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 Interest

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

- **Cryptographic Designs,** Wave, Surf
- **Cryptanalysis,** a signature and an IBE in rank metric
- **Security estimates,** study of the generic decoding problem
- **Security proof,** in the classical or quantum model
- **Algorithmic, Reduction** classical and quantum

Employment

Inria Saclay *Saclay, France*

Researcher Scientist (chargé de recherche) *Sept. 2020 - Present*

Project-Team: Grace

Education

Royal Holloway, University of London, UK *London, UK*

Postdoc in the Information Security Group Department *Sept. 2019 - Sept. 2020*

Advisor: Pr Martin R. Albrecht

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*

Awards

2021-2024 **ANR JCJ** *200 000 €*

COLA: An interface between COde and LAttice-based cryptography

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

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

Eprints

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

Gustavo Banegas and Thomas Debris-Alazard and 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

2020 **An Algorithmic Reduction Theory for Binary Codes: LLL and more** *iacr.org*

Thomas Debris-Alazard, Léo Ducas and Wessel P.J. van Woerden

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

Polytechnique (2020-2021)

- **Introduction à l'informatique,** under the supervision of Philippe Chassignet and François Morain
- **Introduction to Cryptology,** 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
- **Environment and Development in Linux,** 2nd year Bachelor
- **Programming in C,** 1st year Bachelor

Presentations

Seminars and Conferences

Sept, 2021	**Quantum Reduction of Finding Short Code Vectors to the Decoding Problem,** ENS Lyon, RHUL and CWI	*Online*
June, 2020	**Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures,** PKC	*Online*
Dec, 2019	**Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** Asiacrypt 19'	*Kobe*
Oct, 2019	**Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** Cryptography Seminar LIP6	*Université Jussieu, Paris*
Oct, 2019	**Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** Cryptography Seminar, Research Team GRACE	*Inria, Paris-Saclay*
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*
June, 2019	**Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** CBC 19'	*Darmstadt*
June, 2019	**Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** CCA seminar	*Université Jussieu, Paris*
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*
Jan, 2019	**Wave: A New Code-Based Signature Scheme,** Cryptography Seminar	*Research Institute, Rennes*
Dec, 2018	**Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme,** Asiacrypt 18'	*Brisbane*
Nov, 2018	**WAVE: A New Code-Based Signature Scheme,** AcroCrypt	*Research Institute, Caen*
Oct, 2018	**Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme,** Journées C2	*Aussois*
June, 2017	**Statistical Decoding,** ISIT 17'	*Aachen*
June, 2017	**Statistical Decoding *and* Surf : a new code-based signature scheme,** CBC 2017	*Tenerife*
Apr, 2017	**Statistical Decoding,** Journées C2	*La Bresse*

Workshops

Mar. 2016 -	**Workshop "code-based cryptography",** organized by Jean-Pierre Tillich 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	*Inria Paris*
Sept. 2020-	**Workshop on Transference,** organized by Léo Ducas Presentation: Smoothing bounds for codes and lattices	*CWI*

Sept. 2019-**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

Scientific Mediation

2021	**Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)**
2018	**International Tournament of Young Mathematicians (Jury Member)**
2018	**Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)**
2018	**Les Rendez-vous des Jeunes Mathématiciennes et Informaticiennes**

Skills

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

Reviews

2021	**Eurocrypt, Crypto, CTRSA, DCC, ISIT, PQCrypto, ANR**
2020	**Advances in Mathematics of Communications, ITW, IEEE**
2019	**Eurocrypt, ISIT, DCC, PKC**
2018	**PQCrypto, WCC**
2017	**C2SI**