

# Liste des publications

Damien Robert

13 novembre 2023

## 1 Prépublications

1. 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 ». Nov. 2023. URL : [http://www.normalesup.org/~robert/pro/publications/articles/\\_2\\_2\\_\\_isogenies\\_in\\_the\\_theta\\_model.pdf](http://www.normalesup.org/~robert/pro/publications/articles/_2_2__isogenies_in_the_theta_model.pdf)
2. P. DARTOIS, A. LEROUX, D. ROBERT et B. WESOŁOWSKI. « SQISignHD : New Dimensions in Cryptography ». Mars 2023. URL : <http://www.normalesup.org/~robert/pro/publications/articles/SQISignHD.pdf>. eprint : 2023/436.
3. 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](http://www.normalesup.org/~robert/pro/publications/articles/geometric_tate_pairing.pdf). eprint : 2023/177.
4. 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](http://www.normalesup.org/~robert/pro/publications/articles/isogenies_applications.pdf). eprint : 2022/1704, HAL : hal-03943973.
5. D. ROBERT. « Evaluating isogenies in polylogarithmic time ». Août 2022. URL : [http://www.normalesup.org/~robert/pro/publications/articles/polylog\\_isogenies.pdf](http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf). eprint : 2022/1068, HAL : hal-03943970.
6. 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](http://www.normalesup.org/~robert/pro/publications/articles/fast_canonical_lift_g1.pdf). HAL : hal-03702658.
7. 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](http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf). HAL : hal-03738314.
8. 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.
9. J. KIEFFER, A. PAGE et D. ROBERT. « Computing isogenies from modular equations between Jacobians of genus 2 curves ». Oct. 2020. arXiv : 2001.04137 [math.AG]. URL : [http://www.normalesup.org/~robert/pro/publications/articles/modular\\_isogenies\\_g2.pdf](http://www.normalesup.org/~robert/pro/publications/articles/modular_isogenies_g2.pdf). HAL : hal-02436133.

## 2 Publications

1. D. ROBERT. « Breaking SIDH in polynomial time ». Avr. 2023. URL : [http://www.normalesup.org/~robert/pro/publications/articles/breaking\\_sidh.pdf](http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf). eprint : 2022/1038, HAL : [hal-03943959](https://hal.archives-ouvertes.fr/hal-03943959), Transparents : [2023-04-Eurocrypt.pdf](https://hal.archives-ouvertes.fr/hal-03943959/2023-04-Eurocrypt.pdf) (15 min, Eurocrypt 2023, Avril 2023, Lyon, France).
2. 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](https://doi.org/10.1007/s40993-022-00407-9). URL : [http://www.normalesup.org/~robert/pro/publications/articles/change\\_level.pdf](http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf). HAL : [hal-03738315](https://hal.archives-ouvertes.fr/hal-03738315).
3. 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](https://hal.archives-ouvertes.fr/hal-01629829).
4. 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](https://doi.org/10.1090/mcom/3672). arXiv : [2004.08315](https://arxiv.org/abs/2004.08315). URL : [http://www.normalesup.org/~robert/pro/publications/articles/algebraic\\_obstruction.pdf](http://www.normalesup.org/~robert/pro/publications/articles/algebraic_obstruction.pdf). HAL : [hal-02554714](https://hal.archives-ouvertes.fr/hal-02554714).
5. 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](https://doi.org/10.1007/978-981-16-6890-6_48). URL : [http://www.normalesup.org/~robert/pro/publications/articles/canonical\\_lift\\_g2\\_p2.pdf](http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2_p2.pdf). HAL : [hal-03119147](https://hal.archives-ouvertes.fr/hal-03119147).
6. 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](https://doi.org/10.1016/j.jnt.2020.04.014). URL : <https://www.sciencedirect.com/science/article/abs/pii/S0022314X20301402>. HAL : [hal-01520262](https://hal.archives-ouvertes.fr/hal-01520262), Reproducible archive : <https://data.mendeley.com/datasets/yy3bty5ktk/1>.
7. 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](https://doi.org/10.1016/j.ffa.2016.01.009). URL : <http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf>. HAL : [hal-01057467](https://hal.archives-ouvertes.fr/hal-01057467), eprint : 2014/493.
8. 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](https://doi.org/10.1112/S146115701400045X). arXiv : [1402.3628](https://arxiv.org/abs/1402.3628). URL : <http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf>. HAL : [hal-00954895](https://hal.archives-ouvertes.fr/hal-00954895).
9. 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](https://doi.org/10.1016/j.jsc.2014.08.001). URL : <http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf>. HAL : [hal-00806923](https://hal.archives-ouvertes.fr/hal-00806923), eprint : 2013/192.
10. R. COSSET et D. ROBERT. « An algorithm for computing  $(\ell, \ell)$ -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](https://doi.org/10.1090/S0025-5718-2014-02899-8). URL : <http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf>. HAL : [hal-00578991](https://hal.archives-ouvertes.fr/hal-00578991), eprint : 2011/143.
11. 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](https://doi.org/10.2140/obs.2013.1.437). URL : <http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf>. Transparents : [2012-07-ANTS-SanDiego.pdf](#) (30min, International Algorithmic Number Theory Symposium (ANTS-X), Juillet 2012, San Diego, USA), HAL : [hal-00734450](https://hal.archives-ouvertes.fr/hal-00734450), eprint : 2012/443.
  12. D. LUBICZ et D. ROBERT. « Computing isogenies between abelian varieties ». In : *Compositio Mathematica* 148.5 (sept. 2012), p. 1483-1515. DOI : [10.1112/S0010437X12000243](https://doi.org/10.1112/S0010437X12000243). arXiv : [1001.2016](https://arxiv.org/abs/1001.2016) [math.AG]. URL : <http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf>. HAL : [hal-00446062](https://hal.archives-ouvertes.fr/hal-00446062).
  13. 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](https://doi.org/10.1016/j.jalgebra.2011.06.031). arXiv : [0910.4668](https://arxiv.org/abs/0910.4668) [cs.SC]. URL : <http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf>. HAL : [hal-00426338](https://hal.archives-ouvertes.fr/hal-00426338).
  14. 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 Comput. Sci. 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](https://doi.org/10.1007/978-3-642-14518-6_21). URL : <http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf>. Transparents : [2010-07-ANTS-Nancy.pdf](#) (30min, International Algorithmic Number Theory Symposium (ANTS-IX), Juillet 2010, Nancy), HAL : [hal-00528944](https://hal.archives-ouvertes.fr/hal-00528944).

### 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](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-Poincaré, 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. « 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>
2. D. ROBERT. « Efficient representation of isogenies ». [EWA-KMS International Workshop on Cryptography](#). Juill. 2023. URL : <http://www.normalesup.org/~robert/pro/publications/slides/2023-07-Korea-EwhaKMS.pdf>
3. 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>
4. 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>
5. 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>
6. D. ROBERT. « Isogenies, Polarisation 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>
7. D. ROBERT. « Isogenies, Polarisation 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>
8. 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>
9. 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>
10. 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>

11. 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>
12. 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>
13. 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. « New applications of higher dimensional isogenies ». Loria, Nancy. Sept. 2023. URL : <http://www.normalesup.org/~robert/pro/publications/slides/2023-09-Nancy.pdf>
2. 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>
3. D. ROBERT. « Applications of isogenies between abelian varieties to elliptic curves ». *LFANT Seminar*. Mars 2023. On blackboard
4. D. ROBERT. « The geometric interpretation of the Tate pairing ». ANR Ciao Workshop. Déc. 2022. On blackboard
5. D. ROBERT. « Evaluating isogenies in polylogarithmic time ». *LFANT Seminar*. Oct. 2022. On blackboard
6. 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>
7. D. ROBERT. « Towards computing the canonical lift of an ordinary elliptic curve in medium characteristic ». *LFANT Seminar*, Bordeaux. Avr. 2022. On blackboard
8. D. ROBERT. « Revisiter l'algorithme de Satoh de comptage de points en petite caractéristique par relèvement canonique ». *LFANT Seminar*, Bordeaux. Oct. 2021. On blackboard
9. D. ROBERT. « Calcul d'isogénies sur des variétés abéliennes ». *CIAO Kickoff Meeting*, Bordeaux. Fév. 2020. On blackboard

10. D. ROBERT. « Extending Elkies' isogeny algorithm to genus 2 ». **GAATI team**, Tahiti. Jan. 2020. On blackboard
11. D. ROBERT. « An overview of isogenies computations ». **LFANT Seminar**, Bordeaux. Sept. 2019. On blackboard
12. D. ROBERT. « Modular Polynomials ». **LIRIMA Team FAST kick-off conference**, Bordeaux. Sept. 2017. On blackboard
13. D. ROBERT. « Arithmetic on Abelian and Kummer varieties ». **INRIA Team LFANT seminar**, Bordeaux. Mai 2015. On blackboard, [notes](#).
14. 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>
15. 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](http://www.normalesup.org/~robert/pro/publications/slides/2014-12-Caen-Arithmetic_slides.pdf). On blackboard, [notes](#).
16. 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>
17. 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](#).
18. 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>
19. D. ROBERT. « Computing optimal pairings on abelian varieties with theta functions ». **ANR Industrielle Simpatc meeting**, Caen. Jan. 2014. URL : <http://www.normalesup.org/~robert/pro/publications/slides/2014-01-Caen.pdf>
20. 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>
21. D. ROBERT. « On isogenies and polarisations ». **LFANT Seminar**, Bordeaux. Nov. 2013. URL : <http://www.normalesup.org/~robert/pro/publications/slides/2013-11-Lfant.pdf>
22. 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>
23. 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>
24. 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>

25. 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>
26. 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>
27. 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>
28. 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>
29. 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>
30. 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>
31. 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>
32. 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>
33. 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>
34. D. ROBERT. « Algorithms on abelian varieties for cryptography ». *Bûtte aux cailles* Seminar, Télécom ParisTech, Paris. Jan. 2012. URL : <http://www.normalesup.org/~robert/pro/publications/slides/2012-01-Telecom-Paris.pdf>
35. 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>
36. 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>
37. 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-C2-0leron.pdf>

38. 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>
39. 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](http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_pairings.pdf)
40. 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](http://www.normalesup.org/~robert/pro/publications/slides/2011-02-Marseille_theta.pdf)
41. 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>
42. 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>
43. 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.
44. 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>
45. 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>
46. 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>
47. 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>
48. D. ROBERT. « Arithmétique rapide avec les fonctions thêta ». *ANR Chic*, Paris. Juin 2010
49. 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>
50. D. ROBERT. « Calcul de pairing avec les fonctions thêta ». *LFANT Cryptographic Seminar*, Bordeaux. Fév. 2010
51. 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>



52. 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](http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-Paris_pairings.pdf)
53. 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](http://www.normalesup.org/~robert/pro/publications/slides/2009-10-Chic-Paris_isogenies.pdf)
54. 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>
55. 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>
56. 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](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](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](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>

## 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>