Liste des publications

Damien Robert

1 Publications

1. K. Lauter et D. Robert. « Improved CRT Algorithm for class polynomials in genus 2 ». In : *ANTS* (2012). Accepted for publication at the Tenth Algorithmic Number Theory Symposium ANTS-X. University of California, San Diego, July 9 – 13, 2012 http://math.ucsd.edu/~kedlaya/ants10/. URL : http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. Slides http://www.normalesup.org/~robert/publications/slides/2012-07-ANTS-SanDiego.pdf, eprint : 2012/443, HAL : hal-00734450.
2. D. Lubicz et D. Robert. « Computing isogenies between abelian varieties ». In : *Compositio Mathematica* 148.05 (sept. 2012), p. 1483–1515. DOI : 10.1112/S0010437X12000243. arXiv : 1001.2016 [math.AG]. URL : http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL : hal-00446062.
3. 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. arXiv : 0910.4668 [cs.SC]. URL : http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL : hal-00426338.
4. D. Lubicz et D. Robert. « Efficient pairing computation with theta functions ». In : *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. 6197 (juil. 2010). Sous la dir. de G. Hanrot, F. Morain et E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. DOI : 10.1007/978-3-642-14518-6_21. URL : http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides http://www.normalesup.org/~robert/publications/slides/2010-07-ants.pdf. ANTS est une conférence internationale avec comité de lecture de référence sur la théorie algorithmique des nombres.

2 Prépublications

1. D. Lubicz et D. Robert. « A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties ». Mar. 2013. URL : http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL : hal-00806923, eprint : 2013/192.
2. R. Cosset et D. Robert. « An algorithm for computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2 ». Mar. 2011. URL : http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL : hal-00578991, eprint : 2011/143.

3 Prix

1. Second prix en Sciences pour le prix de thèse de la région Lorraine ;
2. Prix de thèse de l'université de Lorraine dans le domaine IAEM (Informatique, Automatique, Électronique, Mathématiques). *Liens.*

4 Rapports

1. A. Enge et D. Robert. « Computing class polynomials in genus 2 ». DGA Report. Avr. 2013. URL : http://www.normalesup.org/~robert/pro/publications/report/2013-04-class_poly_g2.pdf

5 Conférencier invité

1. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Geocrypt 2011 http://iml.univ-mrs.fr/ati/GeoCrypt2011/. 2011-06-23. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-06-Geocrypt.pdf
2. D. Robert. « Generalizing Vélu's formulas and some applications ». Elliptic Curves Cryptography (25th anniversary of elliptic curves computation), Redmond, http://2010.eccworkshop.org/. Oct. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-10-ECC.pdf. ECC est une conférence internationale avec conférenciers invités de référence sur la cryptologie des courbes elliptiques.
3. D. Robert. « A Vélu's like formula for computing isogenies on Abelian Varieties ». Conférence Algorithmique et Arithmétique, avec applications à la cryptographie, Moscow, http://www.mccme.ru/lifr/zykin/fr/arithalgo/index.html. Mai 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-05-Moscou.pdf

6 Exposé Cours

1. D. Robert. « Isogenies and endomorphism rings of elliptic curves ». ECC 2011 Summer School http://ecc2011.loria.fr/school.html. 2011-09-15. URL : http://www.normalesup.org/~robert/pro/publications/teaching/2011-09-ECCSummerSchool.pdf

7 Exposés à des séminaires et conférences

1. D. Robert. « On isogenies between abelian varieties ». Microsoft Research. Août 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Isogeny.pdf
2. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Microsoft Research. Août 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Pairing.pdf
3. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». AGCT 14, Luminy, http://iml.univ-mrs.fr/ati/conferences/AGCT-14_2013/. Juin 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-06-AGCT.pdf
4. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Lacal, Lausanne, http://lacal.epfl.ch/. Mai 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-05-Lausanne.pdf
5. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Talk given for the CCIS seminar, Grenoble, http://www-verimag.imag.fr/~async/CCIS/index.php. Avr. 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-04-Grenoble.pdf
6. D. Robert. « Computing cyclic isogenies using real multiplication ». ANR Peace Meeting, Paris. Notes available on http://www.normalesup.org/~robert/pro/publications/notes/2013-04-cyclic-isogenies.pdf. Avr. 2013
7. D. Robert. « Computing rational isogenies from the equations of the kernel ». ANR Peace Meeting, Paris. Nov. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-11-Peace.pdf
8. D. Robert. « Improved CRT Algorithm for class polynomials in genus 2 ». Microsoft Research, Redmond. Août 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-08-Microsoft.pdf
9. D. Robert. « About the CRT method to compute class polynomials in dimension 2 ». INRIA Team LFANT seminar, Bordeaux http://www.math.u-bordeaux1.fr/~aenge/lfant/index.php?category=seminar&page=2011. Mai 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-05-Bordeaux.pdf
10. D. Robert. « Algorithms on abelian varieties for cryptography ». Cryptographic Seminar, Caen http:

//math.unicaen.fr/~castel/seminaire_crypto/seminaire.html. Mar. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-03-Caen.pdf

11. D. Robert. « Algorithms on abelian varieties for cryptography ». INRIA Team Grace Seminar, LIX, École Polytechnique, Paris http://www.lix.polytechnique.fr/cryptologie/. Jan. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-01-LIX.pdf
12. D. Robert. « Algorithms on abelian varieties for cryptography ». Groupe de Travail « Buttes aux Cailles », ENST (Télécom ParisTech), Paris http://www.infres.enst.fr/~flori/gtbac/. Jan. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-01-Telecom.pdf
13. D. Robert. « Public key cryptography with abelian varieties : results and challenges ». Séminaire ARITH, Montpellier https://www2.lirmm.fr/arith/wiki/GT/DamienRobert-CryptographieEtCourbesElliptiques-Pr%C3%A9vuPourNovembre2011?setskin=wiki. Nov. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-11-Montpellier.pdf
14. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Séminaire de théorie des nombres, Bordeaux. Sept. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-09-Bordeaux_pairings.pdf
15. D. Robert. « About the CRT method to compute class polynomials in dimension 2 ». Journées Codage et Cryptographie http://www.lirmm.fr/c2/. Avr. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-04-C2.pdf
16. D. Robert. « Cryptology, elliptic curves and number theory ». Séminaire des doctorants en théorie des nombres, Institut mathématiques de Bordeaux. Mar. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-03-Bordeaux
17. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Séminaire arithmétique et théorie de l'information, Université Méditerranée, Luminy (Marseille). Fév. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_pairings.pdf
18. D. Robert. « Abelian varieties, theta functions and cryptography ». Groupe de travail des doctorants, Université Méditerranée, Luminy (Marseille). Fév. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_theta.pdf
19. D. Robert. « Computing isogenies and applications in cryptography ». Talk given for the UVSQ cryptology seminar, Versailles. Jan. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-01-Versailles.pdf
20. D. Robert. « Computing isogenies and applications in cryptography ». Talk given for the Minalogic cryptology seminar, Grenoble, http://www-verimag.imag.fr/Seminaires-Cryptologie.html. Jan. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-01-Grenoble.pdf
21. D. Robert. « Abelian varieties, theta functions and cryptography ». Talk in two parts given for the AlgoL workshop, Bordeaux, http://www.math.univ-toulouse.fr/~couveig/wbl. Déc. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-12-Bordeaux.pdf
22. D. Robert. « On the CRT method to compute class polynomials in genus 2 ». Talk given for the CHIC project, http://chic.gforge.inria.fr/annonces/DavidLubicz_en.html. Déc. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-12-chic.pdf
23. D. Robert. « Generalizing Vélu's formulas and some applications ». TANC Seminar, LIX, École polytechnique. Nov. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-11-LIX.pdf
24. D. Robert. « Speeding up the CRT method to compute class polynomials in genus 2 ». Microsoft Research, Redmond. Sept. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-09-Microsoft.pdf
25. D. Robert. « Abelian varieties, Theta functions and cryptography ». Microsoft Research, Redmond. Juil. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-07-Microsoft.pdf
26. D. Robert. « Arithmétique rapide avec les fonctions thêta ». Talk given for the CHIC project, http://chic.gforge.inria.fr/. Juin 2010

27. D. Robert. « A Vélu's like formula for computing isogenies on abelian varieties ». Séminaire de théorie des nombres, Bordeaux, http://www.math.u-bordeaux1.fr/imb/spip.php?article44. Fév. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-02-Bordeaux.pdf
28. D. Robert. « Calcul de pairing avec les fonctions thêta ». LFANT Cryptographic Seminar, Bordeaux, http://www.math.u-bordeaux1.fr/~enge/lfant/index.php?category=seminar&page=2009. Fév. 2010
29. D. Robert. « A Vélu's like formula for computing isogenies on abelian varieties ». Séminaire arithmétique et théorie de l'information, Marseille, http://iml.univ-mrs.fr/ati/semATI2009.html. Nov. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-11-Marseille.pdf
30. D. Robert. « An efficient computation of the commutator pairing ». Talk given for the CHIC project, http://chic.gforge.inria.fr/annonces/DavidLubicz_en.html. Oct. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-pairings.pdf
31. D. Robert. « A Vélu's like formula for computing isogenies on abelian varieties ». Talk given for the CHIC project, http://chic.gforge.inria.fr/annonces/DavidLubicz_en.html. Oct. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-isogenies.pdf
32. D. Robert. « Computing isogenies of small degrees on abelian varieties ». Journées d'arithmétiques 2009, Saint-Etienne, http://ja2009.univ-st-etienne.fr/. Juil. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-07-JourneesArithmetiques.pdf
33. D. Robert. « Computing isogenies of small degrees on abelian varieties ». Séminaire de cryptographie, Rennes, http://math2007.univ-rennes1.fr/crypto/index_old_fr.html. Avr. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-04-Rennes.pdf
34. D. Robert. « Abelian varieties and isogenies ». Cryptographic seminar, Tsukuba, http://risk.tsukuba.ac.jp/. Nov. 2008. URL : http://www.normalesup.org/~robert/pro/publication/slides/2008-11-Tsukuba.pdf

8 Thèse

D. Robert. « Fonctions thêta et applications à la cryptographie ». Thèse de doct. Université Henri-Poincarré, Nancy 1, France, juil. 2010. URL : http://www.normalesup.org/~robert/pro/publications/academic/phd.pdf. Slides http://www.normalesup.org/~robert/pro/publications/slides/2010-07-phd.pdf, TEL : tel-00528942.

9 Logiciels

1. G. Bisson, R. Cosset et D. Robert. « AVIsogenies (Abelian Varieties and Isogenies) ». Packet magma dédié au calcul explicite d'isogénies entre variétés abéliennes. 2010. URL : http://avisogenies.gforge.inria.fr. Licence libre (LGPLv2+), enregistré à l'APP (référence IDDN.FR.001.440011.000.R.P.2010.000.10000)

10 Brevet

1. Dépot d'une demande de brevet aux États-Unis avec Kristin Lauter sur « Computing genus 2 curves using general isogenies ».

11 Vulgarisation

1. D. Robert. « Petit panorama des mathématiques de la cryptologie ». Présentation aux étudiants des mines de Nancy, Labri, Bordeaux. Avr. 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-04-LabriMinesNancy.pdf.
2. D. Robert. « Panorama de la cryptographie sur les courbes elliptiques ». Cérémonie du prix de thèse régional, Conseil général de Lorraine, Metz http://net-education.cr-lorraine.fr/jahia/Jahia/pid/194. Fév. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-02-PrixTheseLorraine.pdf. Exposé grand public sur la cryptographie des courbes elliptiques réalisé pour la remise du Prix de thèse de la région Lorraine.

3. Participation au stand commun des EPST CNRS, INRA, INRIA, INSERM au salon des métiers Aquitec 2011 http://aquitec.com/ : rencontres de public jeunes et leurs parents pour parler des métiers des sciences.

12 Séjours à l'étranger et participation à des conférences

1. Arithmétique, géométrie, cryptographie et théorie des codes (AGCT), Marseille, Juin 2013.
2. Visite d'une semaine de l'EPFL, Lausanne, Mai 2013.
3. Atelier PARI/GP, Bordeaux, Janvier 2013.
4. Journées Codage et Cryptographie (C2), Dinard, Octobre 2012.
5. Visite d'une semaine de Microsoft Research, Août 2012.
6. 10th International Algorithmic Number Theory Symposium (ANTS-X), San Diego, Juillet 2012.
7. (ECC 2011), Nancy, Septembre 2011.
8. Elliptic Curves Cryptography (ECC 2011), Nancy, Septembre 2011.
9. Worskshop Algorithmics of L-functions, Bordeaux, Décembre 2010.
10. Elliptic Curves and Computation (ECC 2010, 25 year anniversary), Redmond, Octobre 2010.
11. Séjour de trois mois à Microsoft Research dans l'équipe de cryptographie pour travailler sur les polynômes de classe en genre 2, été 2010.
12. 9th International Algorithmic Number Theory Symposium (ANTS-IX), Nancy, Juillet 2010.
13. Algorithmique et Arithmétique, avec applications à la cryptographie, Moscou, Mai 2010.
14. Elliptic Curves Cryptography (ECC 2009), Calgary, Octobre 2009.
15. Les journées d'arithmétiques 2009, Saint-Etienne, Juillet 2009.
16. Arithmétique, géométrie et théorie des codes (ACGT), Marseille, Mars 2009.
17. Séjour de trois semaines à l'Université de Tsukuba dans l'équipe du professeur Okamoto pour travailler sur les couplages, Tokyo, Novembre 2008.
18. CADO workshop on integer factorisation, Nancy, Octobre 2008.
19. 8th International Algorithmic Number Theory Symposium (ANTS-IX), Banff, Juillet 2008.
20. École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Marseille, Avril 2008.
21. LLL+25, Caen, Juin 2007.
22. École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Nancy, Mars 2007.
23. Journées nationales du calcul formel, Luminy, Février 2007.
24. Théorie géométrique et cohomologie des groupes : rigidité et déformations (École d'été), Luminy, Avril 2006.