List of Notation

$\mathbb{Z}$	the integers $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$, 10
$b \mid a$	b divides a (integers), 10
$b \nmid a$	b does not divide a (integers), 10
gcd	greatest common divisor, 11
$a \equiv b \pmod{m}$	a and b are congruent modulo m, 19
$\mathbb{Z}/m\mathbb{Z}$	the ring of integers modulo m, 21
$(\mathbb{Z}/m\mathbb{Z})^*$	the group of units in $\mathbb{Z}/m\mathbb{Z}$, 22
$\mathrm{ord}_p(a)$	order (or exponent) of p in a, 28
$a^{-1} \bmod p$	the multiplicative inverse of a modulo p, 28
$\mathbb{R}$	the field of real numbers, 29
$\mathbb{Q}$	the field of rational numbers, 29
$\mathbb{C}$	the field of complex numbers, 29
$\mathbb{F}_p$	the finite field $\mathbb{Z}/p\mathbb{Z}$, 29
$\mathcal{K}$	space of keys, 37
$\mathcal{M}$	space of messages (plaintexts), 37
$\mathcal{C}$	space of ciphertexts, 37
e or e_k	encryption function, 37
d or d_k	decryption function, 37
$\oplus$	exclusive or (XOR), 43
$\lfloor x \rfloor$	the greatest integer in x, 53
$\log_g(h)$	the discrete logarithm of h to the base g, 65
$\star$	composition operation in a group, 74
$\lvert G \rvert$	the order of the group G, 74
$\#G$	the order of the group G, 74
GL_n	the general linear group, 75
g^x	exponentiation of g in a group G, 75
$\mathcal{O}\big(g(x)\big)$	big-$\mathcal{O}$ notation, 78
$\star$	multiplication in a ring, 95
$\mathbb{Z}[x]$	ring of polynomials with integer coefficients, 96
$b \mid a$	b divides a (in a ring), 96
$b \nmid a$	b does not divide a (in a ring), 96
$a \equiv b \pmod{m}$	a and b are congruent modulo m (in a ring), 97
R/mR	quotient ring of R by m, 98
$R/(m)$	quotient ring of R by m, 98
$R[x]$	ring of polynomials with coefficients in R, 98

J. Hoffstein et al., *An Introduction to Mathematical Cryptography*,
Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4939-1711-2

$\deg$	degree of a polynomial, 98
$\mathbb{F}_{p^d}$	a finite field with p^d elements, 106
$\mathrm{GF}(p^d)$	a field with p^d elements, 106
$\pi(X)$	number of primes between 2 and X, 133
$\zeta(s)$	Riemann zeta function, 135
$\psi(X, B)$	Number of B-smooth integers between 2 an X, 150
$o\big(g(x)\big)$	little-o notation, 151
$L(X)$	the function $e^{\sqrt{(\ln X)(\ln\ln X)}}$, 151
$\Omega\big(g(x)\big)$	big-Ω notation, 152
$\Theta\big(g(x)\big)$	big-Θ notation, 152
$f(X) \ll g(X)$	alternative for $f(X) = \mathcal{O}\big(g(X)\big)$, 152
$f(X) \gg g(X)$	alternative for $f(X) = \Omega\big(g(X)\big)$, 152
$f(X) \gg\ll g(X)$	alternative for $f(X) = \Theta\big(g(X)\big)$, 152
$\mathbb{Z}[\beta]$	the ring generated by the complex number β, 162
$L_\epsilon(X)$	the function $e^{(\ln X)^\epsilon (\ln\ln X)^{1-\epsilon}}$, 165
$\left(\frac{a}{p}\right)$	the Legendre symbol of a modulo p, 171
$\mathrm{Li}(X)$	the logarithmic integral function, 186
K^{Pri}	private signing key, 194
K^{Pub}	public verification key, 194
Sign	signing algorithm, 194
Verify	verification algorithm, 194
$\binom{n}{r}$	combinatorial symbol n choose r, 212
$\mathrm{IndCo}(\boldsymbol{s}, \boldsymbol{t})$	index of coincidence of $\boldsymbol{s}$, 219
$\mathrm{MutIndCo}(\boldsymbol{s}, \boldsymbol{t})$	mutual index of coincidence of $\boldsymbol{s}$ and $\boldsymbol{t}$, 221
$\Pr$	a probability function, 229
$\Pr(F \mid E)$	conditional probability of F on E, 234
$f_X(x)$	probability density function of X, 239
$F_X(x)$	probability distribution function of X, 239
$f_{X,Y}(x, y)$	joint density function of X and Y, 241
$f_{X,Y}(x \mid y)$	conditional density function of X and Y, 241
$O_f^+(x)$	orbit of x under iteration of f, 254
$H(X)$	the entropy of the random variable X, 270
$\oplus$	addition on an elliptic curve, 302
$\mathcal{O}$	point at infinity on elliptic curve, 305
Δ_E	discriminant of the elliptic curve E, 306
$E(\mathbb{F}_p)$	points of elliptic curve with coordinates in $\mathbb{F}_p$, 308
$\log_P(Q)$	the elliptic discrete logarithm of Q with respect to P, 313
τ	the p-power Frobenius map $\mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, 334
τ	the p-power Frobenius map on an elliptic curve $E(\mathbb{F}_{p^k})$, 334
$E[m]$	points of order m on an elliptic curve E, 339
$\deg(D)$	degree of the divisor D, 341
$\mathrm{Sum}(D)$	sum of points in the divisor D, 341
e_m	the Weil pairing on an elliptic curve, 342
$\tau(P, Q)$	Tate pairing on an elliptic curve, 348
$\hat{\tau}(P, Q)$	modified Tate pairing on an elliptic curve, 348
$\hat{e}_\ell$	modified Weil pairing on an elliptic curve, 354
$\boldsymbol{a} \cdot \boldsymbol{b}$	dot product of $\boldsymbol{a}$ and $\boldsymbol{b}$, 385
$\|\boldsymbol{a}\|$	Euclidean norm of $\boldsymbol{a}$, 385

$\mathrm{GL}_n(\mathbb{Z})$	the special linear group (over $\mathbb{Z}$), 390
$\det(L)$	the determinant (covolume) of the lattice L, 392
γ_n	Hermite constant, 397
$\mathcal{H}(\mathcal{B})$	the Hadamard ratio of the basis $\mathcal{B}$, 397
$\mathbb{B}_R(\boldsymbol{a})$	closed ball of radius R centered at $\boldsymbol{a}$, 397
$\Gamma(s)$	the gamma function, 400
$\sigma(L)$	Gaussian expected shortest length of a vector in L, 402
R	the convolution polynomial ring $\mathbb{Z}[x]/(x^N-1)$, 412
R_q	the convolution polynomial ring $(\mathbb{Z}/q\mathbb{Z})[x]/(x^N-1)$, 412
$\boldsymbol{a} \star \boldsymbol{b}$	multiplication in convolution polynomial ring, 413
$\star$	convolution product of vectors, 414
$\mathcal{T}(d_1, d_2)$	ternary polynomial, 417
$L_{\boldsymbol{h}}^{\mathrm{NTRU}}$	the NTRU lattice associated to $\boldsymbol{h}(x)$, 425
$M_{\boldsymbol{h}}^{\mathrm{NTRU}}$	matrix for the NTRU lattice associated to $\boldsymbol{h}(x)$, 425
$\|\boldsymbol{a}\|_\infty$	sup norm of $\boldsymbol{a}$, 434
$\mathcal{B}^*$	Gram–Schmidt orthogonal basis associated to $\mathcal{B}$, 439
$W^\perp$	the orthogonal complement of W, 440
Hash	a hash function, 472
$\mathrm{Div}(C)$	group of divisors on a curve, 495
$\mathrm{Div}_0(C)$	group of divisors of degree 0 on a curve, 495
$\mathrm{Jac}_0(C)$	the Jacobian variety of the curve C, 495
$J(\mathbb{F}_p)$	the group of points modulo p on the Jacobian $\mathrm{Jac}_0(C)$, 495
$\|0\rangle$	ket notation in quantum mechanics, 497

References

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P. Ann. Math. (2) **160**(2), 781–793 (2004)

[2] L.V. Ahlfors, *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable*. International Series in Pure and Applied Mathematics, 3rd edn. (McGraw-Hill, New York, 1978)

[3] M. Ajtai, The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract), in *STOC '98: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, Dallas (ACM, New York, 1998), pp. 10–19

[4] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in *STOC '97*, El Paso (ACM, New York, 1999), pp. 284–293 (electronic)

[5] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers. Ann. Math. (2) **139**(3), 703–722 (1994)

[6] ANSI-ECDSA, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA). ANSI Report X9.62, American National Standards Institute, 1998

[7] T.M. Apostol, *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics (Springer, New York, 1976)

[8] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986)

[9] E. Bach, Explicit bounds for primality testing and related problems. Math. Comput. **55**(191), 355–380 (1990)

[10] E. Bach, J. Shallit, *Algorithmic Number Theory: Efficient Algorithms*. Foundations of Computing Series, vol. 1 (MIT, Cambridge, 1996).

[11] M. Bellare, Practice oriented provable-security, in *Proceedings of the First International Workshop on Information Security—ISW '97*, Tatsunokuchi. Volume of 1396 Lecture Notes in Computer Science (Springer, Berlin, 1998)

[12] M. Bellare, P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols, in *Proceedings of the First Annual Conference on Computer and Communications Security*, Fairfax, 1993, pp. 62–73

J. Hoffstein et al., *An Introduction to Mathematical Cryptography*,
Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4939-1711-2

[13] M. Bellare, P. Rogaway, Optimal asymmetric encryption, in *Advances in Cryptology—EUROCRYPT '94*, Perugia. Volume 950 of Lecture Notes in Computer Science (Springer, Berlin, 1995), pp. 92–111

[14] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography. Volume 265 of London Mathematical Society Lecture Note Series (Cambridge University Press, Cambridge, 2000)

[15] G. Blakley, Safeguarding cryptographic keys, in *Proceedings of AFIPS National Computer Conference*, Zurich, vol. 48, 1979, pp. 313–317

[16] D. Bleichenbacher, Chosen ciphertext attacks against protocols based on RSA encryption standard PKCS #1, in *Advances in Cryptology—CRYPTO 1998*, Santa Barbara. Volume 1462 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 1–12

[17] J. Blömer, A. May, Low secret exponent RSA revisited, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 4–19

[18] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, in *Advances in Cryptology—EUROCRYPT '99*, Prague. Volume 1592 of Lecture Notes in Computer Science (Springer, Berlin, 1999), pp. 1–11

[19] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans. Inf. Theory **46**(4), 1339–1349 (2000)

[20] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Advances in Cryptology—CRYPTO 2001*, Santa Barbara. Volume 2139 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 213–229

[21] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing. SIAM J. Comput. **32**(3), 586–615 (electronic) (2003)

[22] D. Boneh, R. Venkatesan, Breaking RSA may not be equivalent to factoring (extended abstract), in *Advances in Cryptology—EUROCRYPT '98*, Espoo. Volume 1403 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 59–71

[23] R.P. Brent, An improved Monte Carlo factorization algorithm. BIT **20**(2), 176–184 (1980)

[24] E.R. Canfield, P. Erdős, C. Pomerance, On a problem of Oppenheim concerning "factorisatio numerorum". J. Number Theory **17**(1), 1–28 (1983)

[25] J.W.S. Cassels, *Lectures on Elliptic Curves*. Volume 24 of London Mathematical Society Student Texts (Cambridge University Press, Cambridge, 1991)

[26] D. Chaum, Blind signatures for untraceable payments, in *Advances in Cryptology—CRYPTO '82*, Santa Barbara. Lecture Notes in Computer Science (Plenum Press, New York/London, 1983), pp. 199–203

[27] D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, in *Advances in Cryptology—CRYPTO 1988*, Santa Barbara. Volume 403 of Lecture Notes in Computer Science (Springer, 1988), pp. 319–327

[28] H. Cohen, *A Course in Computational Algebraic Number Theory*. Volume 138 of Graduate Texts in Mathematics (Springer, Berlin, 1993)

[29] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications (Boca Raton) (Chapman & Hall/CRC, Boca Raton, 2006)

[30] S.A. Cook, The complexity of theorem-proving procedures, in *STOC '71: Proceedings of the Third Annual ACM Symposium on Theory of Computing*, Shaker Heights (ACM, New York, 1971), pp. 151–158

[31] D. Coppersmith, Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. Math. Comput. **62**(205), 333–350 (1994)

[32] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. **10**(4), 233–260 (1997)

[33] D. Coppersmith, Finding small solutions to small degree polynomials, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 20–31

[34] R. Crandall, C. Pomerance, *Prime Numbers* (Springer, New York, 2001)

[35] H. Davenport, *The Higher Arithmetic* (Cambridge University Press, Cambridge, 1999)

[36] M. Dietzfelbinger, *Primality Testing in Polynomial Time: From Randomized Algorithms to "PRIMES is in P"*. Volume 3000 of Lecture Notes in Computer Science (Springer, Berlin, 2004)

[37] W. Diffie, The first ten years of public key cryptology, G.J. Simmons (ed.), in *Contemporary Cryptology* (IEEE, New York, 1992), pp. 135–175

[38] W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory IT-**22**(6), 644–654 (1976)

[39] L. Ducas, P.Q. Nguyen, Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures, in *Advances in Cryptology—ASIACRYPT 2012*, Beijing. Volume 7658 of Lecture Notes in Computer Science (Springer, Berlin, 2012), pp. 433–450

[40] D.S. Dummit, R.M. Foote, *Abstract Algebra*, 3rd edn. (Wiley, Hoboken, 2004)

[41] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)

[42] J. Ellis, The story of non-secret encryption, 1987 (released by CSEG in 1997). https://cryptocellar.web.cern.ch/cryptocellar/cesg/ellis.pdf

[43] W. Fleming, *Functions of Several Variables*. Undergraduate Texts in Mathematics, 2nd edn. (Springer, New York, 1977)

[44] M. Fouquet, P. Gaudry, R. Harley, An extension of Satoh's algorithm and its implementation. J. Ramanujan Math. Soc. **15**(4), 281–318 (2000)

[45] J. Fraleigh, *A First Course in Abstract Algebra*, 7th edn. (Addison Welsley, Boston/London, 2002)

[46] M.R. Garey, D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. A Series of Books in the Mathematical Sciences (W. H. Freeman, San Francisco, 1979)

[47] C. Gentry, *A Fully Homomorphic Encryption Scheme*, PhD thesis, Stanford University, 2009. crypto.stanford.edu/craig

[48] C. Gentry, Fully homomorphic encryption using ideal lattices, in *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, Bethesda (ACM, New York, 2009), pp. 169–178

[49] O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, in *Advances in Cryptology—CRYPTO '97*, Santa Barbara, 1997. Volume 1294 of Lecture Notes in Computer Science (Springer, Berlin, 1997), pp. 112–131

[50] O. Goldreich, D. Micciancio, S. Safra, J.-P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. Inf. Process. Lett. **71**(2), 55–61 (1999)

[51] G.R. Grimmett, D.R. Stirzaker, *Probability and Random Processes*, 3rd edn. (Oxford University Press, New York, 2001)

[52] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edn. (The Clarendon Press/Oxford University Press, New York, 1979)

[53] I.N. Herstein, *Topics in Algebra*, 2nd edn. (Xerox College Publishing, Lexington, 1975)

[54] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a ring-based public key cryptosystem, in *Algorithmic Number Theory*, Portland, 1998. Volume 1423 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 267–288

[55] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, W. Whyte, NTRUSign: digital signatures using the NTRU lattice, in *Topics in Cryptology—CT-RSA 2003*. Volume 2612 of Lecture Notes in Computer Science (Springer, Berlin, 2003), pp. 122–140. https://www.securityinnovation.com/uploads/Crypto/NTRUSign-preV2.pdf

[56] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, W. Whyte, Performance improvements and a baseline parameter generation algorithm for NTRUSign. Presented at Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, 2005. https://www.securityinnovation.com/uploads/Crypto/NTRUSignParams-2005-08.pdf

[57] J. Hoffstein, J. Pipher, J. Schanck, J. Silverman, W. Whyte, Transcript secure signatures based on modular lattices. Cryptology ePrint archive, report 2014/457, 2014. http://eprint.iacr.org/2014/457

[58] N. Howgrave-Graham, Approximate integer common divisors, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 51–66

[59] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Volume 84 of Graduate Texts in Mathematics (Springer, New York, 1990)

[60] E.T. Jaynes, Information theory and statistical mechanics. Phys. Rev. (2) **106**, 620–630 (1957)

[61] A. Joux, A one round protocol for tripartite Diffie-Hellman, in *Algorithmic Number Theory*, Leiden, 2000. Volume 1838 of Lecture Notes in Computer Science (Springer, Berlin, 2000), pp. 385–393

[62] A. Joux, A one round protocol for tripartite Diffie-Hellman. J. Cryptol. **17**(4), 263–276 (2004)

[63] D. Kahn, *The Codebreakers: The Story of Secret Writing* (Scribner Book, New York, 1996)

[64] P. Kaye, R. Laflamme, M. Mosca, *An Introduction to Quantum Computing* (Oxford University Press, Oxford, 2007)

[65] A.W. Knapp, *Elliptic Curves*. Volume 40 of Mathematical Notes (Princeton University Press, Princeton, 1992)

[66] D. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2nd edn. (Addison-Wesley, Reading, 1981)

[67] N. Koblitz, Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)

[68] N. Koblitz, *Algebraic Aspects of Cryptography*. Volume 3 of Algorithms and Computation in Mathematics (Springer, Berlin, 1998)

[69] N. Koblitz, The uneasy relationship between mathematics and cryptography. Not. Am. Math. Soc. **54**, 972–979 (2007)

[70] N. Koblitz, A.J. Menezes, Another look at "provable security". J. Cryptol. **20**(1), 3–37 (2007)

[71] J.C. Lagarias, H.W. Lenstra Jr., C.-P. Schnorr, Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica **10**(4), 333–348 (1990)

[72] B.A. LaMacchia, A.M. Odlyzko, Solving large sparse linear systems over finite fields, in *Advances in Cryptology—CRYPTO '90*, Santa Barbara, 1990. Lecture Notes in Computer Science (Springer, Berlin, 1990)

[73] S. Lang, *Elliptic Curves: Diophantine Analysis*. Volume 231 of Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences) (Springer, Berlin, 1978)

[74] S. Lang, *Elliptic Functions*. Volume 112 of Graduate Texts in Mathematics, 2nd edn. (Springer, New York, 1987). With an appendix by J. Tate

[75] H.W. Lenstra Jr., Factoring integers with elliptic curves. Ann. Math. (2) **126**(3), 649–673 (1987)

[76] H.W. Lenstra jr., C. Pomerance, Primality testing with Gaussian periods (2011). https://www.math.dartmouth.edu/~carlp/PDF/complexity12.pdf

[77] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)

[78] V. Lyubashevsky, Lattice-based identification schemes secure under active attacks, in *Public Key Cryptography—PKC 2008*, Barcelona. Volume 4939 of Lecture Notes in Computer Science (Springer, Berlin, 2008), pp. 162–179

[79] V. Lyubashevsky, Fiat-Shamir with aborts: applications to lattice and factoring-based signatures, in *Advances in Cryptology—ASIACRYPT 2009*, Tokyo. Volume 5912 of Lecture Notes in Computer Science (Springer, Berlin, 2009), pp. 598–616

[80] V. Lyubashevsky, Lattice signatures without trapdoors, in *Advances in Cryptology—EUROCRYPT 2012*, Cambridge. Volume 7237 of Lecture Notes in Computer Science (Springer, Heidelberg, 2012), pp. 738–755

[81] A. Menezes, *Elliptic Curve Public Key Cryptosystems*. The Kluwer International Series in Engineering and Computer Science, 234 (Kluwer Academic, Boston, 1993)

[82] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**(5), 1639–1646 (1993)

[83] R.C. Merkle, Secure communications over insecure channels, in *Secure Communications and Asymmetric Cryptosystems*, ed. by G.J. Simmons. Volume 69 of AAAS Selected Symposium Series (Westview, Boulder, 1982), pp. 181–196

[84] R.C. Merkle, M.E. Hellman, Hiding information and signatures in trapdoor knapsacks, in *Secure Communications and Asymmetric Cryptosystems*, ed. by G.J. Simmons. Volume 69 of AAAS Selected Symposium Series (Westview, Boulder, 1982), pp. 197–215

[85] D. Micciancio, Improving lattice based cryptosystems using the Hermite normal form, in *Cryptography and Lattices*, Providence, 2001. Volume 2146 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 126–145

[86] D. Micciancio, S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. The Kluwer International Series in Engineering and Computer Science, 671 (Kluwer Academic, Boston, 2002)

[87] G.L. Miller, Riemann's hypothesis and tests for primality. J. Comput. Syst. Sci. **13**(3), 300–317 (1976). Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing, Albuquerque, 1975

[88] V.S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology—CRYPTO '85*, Santa Barbara, 1985. Volume 218 of Lecture Notes in Computer Science (Springer, Berlin, 1986), pp. 417–426

[89] V.S. Miller, The Weil pairing, and its efficient calculation. J. Cryptol. **17**(4), 235–261 (2004). Updated and expanded version of unpublished manuscript *Short programs for functions on curves*, 1986

[90] P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization. Math. Comput. **48**(177), 243–264 (1987)

[91] S.p. Nakamoto, Bitcoin: a peer-to-peer electronic cash system (2009). https://bitcoin.org/bitcoin.pdf

[92] P. Nguyen, Cryptanalysis of the Goldreich–Goldwasser–Halevi cryptosystem from crypto'97, in *Advances in Cryptology—CRYPTO '99*, Santa Barbara, 1999. Volume 1666 of Lecture Notes in Computer Science (Springer, Berlin, 1999), pp. 288–304

[93] P. Nguyen, O. Regev, Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures, in *Advances in Cryptology—EUROCRYPT '06*, St. Petersburg. Volume 4004 of Lecture Notes in Computer Science (Springer, Berlin, 2006)

[94] P.Q. Nguyen, O. Regev, Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. J. Cryptol. **22**(2), 139–160 (2009)

[95] P. Nguyen, J. Stern, Cryptanalysis of the Ajtai-Dwork cryptosystem, in *Advances in Cryptology—CRYPTO '98*, Santa Barbara, 1998. Volume 1462 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 223–242

[96] NIST–AES, Advanced Encryption Standard (AES). FIPS Publication 197, National Institue of Standards and Technology, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[97] NIST–DES, Data Encryption Standard (DES). FIPS Publication 46-3, National Institue of Standards and Technology, 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[98] NIST–DSS, Digital Signature Standard (DSS). FIPS Publication 186-2, National Institue of Standards and Technology, 2004. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[99] NIST–SHS, Secure Hash Standard (SHS). FIPS Publication 180-2, National Institue of Standards and Technology, 2003. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[100] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers* (Wiley, New York, 1991)

[101] NTRU Cryptosystems, A meet-in-the-middle attack on an NTRU private key. Technical report, 1997, updated 2003. Tech. Note 004, https://www.securityinnovation.com/uploads/Crypto/NTRUTech004v2.pdf

[102] NTRU Cryptosystems, Estimated breaking times for NTRU lattices. Technical report, 1999, updated 2003. Tech. Note 012, https://www.securityinnovation.com/uploads/Crypto/NTRUTech012v2.pdf

[103] A.M. Odlyzko, The rise and fall of knapsack cryptosystems, in *Cryptology and Computational Number Theory*, Boulder, 1989. Volume 42 of Proceedings of Symposia in Applied Mathematics (American Mathematical Society, Providence, 1990), pp. 75–88

[104] J.M. Pollard, Monte Carlo methods for index computation (mod p). Math. Comput. **32**(143), 918–924 (1978)

[105] C. Pomerance, A tale of two sieves. Not. Am. Math. Soc. **43**(12), 1473–1485 (1996)

[106] E.L. Post, A variant of a recursively unsolvable problem. Bull. Am. Math. Soc. **52**, 264–268 (1946)

[107] J. Proos, C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Inf. Comput. **3**(4), 317–344 (2003)

[108] M.O. Rabin, Digitized signatures and public-key functions as intractible as factorization. Technical report, MIT Laboratory for Computer Science, 1979. Technical Report LCS/TR-212

[109] H. Riesel, *Prime Numbers and Computer Methods for Factorization*. Volume 126 of Progress in Mathematics (Birkhäuser, Boston, 1994)

[110] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)

[111] K.H. Rosen, *Elementary Number Theory and Its Applications*, 4th edn. (Addison-Wesley, Reading, 2000)

[112] S. Ross, *A First Course in Probability*, 9th edn. (Pearson, England, 2001)

[113] T. Satoh, The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc. **15**(4), 247–270 (2000)

[114] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Comment. Math. Univ. St. Paul. **47**(1), 81–92 (1998)

[115] C.-P. Schnorr, A hierarchy of polynomial time lattice basis reduction algorithms. Theor. Comput. Sci. **53**(2–3), 201–224 (1987)

[116] C.P. Schnorr, Fast LLL-type lattice reduction. Inf. Comput. **204**(1), 1–25 (2006)

[117] C.-P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, in *Fundamentals of Computation Theory*, Gosen, 1991. Volume 529 of Lecture Notes in Computer Science (Springer, Berlin, 1991), pp. 68–85

[118] C.-P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Program. **66**(2, Ser. A), 181–199 (1994)

[119] C.P. Schnorr, H.H. Hörner, Attacking the Chor–Rivest cryptosystem by improved lattice reduction, in *Advances in Cryptology—EUROCRYPT '95*, Saint-Malo, 1995. Volume 921 of Lecture Notes in Computer Science (Springer, Berlin, 1995), pp. 1–12

[120] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p. Math. Comput. **44**(170), 483–494 (1985)

[121] R. Schoof, Counting points on elliptic curves over finite fields. J. Théor. Nombres Bordx. **7**(1), 219–254 (1995). Les Dix-huitièmes Journées Arithmétiques, Bordeaux, 1993

[122] I.A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Math. Comput. **67**(221), 353–356 (1998)

[123] A. Shamir, How to share a secret. Commun. ACM **22**(11), 612–613 (1979)

[124] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans. Inf. Theory **30**(5), 699–704 (1984)

[125] A. Shamir, Identity-based cryptosystems and signature schemes, in *Advances in Cryptology*, Santa Barbara, 1984. Volume 196 of Lecture Notes in Computer Science (Springer, Berlin, 1985), pp. 47–53

[126] C.E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J. **27**, 379–423, 623–656 (1948)

[127] C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)

[128] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 1994 (IEEE Computer Society, Los Alamitos, 1994), pp. 124–134

[129] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)

[130] V. Shoup, Lower bounds for discrete logarithms and related problems, in *Advances in Cryptology—EUROCRYPT '97*, Konstanz. Volume 1233 of Lecture Notes in Computer Science (Springer, Berlin, 1997), pp. 256–266

[131] V. Shoup, OAEP reconsidered, in *Advances in Cryptology—CRYPTO 2001*, Santa Barbara. Volume 2139 of Lecture Notes in Computer Science (Springer, Berlin, 2001), pp. 239–259

[132] V. Shoup, *A Computational Introduction to Number Theory and Algebra* (Cambridge University Press, 2005). http://shoup.net/ntb/ntb-b5.pdf

[133] C.L. Siegel, A mean value theorem in geometry of numbers. Ann. Math. (2) **46**, 340–347 (1945)

[134] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Volume 151 of Graduate Texts in Mathematics (Springer, New York, 1994)

[135] J.H. Silverman, Elliptic curves and cryptography, in *Public-Key Cryptography*, Les Diablerets. Volume 62 of Proceedings of Symposia in Applied Mathematics (American Mathematical Society, Providence, 2005), pp. 91–112

[136] J.H. Silverman, *The Arithmetic of Elliptic Curves*. Volume 106 of Graduate Texts in Mathematics, 2nd edn. (Springer, Dordrecht, 2009)

[137] J.H. Silverman, *A Friendly Introduction to Number Theory*, 4th edn. (Pearson, Upper Saddle River, 2013)

[138] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics (Springer, New York, 1992)

[139] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* Reprint edn. (Anchor, New York, 2000)

[140] B. Skjernaa, Satoh's algorithm in characteristic 2. Math. Comput. **72**(241), 477–487 (electronic) (2003)

[141] N.P. Smart, The discrete logarithm problem on elliptic curves of trace one. J. Cryptol. **12**(3), 193–196 (1999)

[142] Standards for Efficient Cryptography, SEC 2: recommended elliptic curve domain parameters (Version 1), 20 Sept 2000. http://www.secg.org/collateral/sec2_final.pdf

[143] J. Talbot, D. Welsh, *Complexity and Cryptography: An Introduction* (Cambridge University Press, Cambridge, 2006)

[144] E. Teske, Speeding up Pollard's rho method for computing discrete logarithms, in *Algorithmic Number Theory*, Portland, 1998. Volume 1423 of Lecture Notes in Computer Science (Springer, Berlin, 1998), pp. 541–554

[145] E. Teske, Square-root algorithms for the discrete logarithm problem (a survey), in *Public-Key Cryptography and Computational Number Theory*, Warsaw, 2000 (de Gruyter, Berlin, 2001), pp. 283–301

[146] J. Von Neumann, Various techniques used in connection with random digits. Natl. Bur. Stand. Appl. Math. Ser. **12**(36–38), 1 (1951). Reprinted in von Neumann's Collected Works, 5 (1963), Pergamon Press, pp. 768–770. https://dornsifecms.usc.edu/assets/sites/520/docs/VonNeumann-ams12p36-38.pdf

[147] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications (Chapman & Hall/CRC, Boca Raton, 2003)

[148] A.E. Western, J.C.P. Miller, *Tables of Indices and Primitive Roots*. Royal Society Mathematical Tables, vol. 9 (Published for the Royal Society at the Cambridge University Press, London, 1968)

[149] M.J. Wiener, Cryptanalysis of short RSA secret exponents. IEEE Trans. Inf. Theory **36**(3), 553–558 (1990)

[150] S.Y. Yan, *Primality Testing and Integer Factorization in Public-Key Cryptography*. Volume 11 of Advances in Information Security (Kluwer Academic, Boston, 2004)

Index

J. Hoffstein et al., *An Introduction to Mathematical Cryptography*,
Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4939-1711-2