List of publications

Damien Robert

January 19, 2018

1 Preprints

1. E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". Sept. 2017. HAL: hal-01520262.
2. A. Dudeanu, jetchev, D. Robert, et al. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". Oct. 2017. HAL: hal-01629829.

2 Publications

1. D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: 10.1016/j.ffa.2016.01.009. URL: http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 2014/493.
2. D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS Journal of Computation and Mathematics* 18 (1 Feb. 2015), pp. 198–216. DOI: 10.1112/S146115701400045X. arXiv: 1402.3628. URL: http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL: hal-00954895.
3. D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: 10.1016/j.jsc.2014.08.001. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192.
4. R. Cosset and 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), pp. 1953–1975. DOI: 10.1090/S0025-5718-2014-02899-8. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143.
5. K. E. Lauter and D. Robert. "Improved CRT Algorithm for Class Polynomials in Genus 2". In: *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Berkeley: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: 10.2140/obs.2013.1.437. URL: http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. Slides: 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA), HAL: hal-00734450, eprint: 2012/443.
6. D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compositio Mathematica* 148.5 (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.
7. 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.

8. D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, July 2010. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides: 2010-07-ANTS-Nancy.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy), HAL: hal-00528944.

3 Reports

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

4 PhD Thesis

1. D. Robert. "Theta functions and cryptographic applications". PhD thesis. Université Henri-Poincarré, Nancy 1, France, July 2010. URL: http://www.normalesup.org/~robert/pro/publications/academic/phd.pdf. Slides: 2010-07-Phd-Nancy.pdf (1h, Nancy), TEL: tel-00528942.

5 Invited Speaker

1. D. Robert. "Isogenies, Polarisations and Real Multiplication". Journées C2 Codage et Cryptographie, La Londe-Les-Maures. Oct. 2015. URL: http://www.normalesup.org/~robert/pro/publications/slides/2015-10-C2-LaLondeLesMaures.pdf

2. D. Robert. "Isogenies, Polarisations and Real Multiplication". Modular Forms and Curves of Low Genus: Computational Aspects, ICERM, Providence, USA.. Sept. 2015. URL: http://www.normalesup.org/~robert/pro/publications/slides/2015-09-Providence-ICERM.pdf

3. D. Robert. "Optimal pairings on abelian varieties". Elliptic Curves Cryptography (ECC 2014), Chennai, India. Oct. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-10-ECC-Chennai.pdf

4. D. Robert. "Isogenies between abelian varieties". ANR Peace conference Effective moduli spaces and applications to cryptography, Rennes. June 2014. URL: http://www.normalesup.org/~robert/pro/publications/notes/2014-06-Rennes-Moduli.pdf

5. D. Robert. "Pairings on abelian varieties and the Discrete Logarithm Problem". Discrete Logarithm Problem Conference DLP 2014, Ascona, Suisse. May 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-05-Ascona.pdf

6. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Geometry and Cryptography (Geocrypt 2011), Bastia. June 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-06-Geocrypt-Bastia.pdf

7. D. Robert. "Generalizing Vélu's formulas and some applications". Elliptic Curves Cryptography (ECC 2010), 25 year anniversary of elliptic curves computation, Redmond, USA.. Oct. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-10-ECC-Redmond.pdf

8. D. Robert. "A Vélu's like formula for computing isogenies on Abelian Varieties". Conférence Algorithmique et Arithmétique avec applications à la cryptographie, Moscow, Russia. May 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-05-Moscou.pdf

6 Teaching Talks

1. D. Robert. "The group structure of rational points of elliptic curves over a finite field". Elliptic Curves Cryptography (ECC 2015) Summer School, Bordeaux. Sept. 2015. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2015-09-Bordeaux-ECCSummerSchool.pdf

2. D. Robert. "Isogenies and endomorphism rings of elliptic curves". ECC 2011 Summer School, Nancy. Sept. 2011. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2011-09-Nancy-ECCSummerSchool.pdf

7 Talks

1. D. Robert. "Arithmetic on Abelian and Kummer varieties". INRIA Team LFANT seminar, Bordeaux. May 2015. On blackboard, notes.

2. D. Robert. "Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties". École Mathématique Africaine, Université de Masuku, Franceville, Gabon. Mar. 2015. URL: http://www.normalesup.org/~robert/pro/publications/slides/2015-03-Franceville-Arithmetic.pdf

3. D. Robert. "Arithmetic on Abelian and Kummer varieties". Number Theory Seminar, Caen. Dec. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Arithmetic_slides.pdf. On blackboard, notes.

4. D. Robert. "Isogeny graphs in dimension 2". Cryptography Seminar, Caen. Dec. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Isogenies.pdf

5. D. Robert. "Arithmetic on Abelian and Kummer varieties". Number Theory Seminar, Institut Fourier, Grenoble. Apr. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-04-Grenoble.pdf. On blackboard, notes.

6. D. Robert. "Arithmetic on abelian varieties and related topics". Seminar in Coding Theory and Cryptography of the University of Zurich and the University of Neuchâtel, Neuchâtel, Suisse. Mar. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-03-Neuchatel.pdf

7. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Industrial ANR Simpatic meeting, Caen. Jan. 2014. URL: http://www.normalesup.org/~robert/pro/publications/slides/2014-01-Caen.pdf

8. D. Robert. "Arithmetic on Abelian and Kummer varieties". ANR Peace meeting, Rennes. Dec. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-12-Rennes-Peace.pdf

9. D. Robert. "On isogenies and polarisations". LFANT Seminar, Bordeaux. Nov. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-11-Lfant.pdf

10. D. Robert. "On isogenies and polarisations". Geometry and Cryptography (Geocrypt 2013), Tahiti. Oct. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-10-Geocrypt-Tahiti.pdf

11. D. Robert. "On isogenies between abelian varieties". Microsoft Research, Redmond, USA.. Aug. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Isogeny.pdf

12. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Microsoft Research, Redmond, USA.. Aug. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Pairing.pdf

13. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Arithmetic Geometry Cryptography and Coding Theory (AGCT 14), Luminy, Marseille. June 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-06-AGCT-Marseille.pdf

14. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Lacal, Lausanne. May 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-05-Lausanne.pdf

15. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". CCIS seminar, Grenoble. Apr. 2013. URL: http://www.normalesup.org/~robert/pro/publications/slides/2013-04-Grenoble.pdf

16. D. Robert. "Computing cyclic isogenies using real multiplication". (Notes). ANR Peace meeting, Paris. Apr. 2013. URL: http://www.normalesup.org/~robert/pro/publications/notes/2013-04-Peace-Paris-Cyclic-Isogenies.pdf

17. 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-Paris.pdf

18. D. Robert. "Improved CRT Algorithm for class polynomials in genus 2". Microsoft Research, Redmond, USA.. Aug. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-08-Microsoft.pdf

19. D. Robert. "About the CRT method to compute class polynomials in dimension 2". INRIA Team LFANT seminar, Bordeaux. May 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-05-Bordeaux.pdf

20. D. Robert. "Algorithms on abelian varieties for cryptography". Caen's Cryptographic Seminar, Caen. Mar. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-03-Caen.pdf

21. D. Robert. "Algorithms on abelian varieties for cryptography". INRIA Team Grace Seminar, LIX, École Polytechnique, Paris. Jan. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-01-LIX-Paris.pdf

22. D. Robert. "Algorithms on abelian varieties for cryptography". Butte aux caillesSeminar, Télécom ParisTech, Paris. Jan. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-01-Telecom-Paris.pdf

23. D. Robert. "Public key cryptography with abelian varieties: results and challenges". ARITH Seminar, Montpellier. Nov. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-11-Montpellier.pdf

24. 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.pdf

25. D. Robert. "About the CRT method to compute class polynomials in dimension 2". Journées C2 Codage et Cryptographie, Oléron. Apr. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-04-C2-Oleron.pdf

26. D. Robert. "Cryptology, elliptic curves and number theory". Number Theory PhD Students' seminar, Bordeaux. Mar. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-03-Bordeaux.pdf

27. D. Robert. "Computing optimal pairings on abelian varieties with theta functions". Séminaire Arithmétique et Théorie de l'Information, Université Méditerranée, Marseille. Feb. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_pairings.pdf

28. D. Robert. "Abelian varieties, theta functions and cryptography". PhD Students' seminar, Université Méditerranée, Marseille. Feb. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_theta.pdf

29. D. Robert. "Computing isogenies and applications in cryptography". Cryptology seminar, Université Versailles Saint-Quentin, Versailles. Jan. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-01-Versailles.pdf

30. D. Robert. "Computing isogenies and applications in cryptography". Minalogic cryptology seminar, Grenoble. Jan. 2011. URL: http://www.normalesup.org/~robert/pro/publications/slides/2011-01-Grenoble.pdf

31. D. Robert. "Abelian varieties, theta functions and cryptography". Algorithmics of L-functions workshop, Bordeaux. Dec. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-12-Bordeaux.pdf. Part 1 on blackboard.

32. D. Robert. "On the CRT method to compute class polynomials in genus 2". ANR Chic, Paris. Dec. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-12-Chic-Paris.pdf

33. D. Robert. "Generalizing Vélu's formulas and some applications". TANC Seminar, LIX, École Polytechnique, Paris. Nov. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-11-LIX-Paris.pdf

34. D. Robert. "Speeding up the CRT method to compute class polynomials in genus 2". Microsoft Research, Redmond, USA.. Sept. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-09-Microsoft.pdf

35. D. Robert. "Abelian varieties, Theta functions and cryptography". Microsoft Research, Redmond, USA.. July 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-07-Microsoft.pdf

36. D. Robert. "Arithmétique rapide avec les fonctions thêta". ANR Chic, Paris. June 2010

37. D. Robert. "A Vélu's like formula for computing isogenies on abelian varieties". Séminaire de théorie des nombres, Bordeaux. Feb. 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-02-Bordeaux.pdf

38. D. Robert. "Calcul de pairing avec les fonctions thêta". LFANT Cryptographic Seminar, Bordeaux. Feb. 2010

39. D. Robert. "A Vélu's like formula for computing isogenies on abelian varieties". Séminaire Arithmétique et Théorie de l'Information, Marseille. Nov. 2009. URL: http://www.normalesup.org/~robert/pro/publications/slides/2009-11-Marseille.pdf

40. D. Robert. "An efficient computation of the commutator pairing". ANR Chic, Paris. Oct. 2009. URL: http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-Paris_pairings.pdf

41. D. Robert. "A Vélu's like formula for computing isogenies on abelian varieties". ANR Chic, Paris. Oct. 2009. URL: http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-Paris_isogenies.pdf

42. D. Robert. "Computing isogenies of small degrees on abelian varieties". Journées d'arithmétiques 2009, Saint-Etienne. July 2009. URL: http://www.normalesup.org/~robert/pro/publications/slides/2009-07-JourneesArithmetiques-SaintEtienne.pdf

43. D. Robert. "Computing isogenies of small degrees on abelian varieties". Séminaire de cryptographie, Rennes. Apr. 2009. URL: http://www.normalesup.org/~robert/pro/publications/slides/2009-04-Rennes.pdf

44. D. Robert. "Abelian varieties and isogenies". Tsukuba Cryptographic Seminar, Tsukuba, Japan. Nov. 2008. URL: http://www.normalesup.org/~robert/pro/publications/slides/2008-11-Tsukuba.pdf

8 Vulgarization Talks

1. D. Robert. "Algorithmic number theory and cryptography". Team presentation for the director of Inria Bordeaux, Inria Bordeaux. Apr. 2014. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2014-04-Monique.pdf

2. D. Robert. "Algorithmic number theory and cryptography". Presentation of my research themes to the Inria Bordeaux Scientific commitee, Inria Bordeaux. Dec. 2013. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2013-12-Inria-Bordeaux-CP.pdf

3. D. Robert. "Petit panorama des mathématiques de la cryptologie". Presentation for the students in Mines de Nancy, Labri, Bordeaux. Apr. 2013. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2013-04-Labri-MinesNancy-Bordeaux.pdf

4. D. Robert. "Panorama de la cryptographie sur les courbes elliptiques". Lorraine Phd prize ceremony, Conseil général de Lorraine, Metz. Feb. 2012. URL: http://www.normalesup.org/~robert/pro/teaching/slides/2012-02-PrixTheseLorraine-Metz.pdf

9 Rump Sessions

1. D. Robert. "Sleeping in the volcano". ECC 2011 conference, Nancy. Sept. 2011. URL: http://www.normalesup.org/~robert/pro/publications/rump/2011-09-ecc_rump.pdf

2. D. Robert. "AVIsogenies, a library for computing isogenies between abelian varieties". ECC 2010, Redmond, USA.. Oct. 2010. URL: http://www.normalesup.org/~robert/pro/publications/rump/2010-10-ecc_rump.pdf

10 Softwares

1. G. Bisson, R. Cosset, and D. Robert. "AVIsogenies". Magma package devoted to the computation of isogenies 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). Latest version 0.6, released on 2012-11-28.

11 Patents

1. K. E. Lauter and D. Robert. *Computing genus* 2 *curves using general isogenies*. May 2014. URL: http://www.google.com.ar/patents/US20140105386