- **Introduction to cryptology (INF558),** under the supervision of François Morain

ENSTA (2020-2021)

- **Mathématiques discrètes pour la protection de l'information,** under the supervision of Françoise Levy-Dit-Vehel

University Paris-Sorbonne (2016-2019)

- **Advanced Cryptography,** Master 1 under the supervision of Damien Vergnaud
- **Introduction of Cryptography,** 3rd year Bachelor under the supervision of Valérie Ménissier-Morain
- **Environment and Development in Linux,** 2nd year Bachelor under the supervision of Valérie Ménissier-Morain
- **Programming in C,** 1st year Bachelor

Program Committees

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**, PRESENTATIONS: HERE	*Inria Saclay*
Sept. 2020-	**Workshop on Transference**, ORGANIZED BY LÉO DUCAS PRESENTATION: SMOOTHING BOUNDS FOR CODES AND LATTICES	*CWI*

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: 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

2022	**DCC, AMC**
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**