Lim, C. H. and Lee, P. J. (1994). More flexible exponentiation with precomputation. In *Advances in Cryptology — CRYPTO'94*, volume 839 of *Lecture Notes in Computer Science*, pages 95–107. Springer Berlin / Heidelberg.

López, J. and Dahab, R. (2000). High-speed software multiplication in $\mathbb{F}_{2^m}$. In *Progress in Cryptology — INDOCRYPT 2000*, volume 1977 of *Lecture Notes in Computer Science*, pages 93–102. Springer Berlin / Heidelberg.

Miller, V. S. (1986). Short programs for functions on curves. *Unpublished manuscript*, 97:101–102.

Möller, B. (2001). Algorithms for multi-exponentiation. In *Selected Areas in Cryptography*, volume 2259 of *Lecture Notes in Computer Science*, pages 165–180. Springer Berlin / Heidelberg.

Montgomery, P. L. (1985). Modular multiplication without trial division. *Mathematics of Computation*, 44(170):519–521.

National Institute of Standards and Technology (2007). Recommendation for key management. `http://www.itl.nist.gov`.

National Institute of Standards and Technology (2009). FIPS 186-3: Digital signature standard (DSS). `http://www.itl.nist.gov`.

Nogami, Y., Akane, M., Sakemi, Y., Kato, H., and Morikawa, Y. (2008). Integer variable χ-based Ate pairing. In *Pairing-Based Cryptography — Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 178–191. Springer Berlin / Heidelberg.

Oliveira, L., Scott, M., López, J., and Dahab, R. (2008). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. In *Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, pages 173–180.

Sakai, R., Ohgishi, K., and Kasahara, M. (2000). Cryptosystems based on pairing. In *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*.

Scott, M. (2007). Optimal irreducible polynomials for GF(2^m) arithmetic. Cryptology ePrint Archive, Report 2007/192. `http://eprint.iacr.org/`.

Scott, M., Benger, N., Charlemagne, M., Perez, L. J. D., and Kachisa, E. J. (2009). Fast hashing to G_2 on pairing-friendly curves. In *Pairing-Based Cryptography — Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg.

Solinas, J. A. (2000). Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography*, 19(2):195–249.

Szczechowiak, P., Kargl, A., Scott, M., and Collier, M. (2009). On the application of pairing based cryptography to wireless sensor networks. In *Proceedings of the second ACM conference on Wireless network security*, pages 1–12. ACM New York.

Vercauteren, F. (2010). Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461.