Curve-Based Cryptography

[1] Toru Akishita, Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *Some improved algorithms for hyperelliptic curve cryptosystems using degenerate divisors*, Information Security and Cryptology. ICISC 2004: 7th International Conference, Seoul, Korea, December 2–3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, p. 296.

[2] Christine Abegail Antonio, Satoru Nakamula, and Ken Nakamula, *Comparing implementation efficiency of ordinary and squared pairings*, IACR eprint:2007:457 (2007).

[3] Christine Abegail Antonio, Satoru Tanaka, and Ken Nakamula, *Implementing cryptographic pairings over curves of embedding degrees 8 and 10*, 2007.

[4] Seigo Arita, Kazuto Matsuo, Koh-ichi Nagao, and Mahoro Shimura, *A Weil descent attack against elliptic curve cryptosystems over quartic extension fields*, IEICE Trans. Fundamentals **E89-A** (2006), no. 5, 28.

[5] Daniel V. Bailey, Brian Baldwin, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Gauthier van Damme, Giacomo de Meulenaer, Junfeng Fan, Tim Gneysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Christof Paar, Francesco Regazzoni, Peter Schwabe, and Leif Uhsadel, *The Certicom Challenges ECC2-X*, Tech. report, 2009.

[6] M. Barbosa, A. Moss, and D. Page, *Compiler assisted elliptic curve cryptography*, On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Lecture Notes in Computer Science, vol. 4804/2007, Springer Berlin / Heidelberg, 2007, pp. 1785–1802.

[7] ———, *Constructive and destructive use of compilers in elliptic curve cryptography*, J. Cryptology **Online first** (2008), 23.

[8] Paulo S. L. M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks: Third International Conference,SCN 2002,Amalfi,Italy,September 11-13,2002. Revised Papers., Lecture Notes in Comput. Sci., vol. 2576, Springer, Berlin, 2003, p. 257.

[9] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel, *Implementing the arithmetic of $C_{3,4}$ curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 87–101. MR MR2137346 (2006a:14101)

[10] Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005 (electronic). MR MR2164107

[11] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, Progress in cryptology—INDOCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4859, Springer, Berlin, 2007, pp. 167–182. MR MR2570254

[12] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 29–50.

[13] Peter Birkner, *Efficient arithmetic on low-genus curves*, Ph D thesis, Technische Universiteit Eindhoven, 2009.

[14] Friederike Brezing and Annegret Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37** (2005), no. 1, 133–141. MR MR2165045

[15] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas, *Hyperelliptic curves with compact parameters*, Des. Codes Cryptogr. **36** (2005), no. 3, 245–261. MR MR2162578

[16] Kyo Il Chung, Mun-Kyu Lee, Kunsoo Park, and Tae Jun Park, *Speeding up scalar multiplication in genus 2 hyperelliptic curves with efficient endomorphisms*, ETRI **27** (2005), no. 5, 617–627.

[17] S. Cui, P. Duan, and C. W. Chan, *A new method of building more non-supersingular elliptic curves*, Computational Science and Its Applications, Lecture Notes in Comput. Sci., vol. 3481, Springer, Berlin, 2005, p. 657.

[18] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)

[19] Claus Diem, *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32. MR MR1966526 (2004a:14030)

[20] ———, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557. MR MR2282948

[21] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611. MR MR2438510

[22] Régis Dupont, Andreas Enge, and François Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, J. Cryptology **18** (2005), no. 2, 79–89. MR MR2148052 (2006c:11073)

[23] I. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology—Asiacrypt'99 (Singapore), Lecture Notes in Comput. Sci., vol. 1716, Springer, Berlin, 1999, pp. 103–121. MR MR1773225

[24] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 1–28. MR MR2484046

[25] David Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing-based cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 152–176. MR MR2423638

[26] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, Journal of Cryptology **23** (2010), no. 2, 224–280.

[27] S. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, IEEE Transactions on Information Theory **54** (2008), no. 12, 5719–5728.

[28] S. D. Galbraith, X. Lin, and D. J. Mireles, *Pairings on hyperelliptic curves with a real model*, LNCS 5209, Eds. Galbraith, S. D. and Paterson, K. G.., Springer, 2008, pp. 256–281.

[29] Steven Galbraith, *Disguising tori and elliptic curves*, 2006.

[30] Steven D. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 495–513. MR MR1934860 (2004b:14037)

[31] ———, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)

[32] Steven D. Galbraith, Michael Harrison, and David J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 342–356. MR MR2467851 (2010f:14024)

[33] Steven D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack*, Advances in Cryptology—Eurocrypt 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, Springer, Berlin, 2002, pp. 29–44. MR MR1975526 (2004f:94060)

[34] Steven D. Galbraith, Xibin Lin, and David J. Mireles Morales, *Pairings on hyperelliptic curves with a real model*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 265–281.

[35] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, 2005.

[36] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR MR1880933 (2003b:14032)

[37] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR MR2444631 (2009j:94110)

[38] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology—Eurocrypt 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34. MR MR1772021

[39] ———, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, 2004.

[40] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR MR1934859 (2003h:11159)

[41] Pierrick Gaudry and Éric Schost, *Construction of secure random curves of genus 2 over prime fields*, Advances in Cryptology—EuroCrypt 2004, Lecture Notes in Comput. Sci., vol. 3027, Springer, Berlin, 2004, pp. 239–256. MR MR2153176

[42] R. Granger and F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, Crypto 2005: 25th Annual International Cryptology Conference (Santa Barbara, Cal., Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, p. 66.

[43] Robert Granger, *On the static Diffie-Hellman problem on elliptic curves over extension fields*, Advances in Cryptology - ASIACRYPT 2010 (Masayuki Abe, ed.), Lecture Notes in Computer Science, vol. 6477, Springer Berlin/Heidelberg, 2010, pp. 283–302.

[44] Nicolas Gürel, *Extracting bits from coordinates of a point of an elliptic curve*, 2005.

[45] Darrel Hankerson, Koray Karabina, and Alfred Menezes, *Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields*, 2008.

[46] David Harvey, *Kedlaya's algorithm in larger characteristic*, Int. Math. Res. Not. IMRN (2007), no. 22, Art. ID rnm095, 29. MR MR2376210

[47] F. Hess, *Weil descent attacks*, Advances in Elliptic Curve Cryptography, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge Univ. Press, Cambridge, 2005, pp. 151–180. MR MR2169214

[48] Laura Hitt, *Families of genus 2 curves with small embedding degree*, J. Math. Cryptol. **3** (2009), no. 1, 19–36. MR MR2524253

[49] Koh ichi Nagao, *Decomposed attack for the jacobian of a hyperelliptic curve over an extension field*, 2007.

[50] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)

[51] Waldyr D. Benits Junior and Steven D. Galbraith, *Constructing pairing-friendly elliptic curves using Gröbner basis reduction*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 336–345.

[52] Koray Karabina and Edlyn Teske, *On prime-order elliptic curves with embedding degrees k=3,4, and 6*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 102–117.

[53] Masanobu Katagi, Toru Akishita, Izuru Kitamura, and Tsuyoshi Takagi, *Efficient hyperelliptic curve cryptosystems using theta divisors*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 151–160.

[54] Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *A point halving algorithm for hyperelliptic curves*.

[55] David R. Kohel, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)

[56] Tanja Lange and Marc Stevens, *Efficient doubling on genus two curves over binary fields*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3357, Springer, Berlin, 2005, pp. 170–181. MR MR2181316

[57] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park, *Efficient and generalized pairing computation on abelian varieties*, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1793–1803. MR MR2582765

[58] Reynald Lercier and David Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), no. 3, 399–423. MR MR2293798 (2008b:11069)

[59] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)

[60] Markus Maurer, Alfred Menezes, and Edlyn Teske, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree (extended abstract)*, Progress in Cryptology—Indocrypt 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 195–213. MR MR1934497

[61] ———, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree*, LMS J. Comput. Math. **5** (2002), 127–174 (electronic). MR MR1942257 (2003k:94034)

[62] J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls, *Isogeny cordillera algorithm to obtain cryptographically good elliptic curves*, ACSW '07: Proceedings of the fifth

Australasian symposium on ACSW frontiers, Australian Computer Society, Inc., 2007, pp. 153–157.

[63] Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica, *A study of pairing computation for curves with embedding degree* 15, 2009.

[64] A. Muzereau, N. P. Smart, and F. Vercauteren, *The equivalence between the DHP and DLP for elliptic curves used in practical applications*, LMS J. Comput. Math. **7** (2004), 50–72 (electronic). MR MR2047214 (2005b:94038)

[65] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng, *CM construction of genus 2 curves with p-rank 1*, 2008.

[66] Tae-Jun Park, Mun-Kyu Lee, and Kunsoo Park, *Efficient scalar multiplication in hyperelliptic curves using a new Frobenius expansion*, ICISC 2003: Information Security and Cryptology, Lecture Notes in Comput. Sci., vol. 2971, Springer, Berlin, 2004, pp. 152–165. MR MR2093706 (2005f:94116)

[67] L. J. D. Perez, Ezekiel J. Kachisa, and Michael Scott, *Implementing cryptographic pairings: A Magma tutorial*, 2009.

[68] Tanaka Satoru and Nakamula Ken, *More constructing pairing-friendly elliptic curves for cryptography*, 2007.

[69] Jasper Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, 2004.

[70] Michael Scott and Paulo S. L. M. Barreto, *On a (flawed) proposal to build more pairing-friendly curves*, 2005.

[71] Katsuyuki Takashima, *New families of hyperelliptic curves with efficient Gallant-Lambert-Vanstone method*, Information Security and Cryptology, ICISC 2004: 7th International Conference, Seoul, Korea, December 2-3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, pp. 279–295.

[72] Katsuyuki Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 124–133.

[73] ———, *Scaling security of elliptic curves with fast pairing using efficient endomorphisms*, IEICE Trans. Fundamentals **E-90A** (2007), no. 1, 152–159.

[74] ———, *Efficiently computable distortion maps for supersingular curves*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer Berlin/Heidelberg, 2008, pp. 88–101.

[75] Satoru Tanaka and Ken Nakamula, *Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 136–145.

[76] Edlyn Teske, *An elliptic curve trapdoor system (extended abstract)*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 341–352. MR MR2076258

[77] ———, *An elliptic curve trapdoor system*, J. Cryptology **19** (2006), no. 1, 115–133. MR MR2210901 (2006k:94116)

[78] Frederik Vercauteren, *The hidden root problem*, Pairing-Based Cryptography - Pairing, Lecture Notes in Computer Science, vol. 5209, SpringerLink, Berlin, 2008, pp. 89–99. MR)

[79] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296. MR MR2090558

[80] Annegret Weng, *Generation of random Picard curves for cryptography*, 2004.

[81] ———, *A low-memory algorithm for point counting on Picard curves*, Des. Codes Cryptogr. **38** (2006), no. 3, 383–393. MR MR2195523 (2006j:11168)

[82] Fangguo Zhang, *Twisted ate pairing on hyperelliptic curves and applications*, 2008.

[83] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang, *All pairings are in a group*, IEICE Trans A: Fundamentals **E91-A** (2008), no. 10, 3084–3087.