Thomas **Debris-Alazard**

Born in Paris, France, May 1, 1991 · Researcher Scientist at Inria

12 rue de la Véga, Paris 75012

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

Research Interest

Research Area: Code-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,** 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*

Award

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

2020 **Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures** *PKC '20*

Thomas Debris-Alazard and André Chailloux

2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes *(58 pages)*** *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

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 **Surf: a new code-based signature scheme (*56pages*)** *arXiv*

Thomas Debris-Alazard, Nicolas Sendrier and Jean-Pierre Tillich

Teaching

Courses in University Paris-Sorbonne (192 hours)

- **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

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 *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

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

Jan. 2019 - **GT BAC,** organized by Édouard Rousseau *Telecom ParisTech*

Presentation: Wave

Scientific Mediation

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, LaTeX
Languages	French (native), English (fluent)

Reviews

2020 **Advances in Mathematics of Communications**

2019 **Eurocrypt, ISIT, Design Codes and Cryptography, PKC**

2018 **PQCrypto, WCC**

2017 **C2SI**