List of publications

Damien Robert

June 12, 2025

1 Preprints

1. J. Lin, D. Robert, C.-A. Zhao, and Y. Zheng. "Biextensions in pairing-based cryptography". Apr. 2025. URL: http://www.normalesup.org/~robert/pro/publications/articles/biextension_pairings.pdf. eprint: 2025/670.

2. R. Barbulescu, D. Robert, and N. Sarkis. "Models of Kummer lines and Galois representations". Mar. 2025. URL: http://www.normalesup.org/~robert/pro/publications/articles/kummer_models.pdf. eprint: 2025/543.

3. 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.

4. D. Robert. "Fast pairings via biextensions and cubical arithmetic". Apr. 2024. URL: http://www.normalesup.org/~robert/pro/publications/articles/biextensions.pdf. eprint: 2024/517, HAL: hal-04848028.

5. A. Page and 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". Feb. 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)". Dec. 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". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf. eprint: 2022/1068, HAL: hal-03943970.

9. A. Maiga and D. Robert. "Towards computing canonical lifts of ordinary elliptic curves in medium characteristic". Mar. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/fast_canonical_lift_g1.pdf. HAL: hal-03702658.

10. A. Maiga and D. Robert. "Computing the canonical lift of genus 2 curves in odd characteristic". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf. HAL: hal-03738314.

11. D. Lubicz and D. Robert. "Linear representation of endomorphisms of Kummer varieties". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/action.pdf. HAL: hal-03204365.

2 Publications

1. G. Pope, K. Reijnders, D. Robert, A. Sferlazza, and B. Smith. "Simpler and Faster Pairings from the Montgomery Ladder". Accepted for publication at IACR Communications in Cryptology (CiC). Apr. 2025. URL: http://www.normalesup.org/~robert/pro/publications/articles/cubical_ladder.pdf. eprint: 2025/672.

2. P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. H. L. Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, and B. Wesolowski. "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies". Accepted for publication at Crypto 2025. Mar. 2025. URL: http://www.normalesup.org/~robert/pro/publications/articles/pegasis.pdf. eprint: 2025/401.

3. S. Kunzweiler, L. Maino, T. Moriya, C. Petit, G. Pope, D. Robert, M. Stopar, and Y. B. Ti. "Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3". In: *Public-Key Cryptography – PKC 2025*. Vol. 15676, Lecture Notes in Computer Science. Springer, May 2025, pp. 265–299. DOI: https://doi.org/10.1007/978-3-031-91826-1_9. URL: http://www.normalesup.org/~robert/pro/publications/articles/thetaCGL.pdf. eprint: 2024/1732, HAL: hal-04837057.

4. D. Robert and N. Sarkis. "Halving differential additions on Kummer lines". In: *Advances in Cryptology – EUROCRYPT 2025*. Vol. 15606. Lecture Notes in Computer Science. Springer, Apr. 2025, pp. 416–445. DOI: https://doi.org/10.1007/978-3-031-91095-1_15. URL: http://www.normalesup.org/~robert/pro/publications/articles/halfdiffadd.pdf. eprint: 2024/1582, HAL: hal-04724019.

5. D. Robert. "On the efficient representation of isogenies (a survey)". In: *Number-Theoretic Methods in Cryptology – NuTMiC 2024*. Ed. by A. Dąbrowski, J. Pieprzyk, and J. Pomykała. Vol. 14966. Lecture Notes in Computer Science. Springer Nature Switzerland, Feb. 2025, pp. 3–84. DOI: https://doi.org/10.1007/978-3-031-82380-0_1. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogeny_survey.pdf. eprint: 2024/1071, HAL: hal-04848010.

6. A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. "SQIsign2D-West: The Fast, the Small, and the Safer". In: *Advances in Cryptology – ASIACRYPT 2024, Part III*. Vol. 15486, Lecture Notes in Computer Science. Springer Nature Switzerland, Dec. 2024, pp. 339–370. DOI: 10.1007/978-981-96-0891-1_11. URL: http://www.normalesup.org/~robert/pro/publications/articles/sqisign2d.pdf. eprint: 2024/760, HAL: hal-04603556.

7. P. Dartois, L. Maino, G. Pope, and D. Robert. "An Algorithmic Approach to $(2,2)$-isogenies in the Theta Model and Applications to Isogeny-based Cryptography". In: *Advances in Cryptology – ASIACRYPT 2024, Part III*. Vol. 15486, Lecture Notes in Computer Science. Springer Nature Switzerland, Dec. 2024, pp. 304–338. DOI: 10.1007/978-981-96-0891-1_10. URL: http://www.normalesup.org/~robert/pro/publications/articles/_2_2__isogenies_in_the_theta_model.pdf. eprint: 2023/1747, HAL: hal-04297088.

8. S. Kunzweiler and D. Robert. "Computing modular polynomials by deformation". In: *Research in Number Theory (ANTS XVI Conference)* 11 (10 Dec. 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.

9. J. Kieffer, A. Page, and D. Robert. "Computing isogenies from modular equations between Jacobians of genus 2 curves". In: *Journal of Algebra* 666 (Mar. 2025), pp. 331–386. DOI: 10.1016/j.jalgebra.2024.11.029. arXiv: 2001.04137 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular_isogenies_g2.pdf. HAL: hal-02436133.

10. D. Robert and 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.

11. P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". In: Lecture Notes in Computer Science 14651 (May 2024). Ed. by M. Joye and G. Leander, pp. 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.

12. D. Robert. "Breaking SIDH in polynomial time". In: *Eurocrypt 2023* (Apr. 2023). Ed. by C. Hazay and M. Stam, pp. 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, Slides: 2023-04-Eurocrypt.pdf (15 min, Eurocrypt 2023, April 2023, Lyon, France).

13. D. Lubicz and D. Robert. "Fast change of level and applications to isogenies". In: *Research in Number Theory (ANTS XV Conference)* 9.1 (Dec. 2022). DOI: 10.1007/s40993-022-00407-9. URL: http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf. HAL: hal-03738315.

14. A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". In: *Moscow Mathematical Journal* 22 (Feb. 2022), pp. 613–655. URL: http://www.normalesup.org/~robert/pro/publications/articles/cyclic.pdf. HAL: hal-01629829.

15. M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "Spanning the isogeny class of a power of an elliptic curve". In: *Mathematics of Computation* 91.333 (Sept. 2021), pp. 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.

16. A. Maiga and 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*. Ed. by D. Giri, K.-K. R. Choo, S. Ponnusamy, W. Meng, S. Akleylek, and S. P. Maity. Vol. 1412. Advances in Intelligent Systems and Computing (ICMC 2021). Singapore: Springer, Mar. 2022, pp. 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.

17. E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* 216 (Nov. 2020), pp. 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.

18. 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. eprint: 2014/493, HAL: hal-01057467.

19. 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.

20. 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. eprint: 2013/192, HAL: hal-00806923.

21. 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. eprint: 2011/143, HAL: hal-00578991.

22. 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. eprint: 2012/443, HAL: hal-00734450, Slides: 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA).

23. 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.

24. 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.

25. 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 Computer Science. 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. HAL: hal-00528944, Slides: 2010-07-ANTS-Nancy.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy).

3 Reports

1. M. A. Aardal, G. Adj, D. F. Aranha, A. Basso, I. A. C. Martínez, J. Chávez-Saab, M. C.-R. Santos, P. Dartois, L. D. Feo, M. Duparc, J. K. Eriksen, T. B. Fouotsa, D. L. G. Filho, B. Hess, D. Kohel, A. Leroux, P. Longa, L. Maino, M. Meyer, K. Nakagawa, H. Onuki, L. Panny, S. Patranabis, C. Petit, G. Pope, K. Reijnders, D. Robert, F. Rodríguez-Henríquez, S. Schaeffler, and B. Wesolowski. "SQIsign. Algorithm specifications and supporting documentation". Feb. 2025. URL: https://sqisign.org/spec/sqisign-20250205.pdf

2. 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 Books

1. D. Robert. *General theory of abelian varieties and their moduli spaces*. Mar. 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. "Efficient algorithms for abelian varieties and their moduli spaces". HDR thesis. Université Bordeaux, June 2021. URL: http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux).

6 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.

7 Invited Speaker

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. Aug. 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. June 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. July 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. Mar. 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. Dec. 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. June 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. May 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. June 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, Moscow, Russia. May 2010. URL: http://www.normalesup.org/~robert/pro/publications/slides/2010-05-Moscou.pdf

8 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

9 Talks

1. D. Robert. "The geometric interpretation of the Tate pairing and its applications". Geometric Tate reading group. May 2025. URL: http://www.normalesup.org/~robert/pro/publications/slides/2025-05-GeometricTate.pdf

2. D. Robert. "Cubical arithmetic on abelian varieties: introduction and applications". Biextension reading group. Feb. 2025. URL: http://www.normalesup.org/~robert/pro/publications/slides/2025-02-Cubical.pdf

3. 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

4. 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

5. D. Robert. "Attacks on SIDH and applications". PQC Summer School, Chengdu, China. July 2024. URL: http://www.normalesup.org/~robert/pro/publications/slides/2024-07-Chengdu.pdf

6. D. Robert. "Isogeny++: from ideals to modules". Quantum Safe Workshop, IBM Zurich. May 2024. URL: http://www.normalesup.org/~robert/pro/publications/slides/2024-05-SQISignWorkshop.pdf

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

8. D. Robert. "Number theory for post-quantum cryptography". Conseil Scientifique,, IMB, Bordeaux. Feb. 2024. URL: http://www.normalesup.org/~robert/pro/publications/slides/2024-02-imb.pdf

9. 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

10. 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

11. 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

12. D. Robert. "Breaking SIDH in polynomial time". Institut Fourier, Grenoble. Apr. 2023. URL: http://www.normalesup.org/~robert/pro/publications/slides/2023-04-Grenoble.pdf

13. D. Robert. "Applications of isogenies between abelian varieties to elliptic curves". LFANT Seminar, Bordeaux. Mar. 2023. On blackboard

14. D. Robert. "The geometric interpretation of the Tate pairing". ANR Ciao Workshop, Bordeaux. Dec. 2022. On blackboard

15. D. Robert. "Evaluating isogenies in polylogarithmic time". LFANT Seminar, Bordeaux. Oct. 2022. On blackboard

16. 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

17. D. Robert. "Towards computing the canonical lift of an ordinary elliptic curve in medium characteristic". LFANT Seminar, Bordeaux. Apr. 2022. On blackboard

18. D. Robert. "Revisiter l'algorithme de Satoh de comptage de points en petite caractéristique par relèvement canonique". LFANT Seminar, Bordeaux. Oct. 2021. On blackboard

19. D. Robert. "Calcul d'isogénies sur des variétés abéliennes". CIAO Kickoff Meeting, Bordeaux. Feb. 2020. On blackboard

20. D. Robert. "Extending Elkies' isogeny algorithm to genus 2". GAATI team, Tahiti. Jan. 2020. On blackboard

21. D. Robert. "An overview of isogenies computations". LFANT Seminar, Bordeaux. Sept. 2019. On blackboard

22. D. Robert. "Modular Polynomials". LIRIMA Team FAST kick-off conference, Bordeaux. Sept. 2017. On blackboard

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

24. 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

25. 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.

26. 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

27. 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.

28. 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

29. 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

30. 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

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

32. 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

33. 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

34. 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

35. 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

36. 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

37. 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

38. 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

39. 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

40. 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

41. 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

42. 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

43. 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

44. D. Robert. "Algorithms on abelian varieties for cryptography". B⊠utte aux caillesS⊠eminar, Télécom ParisTech, Paris. Jan. 2012. URL: http://www.normalesup.org/~robert/pro/publications/slides/2012-01-Telecom-Paris.pdf

45. 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

46. 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

47. 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

48. 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

49. 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

50. 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

51. 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

52. 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

53. 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.

54. 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

55. 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

56. 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

57. 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

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

59. 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

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

61. 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

62. 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

63. 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

64. 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

65. 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

66. 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

10 Vulgarization Talks

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 and 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". 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

4. 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

5. 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

6. 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

11 Rump Sessions

1. D. Robert. "Finding a supersingular isogeny path with only one isogeny computation". Eurocrypt 2023, Lyon, France. Apr. 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 Softwares

1. G. Bisson, R. Cosset, and D. Robert. *AVIsogenies*. Magma package devoted to the computation of isogenies between abelian varieties. 2010. URL: https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000). Latest version 0.7, released on 2021-03-13.

2. M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. *FromLatticesToModularForms*. Computation of modular forms in the isogeny class spanned by products of elliptic curves. Apr. 2020. URL: https://gitlab.inria.fr/roberdam/fromlatticestomodularforms

3. P. Dartois, L. Maino, G. Pope, and D. Robert. *ThetaIsogenies*. Fast computations of isogenies in dimension two. Nov. 2023. URL: https://github.com/ThetaIsogenies/two-isogenies

4. D. Robert. "Kummer Line". Toolbox for computing on Kummer lines. Oct. 2023. URL: https://gitlab.inria.fr/roberdam/kummer-line

13 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