

# Publications

- Kachisa, E.J., Schaefer, E.F. and Scott M. *Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field*, Pairing 2008, 126-135.
- Poonen, B., Schaefer, E.F. and Stoll, M. *Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$* , Duke Mathematical Journal, **137**, 2007, 103–158.
- Schaefer, E.F. *Mathematics in Malawi*. Nieuw Archief voor Wiskunde, **5/7**, 2006, 276–277.
- Schaefer, E.F., *Teaching immersion in the developing world*, Explore, (9), Ignation Center at Santa Clara University, Spring 2006.
- Schaefer, E.F. *Improved implementation of pairing based cryptography*, Proceedings of the Southern African Mathematical Sciences Association, 2005.
- Dyer, K. and Schaefer, E.F. *Linear cryptanalysis of a 16 step MD5 algorithm over the rationals*, Proceedings of the Southern African Mathematical Sciences Association, 2005.
- Schaefer, E.F. *A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field*. In: Computational aspects of algebraic curves, 1–12, Lecture Notes Ser. Comput., 13, World Sci. Publ. Hackensack, NJ, 2005.
- Schaefer, E.F. and Wetherell, J.L. *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian*. J. Number Theory **115**, 2005, 158–175.
- Schaefer, E.F. and Stoll, M. *How to do a  $p$ -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356**, 2004, 1209–1231.
- Schaefer, E.F. *When is an integer the product of two and three consecutive integers?*, in David F. Hayes and Tatiana Shubin (eds.): *Mathematical Adventures for Students and Amateurs*, Mathematical Association of America, Washington DC, 2004, 65–71.
- Kloosterman, R. and Schaefer, E.F. *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory, **99**, 2003, 148–163.
- Musa, M.A., Schaefer, E.F. and Wedig, S. *A simplified AES algorithm and its linear and differential cryptanalyses*, Cryptologia, **17**, 2003, 148–177.
- Flynn, E.V., Leprévost, F. Schaefer, E.F. Stein, W.A., Stoll, M. and Wetherell, J.L. *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp., **70**, 2001, 1675–1697.
- Djabri, Z., Schaefer, E.F. and Smart, N. *Computing the  $p$ -Selmer group of an elliptic curve*, Trans. Amer. Math. Soc., **352** 2000, 5583–5597.
- Schaefer, E.F. *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann., **310**, 1998, 447–471.

- Poonen, B. and Schaefer, E.F. *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math., **488**, 1997, 141–188.
- Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J., **90**, 1997, 435–463.
- Schaefer, E.F. *A simplified Data Encryption Standard algorithm*, Cryptologia, **20**, 1996, 77–84.
- Klassen, M.J. and Schaefer, E.F. *Arithmetic and geometry of the curve  $1 + y^3 = x^4$* , Acta Arith., **74**, 1996, 241–257.
- Schaefer, E.F. *Class groups and Selmer groups*, J. Number Theory, **56**, 1996, 79–114.
- Schaefer, E.F. *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory, **51**, 1995, 219–232.
- Clark, H.H. and Schaefer, E.F. *Dealing with Overhearers*, in H.H. Clark, *Arenas of Language Use*. University of Chicago Press, 1991.
- Clark, H.H. and Schaefer, E.F. *Contributing to discourse*, Cognitive Science **13**, 1989, 259–294.
- Clark, H.H. and Schaefer, E.F. *Concealing one’s meaning from overhearers*, Journal of Memory and Language **26**, 1987, 209–225.
- Clark, H.H. and Schaefer, E.F. *Collaborating on contributions to conversation*, Language and Cognitive Processes **2**, 1987, 19–41. Reprinted in R. Dietrich & C.F. Graumann (eds), *Language processing in a social context*, North Holland, Amsterdam, 1989.

## Published reviews

- Schaefer, E.F., review of Blake, I., Seroussi, G. and Smart, N. *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999, for *Nieuw Archief voor Wiskunde* **5-1-3**, 2000, p. 322.
- Schaefer, E.F., review of Holden, Christopher; *Mod 4 Galois representations and elliptic curves*. Proc. Amer. Math. Soc. **136** (2008), no. 1, 31–39. MR2350385 (2008k:11059)
- Schaefer, E.F., review of Lange, Tanja; Shparlinski, Igor *Collisions in fast generation of ideal classes and points on hyperelliptic and elliptic curves*. Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 5, 329–337. MR2122309 (2005m:11115)
- Schaefer, E.F., review of Leprvost, F.; Pohst, M.; Schöpp, A. *Rational torsion of  $J_0(N)$  for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10*. Abh. Math. Sem. Univ. Hamburg **74** (2004), 193–203. MR2112831 (2005h:11131).

- Schaefer, E.F., review of Rubin, Karl; Silverberg, Alice Algebraic tori in cryptography. High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 317–326, Fields Inst. Commun., **41**, Amer. Math. Soc., Providence, RI, 2004. MR2076256 (2005g:14053)
- Schaefer, E.F., review of Bruin, Nils Visualising Sha[2] in abelian surfaces. Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR2047096 (2005c:11067)
- Schaefer, E.F., review of Bruin, N. and Flynn, E.V. *n*-covers of hyperelliptic curves, Math. Proc. Cambridge Philos. Soc. **134**, 2003, no. 3, 397–405, for *Mathematical Reviews*, American Mathematical Society, 2004b:11089.
- Schaefer, E.F., review of DeLong, M. *A formula for the Selmer group of a rational three-isogeny*, Acta Arith. **105**, 2002, 119–131, for *Mathematical Reviews*, American Mathematical Society, 2003i:11069.
- Schaefer, E.F., review of Stoll M. *On the height constant for curves of genus two. II*, Acta Arith. **104**, 2002, 165–182, for *Mathematical Reviews*, American Mathematical Society, 2003f:11093.
- Schaefer, E.F., review of Girard, M. *Géométrie du groupe des points de Weierstrass d'une quartique lisse*, J. Number Theory **94**, 2002, 103–135, for *Mathematical Reviews*, American Mathematical Society, 2003c:11069.
- Schaefer, E.F., review of Goto, T. *Calculation of Selmer groups of elliptic curves with rational 2-torsions and  $\theta$ -congruent number problem*, Comment. Math. Univ. St. Paul. **50**, 2001, 147–172, for *Mathematical Reviews*, American Mathematical Society, 2003a:11066.
- Schaefer, E.F., review of Flynn, E.V. *Coverings of curves of genus 2 in Algorithmic Number Theory*, Leiden, 2000, Lecture notes in Computer Science **1838**, Springer, Berlin, 2000, 65–84, for *Mathematical Reviews*, American Mathematical Society, 2002f:11074.
- Schaefer, E.F., review of Stoll, M. *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arithmetica **98**, 2001, no. 3, 245–277, for *Mathematical Reviews*, American Mathematical Society, 2002b:11089.
- Schaefer, E.F., review of O'Neil, C. *Jacobians of genus one curves*, Mathematical Research Letters **8**, 2001, no. 1-2, 125–140, for *Mathematical Reviews*, American Mathematical Society, 2002a:14031.
- Schaefer, E.F., review of Kulesz, L. *Jacobiennes de courbes algébriques de genre 2 et 3 de grand rang sur  $\mathbf{Q}$* , Journal of the London Mathematical Society **63**, 2001, no. 2, 288–298, for *Mathematical Reviews*, American Mathematical Society, 2001m:11105.
- Schaefer, E.F., review of Howe, E., Leprévost F., and Poonen B. *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12**, 2000, no. 3, 315–364, for *Mathematical Reviews*, American Mathematical Society, 2001e:11071.