Liste des publications

Damien Robert

5 janvier 2025

1 Prépublications

1. S. Kunzweiler, L. Maino, T. Moriya, C. Petit, G. Pope, D. Robert, M. Stopar et Y. B. Ti. « Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3 ». Oct. 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/thetaCGL.pdf. eprint : 2024/1732, HAL : hal-04837057.
2. D. Robert. « The module action for isogeny based cryptography ». Oct. 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/module_action.pdf. eprint : 2024/1556, HAL : hal-04848019.
3. D. Robert et N. Sarkis. « Halving differential additions on Kummer lines ». Oct. 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/halfdiffadd.pdf. eprint : 2024/1582, HAL : hal-04724019.
4. D. Robert. « Fast pairings via biextensions and cubical arithmetic ». Avr. 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/biextensions.pdf. eprint : 2024/517, HAL : hal-04848028.
5. A. Page et D. Robert. « Introducing Clapoti(s) : Evaluating the isogeny class group action in polynomial time ». Nov. 2023. URL : http://www.normalesup.org/~robert/pro/publications/articles/clapotis.pdf. eprint : 2023/1766, HAL : hal-04327451.
6. D. Robert. « The geometric interpretation of the Tate pairing and its applications ». Fév. 2023. URL : http://www.normalesup.org/~robert/pro/publications/articles/geometric_tate_pairing.pdf. eprint : 2023/177, HAL : hal-04295743v1.
7. D. Robert. « Some applications of higher dimensional isogenies to elliptic curves (overview of results) ». Déc. 2022. URL : http://www.normalesup.org/~robert/pro/publications/articles/isogenies_applications.pdf. eprint : 2022/1704, HAL : hal-03943973.
8. D. Robert. « Evaluating isogenies in polylogarithmic time ». Août 2022. URL : http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf. eprint : 2022/1068, HAL : hal-03943970.
9. A. Maiga et D. Robert. « Towards computing canonical lifts of ordinary elliptic curves in medium characteristic ». Mars 2022. URL : http://www.normalesup.org/~robert/pro/publications/articles/fast_canonical_lift_g1.pdf. HAL : hal-03702658.

10. A. Maiga et D. Robert. « Computing the canonical lift of genus 2 curves in odd characteristic ». Déc. 2020. URL : http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf. HAL : hal-03738314.
11. D. Lubicz et D. Robert. « Linear representation of endomorphisms of Kummer varieties ». Déc. 2020. URL : http://www.normalesup.org/~robert/pro/publications/articles/action.pdf. HAL : hal-03204365.
12. D. Robert. « On the efficient representation of isogenies (a survey) ». Accepté pour publication dans NuTMIC 2024 (Invited Speaker). Juin 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/isogeny_survey.pdf. eprint : 2024/1071, HAL : hal-04848010.

2 Publications

1. A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert et B. Wesolowski. « SQIsign2D-West : The Fast, the Small, and the Safer ». Accepté pour publication dans Asiacrypt 2024. Août 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/sqisign2d.pdf. eprint : 2024/760, HAL : hal-04603556.
2. P. Dartois, L. Maino, G. Pope et D. Robert. « An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography ». Accepté pour publication dans Asiacrypt 2024. Août 2024. URL : http://www.normalesup.org/~robert/pro/publications/articles/_2_2__isogenies_in_the_theta_model.pdf. eprint : 2023/1747, HAL : hal-04297088.
3. S. Kunzweiler et D. Robert. « Computing modular polynomials by deformation ». In : *Research in Number Theory (ANTS XVI Conference)* 11 (10 déc. 2024). DOI : 10.1007/s40993-024-00596-5. arXiv : 2408.06990. URL : http://www.normalesup.org/~robert/pro/publications/articles/modular_deformation.pdf. HAL : hal-04671239.
4. J. Kieffer, A. Page et D. Robert. « Computing isogenies from modular equations between Jacobians of genus 2 curves ». Accepté pour publication dans Journal of Algebra. Juin 2024. arXiv : 2001.04137 [math.AG]. URL : http://www.normalesup.org/~robert/pro/publications/articles/modular_isogenies_g2.pdf. HAL : hal-02436133.
5. D. Robert et N. Sarkis. « Computing 2-isogenies between Kummer lines ». In : *IACR Communications in Cryptology* 1 (1 jan. 2024). DOI : 10.62056/abvua69p1. URL : http://www.normalesup.org/~robert/pro/publications/articles/kummer_isogenies.pdf. eprint : 2024/037, HAL : hal-04382643.
6. P. Dartois, A. Leroux, D. Robert et B. Wesolowski. « SQISignHD : New Dimensions in Cryptography ». In : Lecture Notes in Computer Science 14651 (mai 2024). Sous la dir. de M. Joye et G. Leander, p. 3-32. DOI : 10.1007/978-3-031-58716-0_1. URL : http://www.normalesup.org/~robert/pro/publications/articles/SQISignHD.pdf. eprint : 2023/436, HAL : hal-04056062v1, artifact : https://artifacts.iacr.org/tches/2022/a11.
7. D. Robert. « Breaking SIDH in polynomial time ». In : *Eurocrypt 2023* (avr. 2023). Sous la dir. de C. Hazay et M. Stam, p. 472-503. DOI : 10.1007/978-3-031-30589-4_17. URL : http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint :

2022/1038, HAL : hal-03943959, Transparents : 2023-04-Eurocrypt.pdf (15 min, Eurocrypt 2023, Avril 2023, Lyon, France).

8. D. Lubicz et D. Robert. « Fast change of level and applications to isogenies ». In : *Research in Number Theory (ANTS XV Conference)* 9.1 (déc. 2022). doi : 10.1007/s40993-022-00407-9. url : http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf. HAL : hal-03738315.
9. A. Dudeanu, D. Jetchev, D. Robert et M. Vuille. « Cyclic Isogenies for Abelian Varieties with Real Multiplication ». In : *Moscow Mathematical Journal* 22 (fév. 2022), p. 613-655. url : http://www.normalesup.org/~robert/pro/publications/articles/cyclic.pdf. HAL : hal-01629829.
10. M. Kirschmer, F. Narbonne, C. Ritzenthaler et D. Robert. « Spanning the isogeny class of a power of an elliptic curve ». In : *Mathematics of Computation* 91.333 (sept. 2021), p. 401-449. doi : 10.1090/mcom/3672. arXiv : 2004.08315. url : http://www.normalesup.org/~robert/pro/publications/articles/algebraic_obstruction.pdf. HAL : hal-02554714.
11. A. Maiga et D. Robert. « Computing the 2-adic canonical lift of genus 2 curves ». In : *Proceedings of the Seventh International Conference on Mathematics and Computing – ICMC 2021*. Sous la dir. de D. Giri, K.-K. R. Choo, S. Ponnusamy, W. Meng, S. Akleylek et S. P. Maity. T. 1412. Advances in Intelligent Systems and Computing (ICMC 2021). Singapore : Springer, mars 2022, p. 637-672. doi : 10.1007/978-981-16-6890-6_48. url : http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2_p2.pdf. HAL : hal-03119147.
12. E. Milio et D. Robert. « Modular polynomials on Hilbert surfaces ». In : *Journal of Number Theory* 216 (nov. 2020), p. 403-459. doi : 10.1016/j.jnt.2020.04.014. url : https://www.sciencedirect.com/science/article/abs/pii/S0022314X20301402. HAL : hal-01520262, Reproducible archive : https://data.mendeley.com/datasets/yy3bty5ktk/1.
13. 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. url : http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. eprint : 2014/493, HAL : hal-01057467.
14. 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. arXiv : 1402.3628. url : http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL : hal-00954895.
15. 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 (mars 2015), p. 68-92. doi : 10.1016/j.jsc.2014.08.001. url : http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. eprint : 2013/192, HAL : hal-00806923.
16. 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. url : http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. eprint : 2011/143, HAL : hal-00578991.
17. 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. URL : http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. eprint : 2012/443, HAL : hal-00734450, Transparents : 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), Juillet 2012, San Diego, USA).

18. D. Lubicz et D. Robert. « Computing isogenies between abelian varieties ». In : *Compositio Mathematica* 148.5 (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.
19. 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.
20. 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 Computer Science. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, juill. 2010. DOI : 10.1007/978-3-642-14518-6_21. URL : http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. HAL : hal-00528944, Transparents : 2010-07-ANTS-Nancy.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-IX), Juillet 2010, Nancy).

3 Rapports

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

4 Livres

1. D. Robert. *General theory of abelian varieties and their moduli spaces*. Mars 2021. URL : http://www.normalesup.org/~robert/pro/publications/books/avtheory.pdf. Draft version.
2. D. Robert. *Guide to Pairing-Based Cryptography*. 2017. URL : https://www.worldcat.org/title/guide-to-pairing-based-cryptography/oclc/971264380. Chapter 3 on « Pairings » with Sorina Ionica, and Chapter 10 on « Choosing Parameters » with Sylvain Duquesne, Nadia El Mrabet, Safia Haloui and Franck Rondepierre

5 HDR

1. D. Robert. « Algorithmes efficaces pour les variétés abéliennes et leurs espaces de module ». HDR thesis. Université Bordeaux, juin 2021. URL : http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Transparents : 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux).

6 Thèse

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

7 Conférencier invité

1. D. Robert. « From ideals to modules for isogeny based cryptography ». Leuven isogeny days 5, Leuven. Sept. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-09-Leuven.pdf
2. D. Robert. « Quand l'ajout de structure casse un cryptosystème : quelques exemples de cryptanalyse ». JSI 2024, Grenoble. Août 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-08-InriaJSI.pdf
3. D. Robert. « On the efficient representation of isogenies ». NuTMiC 2024, Szczecin. Juin 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-06-Nutmic.pdf
4. D. Robert. « Arithmetic and pairings on Kummer lines ». Leuven isogeny days 4, Leuven. Oct. 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-10-Leuven.pdf
5. D. Robert. « Efficient representation of isogenies ». EWHA-KMS International Workshop on Cryptography. Juill. 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-07-Korea-EwhaKMS.pdf
6. D. Robert. « Applications of isogenies between abelian varieties to elliptic curves ». Arithmétique en Plat Pays. Mars 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-03-Leuven.pdf
7. D. Robert. « Applications of isogenies between abelian varieties to elliptic curves cryptosystems ». Vantage Seminar. Déc. 2022. URL : http://www.normalesup.org/~robert/pro/publications/slides/2022-12-VantageSeminar.pdf
8. D. Robert. « Isogenies between abelian varieties – an algorithmic survey ». Leuven isogeny days 3, Leuven. Sept. 2022. URL : http://www.normalesup.org/~robert/pro/publications/slides/2022-09-Leuven-Isogenies.pdf
9. 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
10. 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
11. 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

12. D. Robert. « Isogenies between abelian varieties ». ANR Peace conference Effective moduli spaces and applications to cryptography, Rennes. Juin 2014. URL : http://www.normalesup.org/~robert/pro/publications/notes/2014-06-Rennes-Moduli.pdf
13. D. Robert. « Pairings on abelian varieties and the Discrete Logarithm Problem ». Discrete Logarithm Problem Conference DLP 2014, Ascona, Suisse. Mai 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-05-Ascona.pdf
14. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Geometry and Cryptography (Geocrypt 2011), Bastia. Juin 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-06-Geocrypt-Bastia.pdf
15. 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
16. D. Robert. « A Vélu's like formula for computing isogenies on Abelian Varieties ». Conférence Algorithmique et Arithmétique avec applications à la cryptographie, Moscou, Russie. Mai 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-05-Moscou.pdf

8 Exposés Cours

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

9 Exposés

1. D. Robert. « The module action on abelian varieties ». Canari Seminar, Bordeaux. Oct. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-10-Bordeaux.pdf
2. D. Robert. « Post-Quantum Cryptography : a survey of isogeny based cryptography ». Inria-Simula Workshop, Paris. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-10-Simula.pdf
3. D. Robert. « Attacks on SIDH and applications ». PQC Summer School, Chengdu, China. Juill. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-07-Chengdu.pdf
4. D. Robert. « Isogeny++ : from ideals to modules ». Quantum Safe Workshop, IBM Zurich. Mai 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-05-SQISignWorkshop.pdf
5. D. Robert. « Isogeny based cryptography : from the fall of SIKE to the rise of higher dimensional isogenies ». Workshop Inria, University of Waterloo, Université de Bordeaux, Inria, Bordeaux.

Fév. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-02-waterloo.pdf

6. D. Robert. « Number theory for post-quantum cryptography ». Conseil Scientifique„ IMB, Bordeaux. Fév. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-02-imb.pdf
7. D. Robert. « Infinitesimal pairings and CSIDH ». PEPR Isogeny meeting„ Cybercampus, Paris. Jan. 2024. URL : http://www.normalesup.org/~robert/pro/publications/slides/2024-01-PQTLS-infinitesimal_pairings.pdf
8. D. Robert. « Recent advances in isogeny based cryptography ». 8th Franco-Japanese Cybersecurity Workshop, ENSC, Bordeaux. Nov. 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-11-Bordeaux.pdf
9. D. Robert. « New applications of higher dimensional isogenies ». Loria, Nancy. Sept. 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-09-Nancy.pdf
10. D. Robert. « Breaking SIDH in polynomial time ». Institut Fourier, Grenoble. Avr. 2023. URL : http://www.normalesup.org/~robert/pro/publications/slides/2023-04-Grenoble.pdf
11. D. Robert. « Applications of isogenies between abelian varieties to elliptic curves ». LFANT Seminar, Bordeaux. Mars 2023. On blackboard
12. D. Robert. « The geometric interpretation of the Tate pairing ». ANR Ciao Workshop, Bordeaux. Déc. 2022. On blackboard
13. D. Robert. « Evaluating isogenies in polylogarithmic time ». LFANT Seminar, Bordeaux. Oct. 2022. On blackboard
14. D. Robert. « Breaking SIDH in polynomial time ». LFANT Seminar, Bordeaux. Sept. 2022. URL : http://www.normalesup.org/~robert/pro/publications/slides/2022-09-Bordeaux-SIDH.pdf
15. D. Robert. « Towards computing the canonical lift of an ordinary elliptic curve in medium characteristic ». LFANT Seminar, Bordeaux. Avr. 2022. On blackboard
16. D. Robert. « Revisiter l'algorithme de Satoh de comptage de points en petite caractéristique par relèvement canonique ». LFANT Seminar, Bordeaux. Oct. 2021. On blackboard
17. D. Robert. « Calcul d'isogénies sur des variétés abéliennes ». CIAO Kickoff Meeting, Bordeaux. Fév. 2020. On blackboard
18. D. Robert. « Extending Elkies' isogeny algorithm to genus 2 ». GAATI team, Tahiti. Jan. 2020. On blackboard
19. D. Robert. « An overview of isogenies computations ». LFANT Seminar, Bordeaux. Sept. 2019. On blackboard
20. D. Robert. « Modular Polynomials ». LIRIMA Team FAST kick-off conference, Bordeaux. Sept. 2017. On blackboard
21. D. Robert. « Arithmetic on Abelian and Kummer varieties ». INRIA Team LFANT seminar, Bordeaux. Mai 2015. On blackboard, notes.
22. D. Robert. « Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties ». École Mathématique Africaine, Université de Masuku, Franceville, Gabon. Mars 2015. URL : http://www.normalesup.org/~robert/pro/publications/slides/2015-03-Franceville-Arithmetic.pdf

23. D. Robert. « Arithmetic on Abelian and Kummer varieties ». Number Theory Seminar, Caen. Déc. 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Arithmetic_slides.pdf. On blackboard, notes.
24. D. Robert. « Isogeny graphs in dimension 2 ». Cryptography Seminar, Caen. Déc. 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Isogenies.pdf
25. D. Robert. « Arithmetic on Abelian and Kummer varieties ». Number Theory Seminar, Institut Fourier, Grenoble. Avr. 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-04-Grenoble.pdf. On blackboard, notes.
26. D. Robert. « Arithmetic on abelian varieties and related topics ». Séminaire Code et Cryptographie de l'Université de Zurich et l'Université de Neuchâtel, Neuchâtel, Suisse. Mars 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-03-Neuchatel.pdf
27. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». ANR Industrielle Simpatic meeting, Caen. Jan. 2014. URL : http://www.normalesup.org/~robert/pro/publications/slides/2014-01-Caen.pdf
28. D. Robert. « Arithmetic on Abelian and Kummer varieties ». ANR Peace meeting, Rennes. Déc. 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-12-Rennes-Peace.pdf
29. D. Robert. « On isogenies and polarisations ». LFANT Seminar, Bordeaux. Nov. 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-11-Lfant.pdf
30. 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
31. D. Robert. « On isogenies between abelian varieties ». Microsoft Research, Redmond, USA. Août 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Isogeny.pdf
32. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Microsoft Research, Redmond, USA. Août 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-08-Microsoft-Pairing.pdf
33. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Arithmétique géométrie cryptographie et théorie des codes (AGCT 14), Luminy, Marseille. Juin 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-06-AGCT-Marseille.pdf
34. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». Lacal, Lausanne. Mai 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-05-Lausanne.pdf
35. D. Robert. « Computing optimal pairings on abelian varieties with theta functions ». CCIS seminar, Grenoble. Avr. 2013. URL : http://www.normalesup.org/~robert/pro/publications/slides/2013-04-Grenoble.pdf
36. D. Robert. « Computing cyclic isogenies using real multiplication ». (Notes). ANR Peace meeting, Paris. Avr. 2013. URL : http://www.normalesup.org/~robert/pro/publications/notes/2013-04-Peace-Paris-Cyclic-Isogenies.pdf

37. 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

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

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

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

41. 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

42. D. Robert. « Algorithms on abelian varieties for cryptography ». B□utte aux cailles S□eminar, Télécom ParisTech, Paris. Jan. 2012. URL : http://www.normalesup.org/~robert/pro/publications/slides/2012-01-Telecom-Paris.pdf

43. 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

44. 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

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

46. D. Robert. « Cryptology, elliptic curves and number theory ». Séminaire des doctorants en théorie des nombres, Bordeaux. Mars 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-03-Bordeaux.pdf

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

48. D. Robert. « Abelian varieties, theta functions and cryptography ». Groupe de travail des doctorants, Université Méditerranée, Marseille. Fév. 2011. URL : http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_theta.pdf

49. 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

50. 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
51. D. Robert. « Abelian varieties, theta functions and cryptography ». Algorithmics of L-functions workshop, Bordeaux. Déc. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-12-Bordeaux.pdf. Part 1 on blackboard.
52. D. Robert. « On the CRT method to compute class polynomials in genus 2 ». ANR Chic, Paris. Déc. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-12-Chic-Paris.pdf
53. 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
54. 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
55. D. Robert. « Abelian varieties, Theta functions and cryptography ». Microsoft Research, Redmond, USA. Juill. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-07-Microsoft.pdf
56. D. Robert. « Arithmétique rapide avec les fonctions thêta ». ANR Chic, Paris. Juin 2010
57. D. Robert. « A Vélu's like formula for computing isogenies on abelian varieties ». Séminaire de théorie des nombres, Bordeaux. Fév. 2010. URL : http://www.normalesup.org/~robert/pro/publications/slides/2010-02-Bordeaux.pdf
58. D. Robert. « Calcul de pairing avec les fonctions thêta ». LFANT Cryptographic Seminar, Bordeaux. Fév. 2010
59. 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
60. 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
61. 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
62. D. Robert. « Computing isogenies of small degrees on abelian varieties ». Journées d'arithmétiques 2009, Saint-Etienne. Juill. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-07-JourneesArithmetiques-SaintEtienne.pdf
63. D. Robert. « Computing isogenies of small degrees on abelian varieties ». Séminaire de cryptographie, Rennes. Avr. 2009. URL : http://www.normalesup.org/~robert/pro/publications/slides/2009-04-Rennes.pdf
64. D. Robert. « Abelian varieties and isogenies ». Tsukuba Cryptographic Seminar, Tsukuba, Japon. Nov. 2008. URL : http://www.normalesup.org/~robert/pro/publications/slides/2008-11-Tsukuba.pdf

10 Exposés de Vulgarisation

1. D. Robert. « Les enjeux de la blockchain écologique ». Plenary session, FrenchTech, Bordeaux. Nov. 2022. URL : http://www.normalesup.org/~robert/pro/teaching/slides/2022-11-FrenchTech.pdf
2. E. Jeannot et D. Robert. « Les Cryptomonnaies et les NFT ». Unithé ou Café, Inria Bordeaux. Sept. 2022. URL : http://www.normalesup.org/~robert/pro/teaching/slides/2022-09-Unithe.pdf
3. D. Robert. « Algorithmic number theory and cryptography ». Présentation de l'équipe auprès de la directrice d'Inria Bordeaux, Inria Bordeaux. Avr. 2014. URL : http://www.normalesup.org/~robert/pro/teaching/slides/2014-04-Monique.pdf
4. D. Robert. « Algorithmic number theory and cryptography ». Présentation de mes thèmes de recherche pour le Comité des Projets d'Inria Bordeaux, Inria Bordeaux. Déc. 2013. URL : http://www.normalesup.org/~robert/pro/teaching/slides/2013-12-Inria-Bordeaux-CP.pdf
5. 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/teaching/slides/2013-04-Labri-MinesNancy-Bordeaux.pdf
6. D. Robert. « Panorama de la cryptographie sur les courbes elliptiques ». Cérémonie du prix de thèse régional, Conseil général de Lorraine, Metz. Fév. 2012. URL : http://www.normalesup.org/~robert/pro/teaching/slides/2012-02-PrixTheseLorraine-Metz.pdf

11 Rump Sessions

1. D. Robert. « Finding a supersingular isogeny path with only one isogeny computation ». Eurocrypt 2023, Lyon, France. Avr. 2023. URL : http://www.normalesup.org/~robert/pro/publications/rump/2023-04-Eurocrypt_rump.pdf
2. 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
3. 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

12 Logiciels

1. G. Bisson, R. Cosset et D. Robert. *AVIsogenies*. Packet magma dédié au calcul explicite d'isogénies entre variétés abéliennes. 2010. URL : https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/. Licence libre (LGPLv2+), enregistré à l'APP (référence IDDN.FR.001.440011.-000.R.P.2010.000.10000). Version actuelle 0.7, publiée le 2021-03-13.
2. M. Kirschmer, F. Narbonne, C. Ritzenthaler et D. Robert. *FromLatticesToModularForms*. Calcul de formes modulaire dans la classe d'isogénie d'un produit de courbes elliptiques. Avr. 2020. URL : https://gitlab.inria.fr/roberdam/fromlatticestomodularforms

3. P. Dartois, L. Maino, G. Pope et D. Robert. *ThetaIsogenies*. Calcul rapide d'isogénies en dimension deux. Nov. 2023. URL : https://github.com/ThetaIsogenies/two-isogenies
4. D. Robert. « Kummer Line ». Boîte à outil de calculs sur les lignes de Kummer. Oct. 2023. URL : https://gitlab.inria.fr/roberdam/kummer-line

13 Brevets

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