IEEE P1363 / D13 (Draft Version 13). Standard Specifications for Public Key Cryptography

Annex F (Informative). Bibliography.

Comments and suggestions are welcome. Please contact the chair, Ari Singer, at singerar@pb.com.

ANNEX F (informative) Bibliography

[AM98] C. Adams and M. Myers, "Certificate Management Message Formats," Internet Engineering Task Force (IETF), PKIX working group, work in progress. Available at `http://www.ietf.org/ids.by.wg/pkix.html`.

[AK98] Ross Anderson and Markus Kuhn, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," D. Aucsmith, editor, *Second International Workshop on Information Hiding – IH'98, Lecture Notes In Computer Science* **1525** (1998), Springer-Verlag.

[ANS85] ANSI X9.17-1985, Financial institution key management (wholesale).

[ANS97a] ANSI X9.30:1-1997, Public Key Cryptography for the Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA) (revision of X9.30:1-1995).

[ANS97b] ANSI X9.30:2-1997, Public Key Cryptography for the Financial Services Industry: Part 2: The Secure Hash Algorithm (SHA-1) (revision of X9.30:2-1993).

[ANS97c] ANSI X9.57-1997, Public Key Cryptography for the Financial Services Industry: Certificate Management.

[ANS98a] ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).

[ANS98b] ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithms, draft, 1998.

[ANS98c] ANSI X9.44, Key Management Using Reversible Public Key Cryptography for the Financial Services Industry, draft, 1998.

[ANS98d] ANSI X9.52-1998, Cryptography for the Financial Services Industry: Triple Data Encryption Algorithm Modes of Operation.

[ANS98e] ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

[ANS98f] ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols, draft, 1998.

[ANS98g] ANSI X9.80, Public Key Cryptography for the Financial Services Industry: Prime Number Generation and Validation Methods, draft, 1998.

[ANS98h] ANSI X9.TG-17 Public-Key Cryptography for the Financial Services Industry: Technical Guideline on Elliptic Curve Arithmetic, to appear.

[ABV89] D. Ash, I. Blake, and S. Vanstone, "Low Complexity Normal Bases," *Discrete Applied Mathematics* **25** (1989), 191-210.

[Atk92] O. Atkin, "Square roots and cognate matters modulo $p = 8n + 5$," Internet communication to Number Theory mailing list (11 Nov 1992), archived at http://listserv.nodak.edu/scripts/wa.exe?A2=ind9211&L=nmbrthry&O=T&P=562

[BDPR98] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes," H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98, Lecture Notes in Computer Science* **1462** (1998), Springer-Verlag, 26-45. Full version appears in http://www-cse.ucsd.edu/users/mihir/papers/crypto-papers.html

[BR95] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption – How to Encrypt with RSA," A. De Santis, editor, *Advances in Cryptology — EUROCRYPT '94, Lecture Notes in Computer Science* **950** (1995), Springer-Verlag, 92-111. Revised version appears in http://www-cse.ucsd.edu/users/mihir/papers/crypto-papers.html

[BR96] M. Bellare and P. Rogaway, "The Exact Security of Digital Signatures: How to Sign with RSA and Rabin," U. M. Maurer, editor, *Advances in Cryptology — EUROCRYPT '96, Lecture Notes in Computer Science* **1070** (1996), Springer-Verlag, 399-416. Revised version appears in http://www-cse.ucsd.edu/users/mihir/papers/crypto-papers.html

[Ber68] E. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, 1968, pp. 36-44.

[BJM97] S. Blake-Wilson, D. Johnson and A. Menezes, "Key Agreement Protocols and their Security Analysis," M. Darnell, editor, *Cryptography and Coding: Sixth IMA International Conference, Lecture Notes in Computer Science* **1355** (1997), Springer-Verlag, 30-45. A full version is available from http://www.cacr.math.uwaterloo.ca/.

[BM98] S. Blake-Wilson and A. Menezes, "Unknown key-share attacks on the station-to-station (STS) protocol," H. Imai and Y. Zheng, editors, *Public Key Cryptography: Second International Workshop on Practice and Theory in Public Key Cryptography, PKC'99, Lecture Notes in Computer Science* **1560** (1999), 154-170. Also available as technical report CORR 98-42 from http://www.cacr.math.uwaterloo.ca/

[Ble98] D. Bleichenbacher, "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1," H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98, Lecture Notes in Computer Science* **1462** (1998), Springer-Verlag, 1-12.

[BBS86] L. Blum, M. Blum and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing* **15** (1986), 364-383.

[BM84] M. Blum, S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits," *SIAM Journal on Computing* **13** (1984), 850-864.

[BDL97] D. Boneh, R. A. DeMillo and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," W. Fumy, editor, *Advances in Cryptology — EUROCRYPT '97, Lecture Notes in Computer Science* **1223** (1997), Springer-Verlag, 37-51.

[BD99] D. Boneh and G. Durfee, "Cryptoanalysis of RSA with private key d less than $N^{0.292}$," J. Stern, editor, *Advances in Cryptology — EUROCRYPT '99, Lecture Notes in Computer Science* **1592** (1999), Springer-Verlag, 1-11.

[BDF98] D. Boneh, G. Durfee, Y. Frankel, "An attack on RSA given a small fraction of the private key bits," *K. Ohta and D. Pei, editors, Advances in Cryptology – ASIACRYPT '98, Lecture Notes In Computer Science* **1514** (1998), Springer-Verlag, 25-34.

[BL96] D. Boneh and R. Lipton, "Algorithms for black box fields and their application to cryptography," N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science* **1109** (1996), Springer-Verlag, 283-297.

[BV98] D. Boneh, R. Venkatesan, "Breaking RSA May Not Be Equivalent to Factoring," K. Nyberg, editor, *Advances in Cryptology — EUROCRYPT '98, Lecture Notes in Computer Science* **1403** (1998), Springer-Verlag, 59-71.

[BLS88] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff, "Factorizations of $b^n \pm 1$, b = 2,3, 5,6,7,10,11,12, up to high powers," 2nd ed., American Math. Soc., 1988.

[BLZ94] J. Buchmann, J. Loho and J. Zayer, "An implementation of the general number field sieve," D. R. Stinson, editor, *Advances in Cryptology — CRYPTO '93, Lecture Notes in Computer Science* **773** (1994), Springer-Verlag, 159-165.

[Bue89] D. Buell, *Binary quadratic forms: classical theory and modern computations*, Springer-Verlag, 1989.

[BLP93] J.P. Buhler, H. W. Lenstra, Jr. and C. Pomerance, "Factoring integers with the number field sieve," A. K. Lenstra and H.W. Lenstra, Jr., editors, *The Development of the Number Field Sieve, Lecture Notes in Mathematics* **1554** (1993), Springer-Verlag, 50-94.

[Bur96] R. J. Burthe, Jr., "Further Investigations with the Strong Probable Prime Test," *Mathematics of Computation* **65** (1996), 373-381.

[CW98] Lidong Chen and Charles Williams, "Public Key Sterilization," unpublished draft, August 1998.

[CH98] M. Chen and E. Hughes, "Protocol Failures Related to Order of Encryption and Signature: Computation of Discrete Logarithms in RSA Groups," C. Boyd and E. Dawson, editors, *Third Australian Conference on Information Security and Privacy – ACISP '98, Lecture Notes in Computer Science* **1438** (1998).

[CC87] D.V. Chudnovsky and G.V. Chudnovsky, "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorizations Tests," *Advances in Applied Mathematics*, **7** (1987), 385-434.

[CFP96] D. Coppersmith, M. Franklin, J. Patarin and M. Reiter, "Low-exponent RSA with related messages," U. M. Maurer, editor, *Advances in Cryptology — EUROCRYPT '96, Lecture Notes in Computer Science* **1070** (1996), Springer-Verlag, 1-9.

[CHJ99] D. Coppersmith, S. Halevi and C. Jutla, "ISO 9796-1 and the new forgery strategy (working draft)." Presented at the rump session of *CRYPTO '99*. Available from `http://grouper.ieee.org/groups/1363/contrib.html`.

[CN98] J.-S. Coron and D. Naccache, "An Accurate Evaluation of Maurer's Universal Test," *Selected Areas in Cryptography – SAC '98, Lecture Notes in Computer Science* (1998), Springer-Verlag.

[CNS99] J.-S. Coron, D. Naccache, and J.P. Stern, "On the security of RSA padding," M. J. Wiener, editor, *Advances in Cryptology — CRYPTO '99, Lecture Notes in Computer Science* **1666** (1999), Springer-Verlag, 1-18.

[DLP93] I. Damgard, P. Landrock, and C. Pomerance, "Average Case Error Estimates for the Strong Probable Prime Test," *Mathematics of Computation* **61** (1993), 177-194.

[DIF94] D. Davis, R. Ihaka, and P. Fenstermacher,"Cryptographic randomness from air turbulence in disk drives," Yvo G. Desmedt, editor, *Advances in Cryptology — CRYPTO '94, Lecture Notes in Computer Science* **839** (1994), Springer-Verlag, 114-120.

[DKL98] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater and J.-L. Willems, "A Practical Implementation of the Timing Attack," *CARDIS '98, Lecture Notes in Computer Science,* Springer Verlag, 1998.

[Dif88] W. Diffie, "The first ten years of public-key cryptology," *Proceedings of the IEEE* **76** (1988), 560-577.

[DH76] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory* **22** (1976), 644-654.

[DOW92] W. Diffie, P. C. van Oorschot and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography* **2** (1992), 107-125

[DBP96] H. Dobbertin, A. Bosselaers and B. Preneel, "RIPEMD-160: a strengthened version of RIPEMD," D. Gollmann, editor, *Fast Software Encryption, Third International Workshop, Lecture Notes in Computer Science* **1039** (1996), Springer-Verlag, 71-82. A corrected and updated version is available from `http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html` .

[DL95] B. Dodson and A. K. Lenstra, "NFS with Four Large Primes: An Explosive Experiment," D. Coppersmith, editor, *Advances in Cryptology — CRYPTO '95, Lecture Notes in Computer Science* **963** (1995), Springer-Verlag, 372-385.

[DHR98a] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade and L. Repka, "RFC2311: S/MIME Version 2 Message Specification," Internet Activities Board, March 1998. Available from `http://www.rfc-editor.org/`. See also `http://www.ietf.org/html.charters/smime-charter.html` and `http://www.ietf.org/ids.by.wg/smime.html` for latest developments and drafts.

[DHR98b] S. Dusse, P. Hoffman, B. Ramsdell and J. Weinstein, "RFC2312: S/MIME Version 2 Certificate Handling," Internet Activities Board, March 1998. Available from `http://www.rfc-editor.org/`. See also `http://www.ietf.org/html.charters/smime-charter.html` and `http://www.ietf.org/ids.by.wg/smime.html` for latest developments and drafts.

[ECS94] D. Eastlake, S. Crocker, and J. Schiller. "RFC1750: Randomness Recommendations for Security," Internet Activities Board, December 1994. Available from `http://www.rfc-editor.org/`.

[FIP94a] FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-1, U.S. Department of Commerce/National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia, April 11, 1994 (supersedes FIPS PUB 140). Available at `http://www.itl.nist.gov/div897/pubs/fip140-1.htm`.

[FIP95] FIPS PUB 180-1, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/National Institute of Standards and Technology, National

Technical Information Service, Springfield, Virginia, April 17, 1995 (supersedes FIPS PUB 180). Available at http://www.itl.nist.gov/div897/pubs/fip180-1.htm.

[FIP94b] FIPS PUB 186, *Digital Signature Standard*, Federal Information Processing Standards Publication 186, U.S. Department of Commerce/National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia, 1994. Available at http://www.itl.nist.gov/div897/pubs/fip186.htm.

[GLV98] R. Gallant, R. Lambert and S. Vanstone, "Improving the parallelized Pollard lambda search on binary anomalous curves," *Mathematics of Computation*, to appear.

[GMR98] R. Gennaro, D. Micciancio and T. Rabin, "An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products," *Proceedings of the Fifth ACM Conference on Computer and Communications Security (CCS-5)*, 1998, pp. 67-72. Available from http://www.acm.org/pubs/articles/proceedings/commsec/288090/p67-gennaro/p67-gennaro.pdf

[GGO98] H. Gilbert, D. Gupta, A. Odlyzko and J.-J. Quisquater, "Attacks on Shamir's 'RSA for Paranoids,'" *Information Processing Letters* vol.68 no.4 (November 30, 1998), pp.197-199. Also available from http://www.research.att.com/~amo/doc/crypto.html

[GK86] S. Goldwasser and J. Kilian, "Almost all primes can be quickly certified," *Proceedings of the 18th Annual ACM Symposium on Theory of Computing* (1986), 316-329.

[GM84] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences* **28** (1984), 270-299.

[GMR88] S. Goldwasser, S. Micali and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing* **17** (1988), 281-308.

[Gor93a] D. M. Gordon, "Designing and detecting trapdoors for discrete log cryptosystems," E. F. Brickell, editor, *Advances in Cryptology — CRYPTO '92, Lecture Notes in Computer Science* **740** (1993), Springer-Verlag, 66-75.

[Gor93b] D. M. Gordon, "Discrete logarithms in *GF* (*p*) using the number field sieve," *SIAM Journal on Discrete Mathematics*, **6** (1993), 124-138.

[Gor98] D. M. Gordon, "A survey of fast exponentiation methods," *Journal of Algorithms* **27** (1998), 129-146.

[GM93] D. M. Gordon and K. S. McCurley, "Massively parallel computations of discrete logarithms," E. F. Brickell, editor, *Advances in Cryptology — CRYPTO '92, Lecture Notes in Computer Science* **740** (1993), Springer-Verlag, 312-323.

[Gos90] K. C. Goss, "Cryptographic method and apparatus for public key exchange with authentications," U. S. Patent 4,956,863, 11 Sep 1990.

[GQW91] C. Guillou, J.-J. Quisquater, M. Walker, P. Landrock and C. Shaer, "Precautions taken against various potential attacks in ISO/IEC DIS 9796," I.B. Damgard, editor, *Advances in Cryptology — EUROCRYPT '90, Lecture Notes in Computer Science* **473** (1991), Springer-Verlag, 465-473.

[Gun90] C. G. Gunther, "An identity-based key-exchange protocol," J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89, Lecture Notes in Computer Science* **434** (1990), Springer-Verlag, 29-37.

[HM95] Katie Hafner and John Markoff, *Cyberpunk: Outlaws and hackers on the computer frontier*, updated edition, Touchstone Books, 1995.

[Has88] J. Hastad, "Solving simultaneous modular equations of low degree," *SIAM Journal on Computing* **17** (1988), 336-341.

[ISO98a] ISO/IEC 8824-1:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation. Equivalent to ITU-T Rec. X.680 (1997).

[ISO98b] ISO/IEC 8824-2:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Information Object Specification. Equivalent to ITU-T Rec. X.681 (1997)

[ISO98c] ISO/IEC 8824-3:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Constraint Specification. Equivalent to ITU-T Rec. X.682 (1997).

[ISO98d] ISO/IEC 8824-4:1998, Information Technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications. Equivalent to ITU-T Rec. X.683 (1997).

[ISO98e] ISO/IEC 8825-1:1998, Information Technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Equivalent to ITU-T Rec. X.690 (1997).

[ISO98f] ISO/IEC 8825-2:1998, Information Technology – ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER). Equivalent to ITU-T Rec. X.691 (1997).

[ISO91] ISO/IEC 9796:1991 Information Technology – Security techniques – Digital signature scheme giving message recovery.

[ISO98g] ISO/IEC 9796-4 Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 4: Methods based on the Discrete Logarithm, draft, 1998.

[ISO98h] ISO/IEC DIS 14888-3 Information technology – Security techniques – Digital signature with appendix – Part 3: Certificate-based mechanisms, Draft International Standard, 1998.

[ITT86] T. Itoh, O. Teechai and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in *GF* (2^l) using normal bases," *J. Society for Electronic Communications (Japan)* **44** (1986), 31-36.

[ITU97] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, International Telecommunications Union, June 1997.

[JQ99] M. Joye and J.-J. Quisquater, "On Rabin-type signatures (working draft)." Presented at the rump session of *CRYPTO '99*. Available from `http://grouper.ieee.org/groups/1363/contrib.html`.

[Joh] D. B. Johnson, unpublished communication to ANSI X9F1 and IEEE P1363 working groups.

[JM96] D. B. Johnson and S. M. Matyas, "Asymmetric encryption: Evolution and enhancements," *CryptoBytes* vol. 2 no. 1 (Spring 1996), RSA Laboratories, ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf

[JQ96] M. Joye and J.J. Quisquater, "Efficient computation of full Lucas sequences," Electronics Letters vol. 32 (1996), pp. 537-538. Corrected version available at http://www.dice.ucl.ac.be/crypto/publications.html

[Kal98a] B. S. Kaliski, Jr., "Compatible cofactor multiplication for Diffie-Hellman primitives," Electronics Letters vol. 34 no. 25 (December 10, 1998), pp. 2396-2397.

[Kal98b] B. S. Kaliski, Jr., "MQV vulnerability," Internet communication to ANSI X9F1 and IEEE P1363 mailing lists, June 17, 1998.

[Keh95] Brendan P. Kehoe, *Zen and the Art of the Internet : A Beginner's Guide*, fourth edition, Prentice Hall Computer Books, 1995.

[KSW98] J. Kelsey, B. Schneier, D. Wagner and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," S. Vaudenay, editor, *Fast Software Encryption, Fifth International Workshop Proceedings, Lecture Notes in Computer Science* **1372** (1998), Springer-Verlag, 168-188.

[Ker83] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, 9th Series (February 1883), 161-191.

[Knu81] D. E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, 2nd edition, Addison-Wesley, 1981, p. 379.

[Kob87] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation* **48** (1987), 203-209.

[Kob94] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, 1994.

[Koc96] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science* **1109** (1996), Springer-Verlag, 104-113.

[Kra93] D. W. Kravitz, "Digital signature algorithm," U.S. Patent 5,231,668, 27 Jul 1993.

[LMQ98] L. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone, "An Efficent Protocol for Authenticated Key Agreement," Technical Report CORR 98-05, Dept. of C&O, University of Waterloo, Canada, March 1998 (revised August 28, 1998). Available from http://www.cacr.math.uwaterloo.ca/.

[LZ94] G. Lay and H. Zimmer, "Constructing elliptic curves with given group order over large finite fields," *Algorithmic Number Theory: First International Symposium, Lecture Notes in Computer Science* **877** (1994), Springer-Verlag, 250-263.

[Leh69] D. H. Lehmer, "Computer Technology Applied to the Theory of Numbers," *Studies in Number Theory* (W. J. LeVeque, ed.), Mathematical Association of America, 1969.

[Len87] H. W. Lenstra, Jr., "Factoring integers with elliptic curves," *Annals of Mathematics* **126** (1987), 649-673.

[LL97] C. H. Lim and P. J. Lee, "A key recovery attack on discrete log-based schemes using a prime order subgroup," B. S. Kaliski, Jr., editor, *Advances in Cryptology — CRYPTO '97*, *Lecture Notes in Computer Science* **1294** (1997), Springer-Verlag, 249-263.

[LS98] M. Liskov and R. D. Silverman, "A Statistical Limited-Knowledge Proof for Secure RSA Keys," submitted to *Journal of Cryptology*, 1998.

[MV97] MasterCard International, Inc. and Visa International Service Association, *SET Secure Electronic Transaction Specification*, May 31, 1997. Available from `http://www.setco.org/`.

[MTI86] T. Matsumoto, Y. Takashima and H. Imai, "On seeking smart public-key-distribution systems," *The Transactions of the IECE of Japan* **E69** (1986), 99-106.

[Mau91] U. M. Maurer, "A universal statistical test for random bit generators," A.J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology — CRYPTO '90*, *Lecture Notes in Computer Science* **537** (1991), Springer-Verlag, 409-420.

[Mau95] U. M. Maurer, "Fast generation of prime numbers and secure public-key cryptographic parameters," *Journal of Cryptology* **8** (1995), 123-155.

[Men93a] A. Menezes, editor, *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.

[Men93b] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[Men95] A. Menezes, "Elliptic Curve Cryptosystems," *CryptoBytes* vol. 1 no. 2 (Summer 1995), RSA Laboratories, `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`

[MOV93] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory* **39** (1993), 1639-1646.

[MOV96] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1996.

[MQV95] A. Menezes, M. Qu and S. Vanstone, "Some new key agreement protocols providing implicit authentication," workshop record, 2nd Workshop on Selected Areas in Cryptography (SAC'95), Ottawa, Canada, May 18-19, 1995, 22-32.

[MRS88] S. Micali, C. Rackoff and B. Sloan, "The notion of security for probabilistic cryptosystems," *SIAM Journal on Computing* **17** (1988), 412-426.

[MS91] S. Micali and C. P. Schnorr, "Efficient, perfect polynomial random number generators," *Journal of Cryptology* **3** (1991), 157-172.

[Mih94] P. Mihailescu, "Fast generation of provable primes using search in arithmetic progressions," Yvo G. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, *Lecture Notes in Computer Science* **839** (1994), Springer-Verlag, 282-293.

[Mil86] V. S. Miller, "Use of elliptic curves in cryptography," H. C. Williams, editor, *Advances in Cryptology – Crypto '85*, *Lecture Notes in Computer Science* **218** (1986), Springer-Verlag, 417-426.

[Mor91] F. Morain, "Building cyclic elliptic curves modulo large primes," D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science* **547** (1991), Springer-Verlag, 328-336.

[NIS99] National Institute of Standards and Technology. "Recommended elliptic curves for federal government use," draft, 1999. Available from `http://csrc.nist.gov/encryption/`.

[NR93] K. Nyberg and R. Rueppel, "A new signature scheme based on the DSA giving message recovery," *First ACM Conference on Computer and Communcations Security* (1993), ACM Press, 58-61.

[Odl95] A. M. Odlyzko, "The Future of Integer Factorization," *CryptoBytes* vol. 1 no. 2 (Summer 1995), RSA Laboratories, `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf`

[OW94] P. van Oorschot and M. Wiener, "Parallel collision search with applications to hash functions and discrete logarithms," *2nd ACM Conference on Computer and Communications Security* (1994), ACM Press, 210-218.

[Pol74] J. M. Pollard, "Theorems on factorization and primality testing," *Proceedings of the Cambridge Philosphical Society* **76** (1974), 521-528.

[Pol75] J. M. Pollard, "A Monte Carlo method for factorization," *BIT* **15** (1975), 331-334.

[Pol78] J. M. Pollard, "Monte Carlo methods for index computation (mod *p*)," *Mathematics of Computation* **32** (1978), 918-924.

[PKC93] Public Key Cryptography Standards (PKCS). PKCS #1 v1.5: RSA Encryption Standard. November 1, 1993. Available from `http://www.rsa.com/rsalabs/pubs/PKCS/`.

[PKC98] Public Key Cryptography Standards (PKCS). PKCS #1 v2.0: RSA Cryptography Standard. 1998. Available from `http://www.rsa.com/rsalabs/pubs/PKCS/`.

[Rab79] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Massachusetts Institute of Technology Laboratory for Computer Science Technical Report 212 (MIT/LCS/TR-212), 1979.

[RSA78] R. L. Rivest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM* **21** (1978), 120-126.

[SA98] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," *Commentarii Mathematici Universitatis Sancti Pauli* **47** (1998), 81-92. Errata: ibid. 48(1999), 211-213.

[Sch93] O. Schirokauer, "Discrete logarithms and local units," *Philosophical transactions of the Royal Society of London A*, **345** (1993), 409-423.

[Sch95] B. Schneier, *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, Second Edition, John Wiley and Sons, 1995.

[SOM95] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck. "Fast key exchange with elliptic curve systems," *Univ. of Arizona Comp. Sci. Tech. Report 95-03* (1995). A version also appears in D. Coppersmith, editor, *Advances in Cryptology — CRYPTO '95, Lecture Notes in Computer Science* **963** (1995), Springer-Verlag, 43-56.

[Ser98] G. Seroussi, "Compact representation of elliptic curve points over F_2^n." Research Manuscript, Hewlett-Packard Laboratories, April 1998.

[Sha95] A. Shamir, "RSA for Paranoids," *CryptoBytes* vol. 1 no. 3 (Autumn 1995), RSA Laboratories, `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf`.

[Sha86] J. Shawe-Taylor, "Generating strong primes," *Electronics Letters* **22** (July 31, 1986), 875-877.

[Sil87] R. D. Silverman, "The multiple polynomial quadratic sieve," *Mathematics of Computation* **48** (1987), 329-339.

[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[Sma99] N. P. Smart, "Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic," *J. Cryptology* vol. 12. (1999), pp. 141-151.

[SAK98] D. Solo, C. Adams, D. Kemp and M. Myers, "Internet X.509 Certificate Request Message Format," Internet Engineering Task Force (IETF), PKIX working group, work in progress. Available at `http://www.ietf.org/ids.by.wg/pkix.html`.

[SHW98] D. Solo, R. Housley, W. Ford and T. Polk, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Engineering Task Force (IETF), PKIX working group, work in progress. Available at `http://www.ietf.org/ids.by.wg/pkix.html`.

[Sta98] William Stallings, *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice-Hall, 1998.

[SEC99] Standards for Efficient Cryptography. "GEC1: Recommended Elliptic Curve Domain Parameters," draft, September 1999. Available from `http://www.secg.org/drafts.htm`.

[Sti95] Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

[Vau96] S. Vaudenay, "Hidden collisions on DSS," N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, *Lecture Notes in Computer Science* **1109** (1996), Springer-Verlag, 83-88.

[Wie90] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory* **36** (1990), 553-558

[WZ98] M. J. Wiener and R. Zuccherato, "Faster Attacks on Elliptic Curve Cryptosystems," S. Tavares and H. Meijer, editors, *Selected Areas in Cryptography – SAC '98*, *Lecture Notes in Computer Science* (1998), Springer-Verlag.

[Wil80] H. C. Williams, "A modification on the RSA public-key encryption procedure," *IEEE Transactions of Information Theory* **26** (1980), 726-729.

[Wil82] H. C. Williams, "A p + 1 method of factoring," *Mathematics of Computation* **39** (1982), 225-234.

[Yao82] A. C. Yao, "Theory and applications of trapdoor functions," *Proccedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science (FOCS '92)*, 1992, 80-91.