

Damien ROBERT

Chargé de Recherche en cryptographie

Libourne, France

+33 (0)6 66 56 25 49

+33 (0)5 40 00 21 56

✉ damien.robert@inria.fr

📄 www.normalesup.org/~robert/

👤 DamienRobert

Né en 1984, Français



Recherche

Liste des publications : www.normalesup.org/~robert/pro/publications/ , voir aussi *l'appendice*.

Expérience professionnelle

- Mars 2012–Actuel Chargé de Recherche, *Inria Bordeaux Sud-Ouest, Bordeaux*, Équipe projet LFANT.
Courbes elliptiques, variétés abéliennes et théorie algorithmique des nombres appliquées à la cryptographie
- Août 2011– Ingénieur Chercheur, *Microsoft Research, Redmond*, Chef d'équipe : Kristin Lauter.
- Février 2012 Développement de la librairie cryptographique de Microsoft
- Octobre 2010– Postdoctorant, *Inria Bordeaux Sud-Ouest, Bordeaux*, Chef d'équipe : Andreas Enge.
Août 2011 Genus 2 curves and complex multiplication. Responsable de l'organisation des séminaires de l'équipe LFANT à l'Institut Mathématiques de Bordeaux.
- Juillet 2010– Stage à Microsoft Research, *Redmond, États-Unis*, Mentor : Kristin Lauter.
- Septembre 2010 Génération de polynômes de classe en genre 2 par la méthode des restes Chinois

Parcours

- Janvier 2007– Thèse, *Université Henri Poincaré et Loria, Nancy*, Directeur : Guillaume Hanrot, Monitorat en
Juin 2010 informatique.
Fonctions thêta et applications à la cryptographie. Soutenue le 21 Juillet 2010.
- Septembre– MPRI, *Paris*, Master Parisien de Recherche Informatique, (Inscription pédagogique).
- Décembre 2006 Remise à niveau en informatique (cryptographie), suivi du cours de M2 de théorie des nombres à Orsay.
- 2004–2006 Master 2 de Mathématiques Pures, *Paris VI, Paris VII, Paris XI, Polytechnique*, Algèbre et Géométrie, Mention Très Bien (Cours : 19.88/20, Mémoire de M2 : 18/20, Total : 18.94/20).
(Inscription pédagogique en 2004–2005.) Mémoire de M2 sur la « classification des groupes de réflexions complexes », superviseur : Michel Broué (Institut Henri Poincaré).
- 2004–2005 Agrégation de Mathématiques, option Calcul Scientifique, Rang 9.
- 2003–2007 École Normale Supérieure, *Paris*, Concours Informatique, Rang 1.
- 2003–2006 Magistère de Mathématiques (MMFAI), Mention Très Bien.
- 2003–2004 L3 et M1 de Mathématiques, Mentions Très Bien .
Validation de cours d'Informatiques de L3 et M1 en sus. Mémoire de M1 sur « Modules de Clifford et K -théorie », réalisé avec Mehdi Tibouchi, superviseur : François Pierrot.
- 2001–2003 Classes préparatoires MPSI et MP*, *Lycée du Parc, Lyon*.
- 2000–2001 Bac Scientifique spécialité Mathématiques, *Lycée René Descartes, Saint-Genis-Laval (69)*, mention Très Bien.

Expériences

2003 – 2006 **Tuteur Informatique.** Familiariser les élèves avec le système informatique (Freebsd, Solaris, Linux). Organisation et encadrement de stages de travaux pratiques (\LaTeX , unix,...), École Normale Supérieure, Paris.

2003 – 2006 **Administrateur Élève.** Aider les administrateurs système à gérer le parc informatique, configuration des sessions utilisateurs, installation logicielle, École Normale Supérieure, Paris.

Langages

Français	Natif	
Anglais	Courant	<i>Séjour d'un an à Knoxville, dans le Tennessee</i>
Allemand	Élémentaire	<i>9 ans de cours</i>

Compétences informatiques

Programmation	C, JAVA, Ocaml, Perl, PHP, Ruby, Shell	OS	Linux (Archlinux)
Scientifique	Magma, Matlab, Pari, Sage	VCS	Git, Mercurial, Subversion
Web	(X)HTML, CSS, Javascript	Typographie	Lua \LaTeX

Intérêts

Sport	Cirque, Escalade, Raquettes.
Sécurité	Formation premiers secours.
Divers	Permis de conduire.

Activités scientifiques

Publications

- D. LUBICZ et D. ROBERT. « Arithmetic on Abelian and Kummer Varieties ». In : *Finite Fields and Their Applications* 39 (mai 2016), p. 130-158. DOI : [10.1016/j.ffa.2016.01.009](https://doi.org/10.1016/j.ffa.2016.01.009). URL : <http://www.normalesup.org/~robert/pro/publications/articles/arithmetique.pdf>. HAL : [hal-01057467](https://hal.archives-ouvertes.fr/hal-01057467), eprint : [2014/493](https://hal.archives-ouvertes.fr/hal-01057467).
- D. LUBICZ et D. ROBERT. « Computing separable isogenies in quasi-optimal time ». In : *LMS Journal of Computation and Mathematics* 18 (1 fév. 2015), p. 198-216. DOI : [10.1112/S146115701400045X](https://doi.org/10.1112/S146115701400045X). arXiv : [1402.3628](https://arxiv.org/abs/1402.3628). URL : <http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf>. HAL : [hal-00954895](https://hal.archives-ouvertes.fr/hal-00954895).
- D. LUBICZ et D. ROBERT. « A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties ». In : *Journal of Symbolic Computation* 67 (mar. 2015), p. 68-92. DOI : [10.1016/j.jsc.2014.08.001](https://doi.org/10.1016/j.jsc.2014.08.001). URL : <http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf>. HAL : [hal-00806923](https://hal.archives-ouvertes.fr/hal-00806923), eprint : [2013/192](https://hal.archives-ouvertes.fr/hal-00806923).
- R. COSSET et D. ROBERT. « An algorithm for computing (ℓ, ℓ) -isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2 ». In : *Mathematics of Computation* 84.294 (nov. 2015), p. 1953-1975. DOI : [10.1090/S0025-5718-2014-02899-8](https://doi.org/10.1090/S0025-5718-2014-02899-8). URL : <http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf>. HAL : [hal-00578991](https://hal.archives-ouvertes.fr/hal-00578991), eprint : [2011/143](https://hal.archives-ouvertes.fr/hal-00578991).
- K. E. LAUTER et D. ROBERT. « Improved CRT Algorithm for Class Polynomials in Genus 2 ». In : *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*. Sous la dir. d'E. W. HOWE et K. S. KEDLAYA. T. 1. The Open Book Series. Berkeley : Mathematical Sciences Publisher, nov. 2013, p. 437-461. DOI : [10.2140/obs.2013.1.437](https://doi.org/10.2140/obs.2013.1.437). URL : <http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf>. Transparents : [2012-07-ANTS-SanDiego.pdf](https://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf) (30min, International Algorithmic Number Theory Symposium (ANTS-X), Juillet 2012, San Diego, USA), HAL : [hal-00734450](https://hal.archives-ouvertes.fr/hal-00734450), eprint : [2012/443](https://hal.archives-ouvertes.fr/hal-00734450).
- D. LUBICZ et D. ROBERT. « Computing isogenies between abelian varieties ». In : *Compositio Mathematica* 148.5 (sept. 2012), p. 1483-1515. DOI : [10.1112/S0010437X12000243](https://doi.org/10.1112/S0010437X12000243). arXiv : [1001.2016](https://arxiv.org/abs/1001.2016) [math.AG]. URL : <http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf>. HAL : [hal-00446062](https://hal.archives-ouvertes.fr/hal-00446062).
- J.-C. FAUGÈRE, D. LUBICZ et D. ROBERT. « Computing modular correspondences for abelian varieties ». In : *Journal of Algebra* 343.1 (oct. 2011), p. 248-277. DOI : [10.1016/j.jalgebra.2011.06.031](https://doi.org/10.1016/j.jalgebra.2011.06.031). arXiv : [0910.4668](https://arxiv.org/abs/0910.4668) [cs.SC]. URL : <http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf>. HAL : [hal-00426338](https://hal.archives-ouvertes.fr/hal-00426338).
- D. LUBICZ et D. ROBERT. « Efficient pairing computation with theta functions ». In : sous la dir. de G. HANROT, F. MORAIN et E. THOMÉ. T. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer-Verlag, juil. 2010. DOI : [10.1007/978-3-642-14518-6_21](https://doi.org/10.1007/978-3-642-14518-6_21). URL : <http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf>. Transparents : [2010-07-ANTS-Nancy.pdf](https://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf) (30min, International Algorithmic Number Theory Symposium (ANTS-IX), Juillet 2010, Nancy), HAL : [hal-00528944](https://hal.archives-ouvertes.fr/hal-00528944).

Prépublications

- E. MILIO et D. ROBERT. « Modular polynomials on Hilbert surfaces ». Sept. 2017. HAL : [hal-01520262](https://hal.archives-ouvertes.fr/hal-01520262).

- A. DUDEANU, JETCHEV, D. ROBERT et al. « Cyclic Isogenies for Abelian Varieties with Real Multiplication ». Oct. 2017. HAL : [hal-01629829](#).

Rapports

- Andreas Enge, Damien Robert, Computing class polynomials in genus 2. DGA Report, Avril 2013.

Thèse

- Fonctions thêta et applications à la cryptographie (en Français). PhD thesis in Computer Sciences, Juillet 2010, Université Henri-Poincaré, Nancy. (Transparents : [2010-07-Phd-Nancy.pdf](#) (1h, Nancy), TEL : [tel-00528942](#).)

Prix

- Février 2012 Second prix en Sciences pour le [prix de thèse de la région Lorraine](#), Metz. ([Annonce Inria](#))
- Octobre 2011 [Prix de thèse de l'université de Lorraine](#) dans le domaine IAEM (Informatique, Automatique, Électronique, Mathématiques), Nancy. ([Photos de la cérémonie](#))

Logiciels

- [AVIsogenies](#) (Abelian Varieties and Isogenies), avec [Gaëtan Bisson](#), [Romain Cosset](#). Packet magma dédié au calcul explicite d'isogénies entre variétés abéliennes, 2010. Licence libre (LGPLv2+), enregistré à l'APP (référence IDDN.FR.001.440011.000.R.P.2010.000.10000). Version actuelle 0.6, publiée le 2012-11-28.

Enseignement

- Décembre 2015 Introduction à la cryptologie. Séminaire de sécurité des systèmes d'information du Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun. [À quoi sert la cryptologie ? Petit panorama des mathématiques de la cryptologie](#), [Introduction to cryptology : confidentiality, integrity, authenticity](#), [Modern cryptology : from public key cryptography to homomorphic encryption](#)
- Septembre 2015 [The group structure of rational points of elliptic curves over a finite field](#) (3h). [Elliptic Curves Cryptography \(ECC 2015\) Summer School](#), Bordeaux. ([Exercices](#).)
- Mars 2015 [Théorie Algorithmique des Nombres et Cryptologie](#). Cours d'une semaine dans le cadre de l'École Mathématique Africaine, organisée en soutien avec le Centre International de Mathématiques Pures et Appliquées (CIMPA), Franceville, Gabon. [Introduction aux cours](#), [Transparents](#), [Exemples](#) (X509, ssh, gpg)
- Septembre 2011 [Isogenies and endomorphism rings of elliptic curves](#) (2h30). [ECC 2011 Summer School](#), Nancy.
- 2007 – 2010 Monitorat en Informatique. Université Henri-Poincaré (Nancy).
 - TDs d'introduction à la cryptographie (M1, 30h).
 - Cours de découverte de l'informatique : HTML, CSS, PHP and MySQL (L1, 60h).
 - TDs et TP d'introduction à la programmation : OCaml (L1, 120h).
- Mars 2004 – Mai 2004 [Corps quadratiques et groupes de classes](#). Groupe de travail organisé en commun avec Mehdi Tibouchi, École Normale Supérieure, Paris.

Étudiants

- Novembre 2012 – Décembre 2015 [Enea Milio](#), Isogénies entre surfaces abéliennes, cosupervising with [Andreas Enge](#). Thèse, Inria Bordeaux Sud-Ouest.

- 2014 Illaria Chillotti, Pairings over elliptic curves using isogenies. Master, Institut de Mathématiques de Bordeaux.
- 2013 Giulio Di Piazza, [Arithmetic on Jacobians of algebraic curves](#). Master, Institut de Mathématiques de Bordeaux.
- 2012 Ilaria Lovato, [Computing Modular Polynomials with Theta Functions](#), cosupervising with [Andreas Enge](#). Master, Institut de Mathématiques de Bordeaux.

Responsabilités

- Décembre 2015 – Présent Commission Consultative 25, Institut Mathématiques de Bordeaux.
- Janvier 2015 – Présent Commission Jeunes Chercheurs, Inria Bordeaux.
- 2014 – Présent Jury du concours de l'agrégation de Mathématiques.
- Juin 2013 – Présent Codirecteur de l'équipe-projet MACISA, au sein du Laboratoire international de recherche en informatique et mathématiques appliquées (LIRIMA) (Depuis Septembre 2014 ; auparavant responsable scientifique du thème « Elliptic and hyperelliptic curves cryptography »).
- Octobre 2010 – Présent Organisation des [séminaires de l'équipe LFANT](#).
- 2012 – 2016 Membre de l' ERC [Antics](#) (Algorithmic Number Theory in Computer Science).
- 2013 – 2016 Membre de l' ANR Industrielle [Simpatic](#) (SIM and PAiring Theory for Information and Communications security).
- 2012 – 2015 Membre de l' ANR [Peace](#) (Parameter spaces for Efficient Arithmetic and Curve security Evaluation).
- 2012 – Présent [Membre du LabEx CPU](#) (Numerical certification and reliability).
- 2009 – 2012 Membre de l' ANR [Chic](#) (Courbes Hyperelliptiques Isogénies et Comptage).

Comités

- Décembre 2015 [CRI 2015](#), Yaoundé, Cameroun. Comité scientifique.
- Décembre 2015 [Asiacrypt 2015](#), Auckland. Comité scientifique.
- Septembre 2015 [Elliptic Curves Cryptography \(ECC 2015\)](#), Bordeaux. Comité d'organisation, Comité scientifique.
- Août 2013 [Selected Area in Cryptography \(SAC 2013\)](#), Simon Fraser University, Canada. Comité scientifique.

Conférencier invité

- [Isogenies, Polarizations and Real Multiplication](#) (1h). Journées C2 Codage et Cryptographie, Octobre 2015, La Londe-Les-Maures.
- [Isogenies, Polarizations and Real Multiplication](#) (1h). [Modular Forms and Curves of Low Genus : Computational Aspects](#), Septembre 2015, ICERM, Providence, USA. (Long version.)
- [Optimal pairings on abelian varieties](#) (1h). [Elliptic Curves Cryptography \(ECC 2014\)](#), Octobre 2014, Chennai, India.
- [Isogenies between abelian varieties \(Notes\)](#) (1h). ANR [Peace](#) conference [Effective moduli spaces and applications to cryptography](#), Juin 2014, Rennes.
- [Pairings on abelian varieties and the Discrete Logarithm Problem](#) (1h). Discrete Logarithm Problem Conference [DLP 2014](#), Mai 2014, Ascona, Suisse.

- Computing optimal pairings on abelian varieties with theta functions (1h). *Geometry and Cryptography (Geocrypt 2011)*, Juin 2011, Bastia.
- Generalizing Vélu's formulas and some applications (1h). *Elliptic Curves Cryptography (ECC 2010)*, 25 year anniversary of elliptic curves computation, Octobre 2010, Redmond, USA. (Video link.)
- A Vélu's like formula for computing isogenies on Abelian Varieties (1h). *Conférence Algorithmique et Arithmétique avec applications à la cryptographie*, Mai 2010, Moscou, Russie.

Exposés

- Arithmetic on Abelian and Kummer varieties (2x1h). *INRIA Team LFANT seminar*, Mai 2015, Bordeaux. On blackboard, notes.
- Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties (45min). *École Mathématique Africaine*, Mars 2015, Université de Masuku, Franceville, Gabon.
- Arithmetic on Abelian and Kummer varieties (1h). *Number Theory Seminar*, Décembre 2014, Caen. On blackboard, notes.
- Isogeny graphs in dimension 2 (1h). *Cryptography Seminar*, Décembre 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (1h). *Number Theory Seminar*, Avril 2014, Institut Fourier, Grenoble. On blackboard, notes.
- Arithmetic on abelian varieties and related topics (1h). *Séminaire Code et Cryptographie de l'Université de Zurich et l'Université de Neuchâtel*, Mars 2014, Neuchâtel, Suisse.
- Computing optimal pairings on abelian varieties with theta functions (1h). *ANR Industrielle Simpatc meeting*, Janvier 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (30min). *ANR Peace meeting*, Décembre 2013, Rennes.
- On isogenies and polarisations (1h). *LFANT Seminar*, Novembre 2013, Bordeaux.
- On isogenies and polarisations (30min). *Geometry and Cryptography (Geocrypt 2013)*, Octobre 2013, Tahiti.
- On isogenies between abelian varieties (45min). *Microsoft Research*, Août 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (1h). *Microsoft Research*, Août 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (30min). *Arithmétique géométrie cryptographie et théorie des codes (AGCT 14)*, Juin 2013, Luminy, Marseille.
- Computing optimal pairings on abelian varieties with theta functions (1h). *Lacal*, Mai 2013, Lausanne.
- Computing optimal pairings on abelian varieties with theta functions (1h). *CCIS seminar*, Avril 2013, Grenoble.
- Computing cyclic isogenies using real multiplication (Notes) (1h). *ANR Peace meeting*, Avril 2013, Paris.
- Computing rational isogenies from the equations of the kernel (30min). *ANR Peace meeting*, Novembre 2012, Paris.
- Improved CRT Algorithm for class polynomials in genus 2 (1h). *Microsoft Research*, Août 2012, Redmond, USA.
- About the CRT method to compute class polynomials in dimension 2 (1h). *INRIA Team LFANT seminar*, Mai 2012, Bordeaux.
- Algorithms on abelian varieties for cryptography (1h). *Caen's Cryptographic Seminar*, Mars 2012, Caen.

- Algorithms on abelian varieties for cryptography (2h). INRIA Team Grace Seminar, Janvier 2012, LIX, École Polytechnique, Paris.
- Algorithms on abelian varieties for cryptography (1h). Butte aux cailles Seminar, Janvier 2012, Télécom ParisTech, Paris.
- Public key cryptography with abelian varieties : results and challenges (1h). ARITH Seminar, Novembre 2011, Montpellier.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire de théorie des nombres, Septembre 2011, Bordeaux.
- About the CRT method to compute class polynomials in dimension 2 (1h). Journées C2 Codage et Cryptographie, Avril 2011, Oléron.
- Cryptology, elliptic curves and number theory (1h). Séminaire des doctorants en théorie des nombres, Mars 2011, Bordeaux.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire Arithmétique et Théorie de l'Information, Février 2011, Université Méditerranée, Marseille.
- Abelian varieties, theta functions and cryptography (1h30). Groupe de travail des doctorants, Février 2011, Université Méditerranée, Marseille.
- Computing isogenies and applications in cryptography (1h). Cryptology seminar, Janvier 2011, Université Versailles Saint-Quentin, Versailles.
- Computing isogenies and applications in cryptography (1h). Minalogic cryptology seminar, Janvier 2011, Grenoble.
- Abelian varieties, theta functions and cryptography (40min+40min). Algorithmics of L-functions workshop, Décembre 2010, Bordeaux. Part 1 on blackboard.
- On the CRT method to compute class polynomials in genus 2 (30min). ANR Chic, Décembre 2010, Paris.
- Generalizing Vélu's formulas and some applications (1h). TANC Seminar, Novembre 2010, LIX, École Polytechnique, Paris.
- Speeding up the CRT method to compute class polynomials in genus 2 (1h). Microsoft Research, Septembre 2010, Redmond, USA.
- Abelian varieties, Theta functions and cryptography (30min). Microsoft Research, Juillet 2010, Redmond, USA.
- Arithmétique rapide avec les fonctions thêta (20min). ANR Chic, Juin 2010, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire de théorie des nombres, Février 2010, Bordeaux.
- Calcul de pairing avec les fonctions thêta (1h). LFANT Cryptographic Seminar, Février 2010, Bordeaux.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire Arithmétique et Théorie de l'Information, Novembre 2009, Marseille.
- An efficient computation of the commutator pairing (20min). ANR Chic, Octobre 2009, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (40min). ANR Chic, Octobre 2009, Paris.
- Computing isogenies of small degrees on abelian varieties (20min). Journées d'arithmétiques 2009, Juillet 2009, Saint-Etienne.
- Computing isogenies of small degrees on abelian varieties (1h). Séminaire de cryptographie, Avril 2009, Rennes.
- Abelian varieties and isogenies (30min). Tsukuba Cryptographic Seminar, Novembre 2008, Tsukuba, Japon.

Vulgarisation

- Mars 2015 Échange avec le public autour du film *Imitation Game*, sur les apports d'Alain Turing à l'informatique et la cryptographie, Bordeaux.
- Avril 2014 *Algorithmic number theory and cryptography* (30min). Présentation de l'équipe auprès de la directrice d'Inria Bordeaux, Inria Bordeaux.
- Décembre 2013 *Algorithmic number theory and cryptography* (30min). Présentation de mes thèmes de recherche pour le Comité des Projets d'Inria Bordeaux, Inria Bordeaux.
- 2012 – 2013 Rédaction d'articles pour *Sonews*, le magazine interne du centre de recherche Inria Bordeaux., Bordeaux.
- Avril 2013 *Petit panorama des mathématiques de la cryptologie*. Présentation aux étudiants des *Mines de Nancy*, Labri, Bordeaux.
- Février 2012 *Panorama de la cryptographie sur les courbes elliptiques*. Cérémonie du *prix de thèse* régional, Conseil général de Lorraine, Metz. [Plus d'infos](#).
- Juin 2011 Participation au stand commun des EPST CNRS, INRA, INRIA, INSERM au salon des métiers *Aquitec 2011* : rencontres de public jeunes et leurs parents pour parler des métiers des sciences, Bordeaux.

Transparents d'activités

- Mai 2015 *MACISA — Mathematics applied to cryptology and information security in Africa* (30 min). Réunion des directeurs d'équipes du Lirima, Saint-Louis, Sénégal.
- Septembre 2014 *MACISA — Mathematics applied to cryptology and information security in Africa* (30 min). Journées d'évaluation du Lirima, Paris.
- Août 2014 *Bordeaux 2016 : A canonical choice for ANTS XII* (15 min). Presentation to host ANTS XII in Bordeaux, GyeongJu, Korea.
- Septembre 2013 *MACISA — Mathematics applied to cryptology and information security in Africa* (30min). Présentation de l'équipe MACISA dans le cadre des journées du *Lirima*, Rabat, Maroc.

Brevets

- *Kristin Lauter, Damien Robert, Computing genus 2 curves using general isogenies*. Mai 2014.

Séjours à l'étranger et participation à des conférences

- Décembre 2015 Séminaire de sécurité des systèmes d'information du Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun.
- Octobre 2015 Journées C2 Codage et Cryptographie, La Londe-Les-Maures.
- Septembre 2015 *Elliptic Curves Cryptography (ECC 2015) Summer School*, Bordeaux.
- Septembre 2015 *Modular Forms and Curves of Low Genus : Computational Aspects*, ICERM, Providence, USA.
- Mai 2015 Réunion des directeurs d'équipes du Lirima, Saint-Louis, Sénégal.
- Mars 2015 École Mathématique Africaine, Franceville, Gabon.
- Octobre 2014 *Elliptic Curves Cryptography (ECC 2014)*, Chennai, India.
- Septembre 2014 Journées d'évaluation du Lirima, Paris.
- Août 2014 International Algorithmic Number Theory Symposium (ANTS-XI), GyeongJu, Korea.
- Août 2014 International Congress of Mathematicians (ICM 2014), Seoul, Korea.
- Juin 2014 ANR Peace conference *Effective moduli spaces and applications to cryptography*, Rennes.

- Mai 2014 Discrete Logarithm Problem Conference **DLP 2014**, Ascona, Suisse.
- Mars 2014 Journées C2 Codage et Cryptographie, Grenoble.
- Octobre 2013 **Geometry and Cryptography (Geocrypt 2013)**, Tahiti.
- Septembre 2013 Journées du Lirima, Rabat, Maroc.
- Août 2013 Visite d'une semaine de Microsoft Research, Redmond, USA.
- Août 2013 **Selected Area in Cryptography (SAC 2013)**, Simon Fraser University, Canada.
- Juin 2013 **Arithmétique géométrie cryptographie et théorie des codes (AGCT 14)**, Luminy, Marseille.
- Mai 2013 Visite d'une semaine de l'EPFL, Lausanne.
- Janvier 2013 Atelier Pari/GT, Bordeaux.
- Octobre 2012 Journées C2 Codage et Cryptographie, Dinard.
- Août 2012 Visite d'une semaine de Microsoft Research, Redmond, USA.
- Juillet 2012 **International Algorithmic Number Theory Symposium (ANTS-X)**, San Diego, USA.
- Septembre 2011 Elliptic Curves Cryptography (ECC 2011) and Summer School, Nancy.
- Juin 2011 **Geometry and Cryptography (Geocrypt 2011)**, Bastia.
- Avril 2011 Journées C2 Codage et Cryptographie, Oléron.
- Décembre 2010 **Algorithmics of L-functions** workshop, Bordeaux.
- Octobre 2010 **Elliptic Curves Cryptography (ECC 2010)**, 25 year anniversary of elliptic curves computation, Redmond, USA.
- Juillet 2010 – Séjour de trois mois à Microsoft Research dans l'équipe de cryptographie pour travailler sur les polynômes de classe en genre 2, Redmond, USA.
- Septembre 2010
- Juillet 2010 **International Algorithmic Number Theory Symposium (ANTS-IX)**, Nancy.
- Mai 2010 **Conférence Algorithmique et Arithmétique avec applications à la cryptographie**, Moscou, Russie.
- Octobre 2009 Elliptic Curves Cryptography (ECC 2009), Calgary.
- Juillet 2009 **Journées d'arithmétiques 2009**, Saint-Etienne.
- Mars 2009 Arithmétique géométrie cryptographie et théorie des codes (AGCT), Luminy.
- Novembre 2008 Séjour de trois semaines à l'Université de Tsukuba dans l'équipe du professeur Okamoto pour travailler sur les couplages, Tokyo.
- Octobre 2008 CADO workshop on integer factorisation, Nancy.
- Juillet 2008 International Algorithmic Number Theory Symposium (ANTS-VIII), Banff, Canada.
- Juin 2008 Crypto week, LIX, Saclay.
- Avril 2008 École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Marseille.
- Juin 2007 LLL+25, Caen.
- Mars 2007 École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Nancy.
- Février 2007 Journées nationales du calcul formel, Luminy.
- Avril 2006 Théorie géométrique et cohomologie des groupes : rigidité et déformations (Summer school), Luminy.