Curriculum vitæ

Hugues Randriambololona

Né le 23/09/1975 à Aubervilliers (93). Nationalité française.

Formation et titres :

- Ancien élève de l'École normale supérieure (1994-1998).
- Diplômé de Télécom Paris (2000). Ingénieur du Corps des Mines.
- Docteur en mathématiques (2002) de l'Université Paris-Sud 11 Orsay.

Parcours professionnel :

2000-2002. Chargé d'enseignement-recherche à Télécom Paris.
2002-2003. Chercheur invité à l'École polytechnique fédérale de Zurich.
2003-2019. Maître de conférences à Télécom ParisTech.
2019-présent. Expert à l'Agence nationale de sécurité des systèmes d'information.

Domaines de recherche :

- Cryptographie (notamment asymétrique et post-quantique).
- Codage correcteur, complexité algébrique, corps finis.
- Géométrie algébrique, théorie des nombres, théorie d'Arakelov.

Autres activités :

- Analyse de mécanismes cryptographiques (gouvernementaux ou commerciaux).
- 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).
- Major du concours d'entrée à l'École polytechnique (1994).
- Reçu premier à l'agrégation de mathématiques (1996).

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.

Sélection de publications :

[1] R. Blache, A. Couvreur, E. Hallouin, D. Madore, J. Nardi, M. Rambaud, H. Randriam. Anticanonical codes from del Pezzo surfaces with Picard rank one. Trans. AMS. (sous presse)

[2] L. De Feo, H. Randriam, É. Rousseau. Standard lattices of compatibly embedded finite fields. 2019 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC 2019), Pékin, 15-18 juillet 2019, pp. 122–130.

[3] H. Randriambololona. Harder-Narasimhan theory for linear codes (with an appendix on Riemann-Roch theory). J. Pure Appl. Algebra. 223 (2019) 2997–3030.

[4] L. Decreusefond, E. Ferraz, H. Randriam, A. Vergne. Simplicial homology of random configurations. Adv. in Appl. Probab. 46 (2014) 325–347.

[5] H. Randriambololona. An upper bound of Singleton type for componentwise products of linear codes. IEEE Trans. Inform. Theory 59 (2013) 7936–7939.

[6] H. Randriambololona. Asymptotically good binary linear codes with asymptotically good self-intersection spans. IEEE Trans. Inform. Theory 59 (2013) 3038–3045.

[7] H. Randriambololona. $(2,1)$-separating systems beyond the probabilistic bound. Israel J. Math. 195 (2013) 171–186.

[8] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. J. Complexity 28 (2012) 489–517.

[9] J.-P. Flori, G. Cohen, H. Randriam, S. Mesnager. On a conjecture about binary strings distribution. 6th Conference on Sequences and Their Applications (SETA 2010), Paris, 12-17 septembre 2010. Springer Lecture Notes in Computer Science 6338, pp. 346–358.

[10] E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, M. Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. 30th Annual International Cryptology Conference (CRYPTO 2010), Santa Barbara, 15-19 août 2010. Advances in Cryptology, Springer Lecture Notes in Computer Science 6223, pp. 237–254.

[11] F. Castro, I. Rubio, H. Randriam, H. Mattson. Divisibility of exponential sums via elementary methods. J. Number Theory 130 (2010) 1520–1536.

[12] H. Randriambololona. Métriques de sous-quotient et théorème de Hilbert-Samuel arithmétique pour les faisceaux cohérents. J. reine angew. Math. (Crelle) 590 (2006) 67–88.