Scientific activities

Damien Robert

1 Publications

1. K. Lauter and 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 and D. Robert. “Computing isogenies between abelian varieties”. In: *Compositio Mathematica* 148.05 (Sept. 2012), pp. 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, and D. Robert. “Computing modular correspondences for abelian varieties”. In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 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 and D. Robert. “Efficient pairing computation with theta functions”. In: *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. 6197 (July 2010). Ed. by G. Hanrot, F. Morain, and 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 is an international conference with a lecture comity of reference on algorithmic number theory.

2 Prepublications

1. D. Lubicz and 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 and 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 Prizes

1. Second prize in Sciences for the Lorraine region PhD awards;

2. University of Lorraine PhD award in the IEAM domain (Computer science, Mathematics, Electronic).
See Links.

4 Reports

1. A. Enge and D. Robert. “Computing class polynomials in genus 2”. DGA Report. Apr. 2013. URL: http://www.normalesup.org/~robert/pro/publications/report/2013-04-class_poly_g2.pdf

5 Invited speaker

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 is an international conference of reference on Elliptic Curve Cryptography.

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. May 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-05-Moscou.pdf

6 Teaching talks

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 Talks

1. D. Robert. “On isogenies between abelian varieties”. Microsoft Research. Aug. 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. Aug. 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/. June 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/. May 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. Apr. 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. Apr. 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. Aug. 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. May 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/. Apr. 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). Feb. 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). Feb. 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. Dec. 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. Dec. 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. July 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/. June 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. Feb. 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. Feb. 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/. July 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. Apr. 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 PhD

D. Robert. “Fonctions thêta et applications à la cryptographie”. PhD thesis. Université Henri-Poincarré, Nancy 1, France, July 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 Software

1. G. Bisson, R. Cosset, and D. Robert. "AVIsogenies (Abelian Varieties and Isogenies)". Magma package for explicit isogenies computation between abelian varieties. 2010. URL: http://avisogenies.gforge.inria.fr. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000)

10 Patent

1. A microsoft patent has been deposed with Kristin Lauter on "Computing genus 2 curves using general isogenies".

11 Vulgarization

- D. Robert. "Petit panorama des mathématiques de la cryptologie". Présentation aux étudiants des mines de Nancy, Labri, Bordeaux. Apr. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-04-LabriMinesNancy.pdf.
- 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. Feb. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-02-PrixTheseLorraine.pdf Introductory (for large public) talk on elliptic curve cryptography given during the Lorraine Phd prize ceremony.
- Students meeting Aquitec 2011 http://aquitec.com/.

12 Conferences attended and foreign stays

1. Arithmétique, géométrie, cryptographie et théorie des codes (AGCT), Marseille, June 2013.
2. One week visit to EPFL, Lausanne, May 2013.
3. Atelier PARI/GP, Bordeaux, January 2013.
4. Journées Codage et Cryptographie (C2), Dinard, October 2012.
5. One week visit to Microsoft Research, August 2012.
6. 10th International Algorithmic Number Theory Symposium (ANTS-X), San Diego, July 2012.
7. Elliptic Curves Cryptography (ECC 2011), Nancy, September 2011.
8. Worskshop Algorithmics of L-functions, Bordeaux, December 2010.
9. Elliptic Curves and Computation (ECC 2010, 25 year anniversary), Redmond, October 2010.
10. Three month Microsoft Research Internship in the cryptographic team to work on genus 2 class polynomials with Kristin Lauter.
11. 9th International Algorithmic Number Theory Symposium (ANTS-IX), Nancy, July 2010.
12. Algorithmique et Arithmétique, avec applications à la cryptographie, Moscow, May 2010.
13. Elliptic Curves Cryptography (ECC 2009), Calgary, October 2009.
14. Les journées d'arithmétiques 2009, Saint-Etienne, July 2009.
15. Arithmétique, géométrie et théorie des codes (ACGT), Marseille, March 2009.

16. Three weeks visit at Tsukuba University in the team of professor Okamoto to work on pairings, Tokyo, November 2008.
17. CADO workshop on integer factorisation, Nancy, October 2008.
18. 8th International Algorithmic Number Theory Symposium (ANTS-IX), Banff, July 2008.
19. École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Marseille, April 2008.
20. LLL+25, Caen, June 2007.
21. École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Nancy, March 2007.
22. Journées nationales du calcul formel, Luminy, February 2007.
23. Théorie géométrique et cohomologie des groupes: rigidité et déformations(Summer school), Luminy, April 2006.