

Curriculum vitæ
Hugues RANDRIAMBOLOLONA

Maître de conférences à Télécom ParisTech.

Domaine de recherche : Géométrie algébrique, théorie des nombres, et leurs applications en codage correcteur et cryptographie.

Formation et titres :

- Ancien élève de l'École normale supérieure.
- Diplômé de Télécom Paris (2000). Ingénieur du Corps des Mines.
- Docteur en mathématiques (2002) de l'Université Paris-Sud 11 Orsay.

Thèse : *Hauteurs pour les sous-schémas et exemples d'utilisation de méthodes arakeloviennes en théorie de l'approximation diophantienne*, encadrée par Jean-Benoît BOST.

Parcours professionnel :

- 2000-2002. Chargé d'enseignement-recherche à Télécom Paris.
- 2002-2003. Chercheur invité à l'École polytechnique fédérale de Zurich.
- 2003-présent. Maître de conférences à Télécom ParisTech.

Thèses encadrées :

- Thomas FUHR (2007-2011). *Conception, preuves et analyse de fonctions de hachage cryptographique*. Co-encadrée avec Henri GILBERT.
- Jean-Pierre FLORI (2008-2012). *Boolean functions, algebraic curves and complex multiplication*. Co-encadrée avec Gérard COHEN.
- Eduardo FERRAZ (2008-2012). *Algebraic topology of random simplicial complexes and applications to sensor networks*. Co-encadrée avec Laurent DECREUSEFOND.
- Matthieu RAMBAUD (2014-2017). *Courbes de Shimura et algorithmes bilinéaires de multiplication dans les extensions de corps finis*.
- Édouard ROUSSEAU (2017-). *Arithmétique efficace pour la cryptographie et la cryptanalyse*. Co-encadrée avec Luca DE FEO et Éric SCHOST.

Autres activités :

- Enseignement (responsable de la filière *Algèbre appliquée — Codage, cryptographie, et information quantique* à Télécom ParisTech).
- Animation scientifique (responsable équipe MC2), organisation de séminaires (ex : séminaire Dépt. INFRES, séminaire C2...).
- Organisation de rencontres et conférences (ex : *CohenFest* Paris 2016), d'écoles pour jeunes chercheurs (ex : *École Géométrie diophantienne* Rennes 2009, *École C2* La Chapelle-Gauthier 2016).
- Exposés de séminaires, interventions dans des colloques et conférences...
- Participation à des jurys de thèse, des comités de sélection, etc.
- Arbitrage pour diverses revues et conférences (souvent à l'interface mathématiques-informatique, ex : IEEE Trans. Inform. Th.).
- Activités contractuelles (ex : ACI Cogito 2004–2007, ANR Diophante 2007–2010, ANR Gardio 2015–2019, ANR Manta 2016–2019).
- Activités administratives (ex : membre élu du Conseil de laboratoire LTCI, du Comité de la recherche, du Comité d'évaluation des appellations de Télécom ParisTech).

Trivia :

- Médaille d'or aux Olympiades internationales de mathématiques (1993).
- Agrégation de mathématiques (1996) ; rang : 1^{er}.
- Danseur de Tango argentin (2001-).