## REFERENCES


1. A. menezes , T. Okamoto , S. Vanstone , reducing elliptic curve logarithms to logarithms in a finite field , IEEE Trans. Inform. Theory , 39 , 1639-1646 ,1993
2. A.E. Western and J.C.P. miller, Tables of indices and primitive roots . Royal Soci. Of Mathematical Tables of vol. 9, Cambridge university press , 1968
3. A.H. Koblitz, N.koblitz and A. Menezes : Elliptic curve Cryptography : The Serpentine course of a Paradigm Shift .J. of Number theory 13 , pp. 781-814 , 2011
4. A.M. ODLYZKO Discrete logarithms and their cryptographic significance Advances in cryptographic proceedings of EUROCRYPT '84, Springer-Verlag, New York, pp. 224-314, 1985
5. American National Standard Algorithm (ANSA) X9.62, Public key cryptography for the financial service industry. The Elliptic Curve Digital Signature Algorithm (ECDSA) 1999
6. Arrendondo, B., Jansma, N. : Performance comparison of Elliptic Curve and RSA Digital Signatures, IPCSIT, vol. 4, IACSIT press, Singapore, 2011
7. B.P. Schanning : Data encryption with public key distribution , EASCON Conf. Rec. , Washington D.C. pp. 653-660 ,1979
8. Basin , D., Cremers , C., Miyazaki , K., Radomirovic , S.,& Watanabe, D., improving the Security of Cryptographic protocol Standards. IEE Security & Privacy 13(3) , pp. 24-31, 2015
9. Bauer , F.L. : Decrypted Secrets : Methods and Maxims of Cryptology 2nd Ed. New York: Springer- verlag , 2002
10. Belfield , R. : The Six unsolved ciphers : Inside the mysterious Codes, That Have Confounded the World's Greatest Cryptographer's , Berklery , CA Ulysses press , 2007.
11. Bos, J.; M. Kaigara; et al.; "on the security of 1024-bit RSA and 160-bit Elliptic curve cryptography The Serpentine course of a paradigm shift", Journal of Number theory , vol. 131, ISJ. 8, pp. 781-814, 2014 (www.sciencedirect.com/science/article/pii/500)
12. Brown, D.R.L. : SECI : Elliptic curve cryptography centicom corp. 2009
13. Chen , T.S. , Huang , K.H. , Chung , Y.F. : A practical authenticated encryption sheme based on the elliptic curve cryptosystems , Computer Standards & Interface 26 , pp. 461-469 , 2004
14. Corbelling , A : Elliptic curve cryptography finite fields and discrete logarithms (2015) http://andra.corbollini.name/2015/05/23/elliptic_curve-cryptography-finite-fields-and-discrete-logarithms
15. Cryptography be trusted : Can Elliptic curve ISACA Journal, vol. 03, 2016
16. D. Bernstein. Curve 25519 :new Diffie-Hellman Speed records. Public key cryptography-PKC2006. LNCS 3958, Springer-verlag, pp. 207-228, 2006
17. D. Brown and K. Gjosteen. A Security analysis of the NIST SP 800-90 eliptic curve random number generator, Advances in cryptology CRYPTO 2007, LNCS 4622, Springer-verlag, pp. 466-479, 2007.

18. D. Coppersmith, Evaluating logarithms in GF(2n) , 16th ACM. Symp. Theory of computing , pp. 201-207 , 1984
19. D. Gorden Discrete logarithms in GF(P) using the number field sieve , SIAM J. Discrete math. 6 , pp. 124-138, 1998
20. D. Jao , S. miller , R. Venkatesan , Do all elliptic curves of the same order have the same difficulty of discrete log ? , in : Advances in Cryptology-ASIACRYPT 2005 ,in: Lecture Notes in computer science , vol. 3788 , pp. 21-40 , 2005
21. D. Sadhu khan , S. Ray.: Cryptanalysis of an elliptic curve cryptography , based light weight authentication Scheme for Smart grid Communication , 2018 4th international conference tech no. (RAIT) IEEE (2018) pp. 1-6
22. D. Sravana Kumar et.al. Encryption of Data using Elliptic curve over finite fields , Int. Jr. of Distributed and Parallel Systems (IJDPS) , vol. 3 ,no.1 ,2012
23. D.F. Aranha, P.S.L.M , Barreto , G.C.C.F. Pereira , and J.E. Ricardini. A note on high-security general purpose elliptic curves . Cryptography e- print Archive , http://eprint.iacr.org/ ,2013
24. D.G. Cantor and H. Zassenhaus .A new algorithm for factoring polynomials over finite fields Math computer 36, pp. 587-592 ,1981
25. D.J. Bernstein and T. Lange Faster addition and doubling on elliptic curves. In K. kurosawa editor ASIACRYPT, vol.4833 , of LNCS, pp. 29-50, sprirfer ,2007.
26. D.J. Bernstein and T. Lange. Safe Curves : choosing safe curves for elliptic-curve cryptography http://safecurves.cr.yp.to , 2013.
27. Diffie , Whitefield , Hellman Martin E . New directions in cryptography. IEEE. Transactions on information theory 22(6) pp. 644-654. 1976
28. El Gamal , Taher A public key crypto system and a signature scheme based on Discrete logarithm (PDF) , IEEE Transactions on information theory 31(4) , pp. 469-472 , 1985
29. Esslinger, B., & the CrypTool Team : The cryptool Book, Learning and expensive .
30. H.M. Edwards. A normal form for elliptic curves. Buletin of the American Mathematical Society (AMS) , 44 , pp. 393-422 , 2007.
31. H.W Lenstra Jr. , Factoring integers with elliptic curves , An. of Math .126 , pp.649-673, 1987
32. Hellman , martin , E , : An overview of public key cryptography , IEEE Communications magazine 40(5) pp. 42-49 , 2002
33. https://en.wikipia.org/wiki/fermat_primality_tess
34. Huelsing., D. Butin, S. Gazdag and A. mohaisen : XMSS : Expected Hash based signatures , IETS, Internet Draft, 22, 2016.
35. I. Semaev : Summation polynomials and the discrete logarithm problem on elliptic curves available at http://eprint.iacr.org/2004.031.
36. I.F. Blake, R. Fuji, R.C. Mullin and S.A Vanstone. Computing logarithms in finite fields characteristic two SIAM, J. Alg. Disc. Methods 5, pp. 276-285, 1984

37. Ireland , K and Rosen , M . “Elliptic curves “. Ch.18 in A classical Introduction to modern number theory , 2nd ed. New York : Springer-verlag , pp. 279-318 , 1990
38. J. cheon :security analysis of the strong Di/tie-Hellman problem ,in: advances in cryptology – EUROCRYPT 2006 ,in :Lecture Notes in Computer Science ,vol. 4004 ,pp.1-11,2006
39. J. Kowalchuk , B.P. Schanning and S. Powers , communication privacy : Integration of public and secret key cryptography. NTC Conference , Record , Vol. 3 , pp. 49.1 , 1-49.1.5,1980
40. J. Pillard. Monte Carlo methods for index computations (MODP), math. Comp. 32, pp. 918-924 ,1978.
41. J. Renes, C. Costello and L. Batina : Complete addition formulas for prime order elliptic curves, Advances in Cryptology-EUROCRYPT 2016, LNCS 9665, Springer-verlag, pp. 403-428, 2018
42. J. Silverman , J .Suzuki ,Elliptic curve discrete logarithms and the index calculus , in : advances in cryptology ,ASIACRYPT ’98, in :Lecture Notes in Computer Science , vol 1514,pp.110-125 , 1998
43. J. Silverman : The Arithmetic on Elliptic curves Springer -Verlag, 1986
44. J. Solinas, Efficient arithmetic on koblitz curves , Des , Codes Cryptography . 19 , pp. 195-249 , 2000
45. J.A. Solinas : Efficient arithmetic on koblitz curves , Designers , Codes and Cryptography 19 , pp. 195-249 , 2000.
46. Jerko Teariaho , Cyclic group cryptography with elliptic curves , Brasor , 2001
47. K. Nyberg , R.A. Rueppel. : Message recovery for signature schemes based on discrete logarithm problem. designs , codes and cryptography 7(1-2) pp.61-81 , 1996
48. Koblitz, N., Menezes, A., Vanstone, S. : The state of elliptic curve cryptography In: Towards a Quarter-century of public key cryptography “Kluwer Academic Publishers, pp. 173 -193, Boston (2000)
49. Krists Magons : Applications and Benefits of Elliptic Curve Cryptography : University of Latria, Faculty of Computing
50. Kumar ET. Al., (2019): An identity based authentication frame work for big data Security. Proceeding of 2nd international Conference on Communication Computing and Networking , Springer, pp. 63-71, 2019.
51. L. Washington , Elliptic curves : Number theory and cryptography , second ed. , CRC press , 2008
52. L.D. Singh , and K.M. Singh : Implementation of Text Encryption using Elliptic curve cryptography Procedia Computer Science 54 , pp. 73-82 , 2015
53. L.M. Adleman . A Sub exponential algorithm for discrete logarithm problem with application to cryptography , proc. 20th IEEE found Comp. Sci. Symp., pp. 55-60 , 1979
54. Lawrence C. Washington : Elliptic curves , Number Theory and cryptography , Tayler & Francis Group , second edition , 2008

55. Lyngaas, S. ; Decrypting outbound Data. : A key to security" FCW, 11, 2015 (http://fcw.com/articles/2015/08/11/SSL-encryption.aspx.) Erich H, Goldman, : Encryption in the Hands of End Users. ISACA Journal, vol. 3 pp. 1-6, 2016
56. M. Mosca. Cyber Security in an era with quantum computers: Will we be safe? Available at http://eprint.iacr.org/2015/1075.
57. M. Wiener and R. Zuccherato : faster attacks on elliptic curve cryptosystems, selected areas in cryptology , SAC198. LNCS156, Springer-verlag, pp.190-200, 1999.
58. M.E. Hellman and J.M. Reyneri, Fast Computation of discrete logarithms in GF(9) ,pp. 3-13 in advances in cryptography proceeding of CRYPTO' 82 ,D. chaum , R. Rivest and a . Adleman etc. plenum press, 1983
59. M.O. Rabin. Probabilistic algorithms in finite fields. SIAM , J. Comp. 9,pp. 273-280,1980
60. Mankle, Ralth C. secure communications of the ACM 21(4) pp.294-299, 1978.
61. Mazur , B. and Tate , J. "Points of order 13 on Elliptic curves , .Invent. math .22, pp. 41-49, 1973/74
62. Megha Kolhekar and Anita Jadhav. Implementation of Elliptic curve Cryptography on Text and Image. System, vol. 1, issue 2 , 2011.
63. N. koblitz An elliptic curve implementation of the finite field digital signature algorithm , in: advances in cryptology , CRYPTO-"98", in: Lecture Notes in computer science , vol . 1462, pp. 327-337 , 1998
64. N. Koblitz and A. Menezes : Another look Security definitions. Advances in Mathematics of Communications 7, pp. 1-38, 2013.
65. N. Koblitz and A.J. Menezes : A Riddle Wrapped in an Enigma.
66. N. Koblitz, Introduction to Elliptic curves and modular forms, Springer-verlag, New York , 1984.
67. N. Sharma , Prabhjot and H. Kaur. "A review of information security using cryptography technique International Journal of Advance Research in Computer Science, vol18 No. special issue pp. 323-326,2017
68. N.Koblitz, Elliptic curve cryptosystems, math .comp. 48, pp .203-209, 1987
69. N.koblitz. Introduction to elliptic urves and modular forms , New York : springer –verlag , 1993
70. National Security Agency (NSA): The case of elliptic curve cryptography." USA. 2015.
71. National Security Agency. The case for elliptic curves cryptography tinyurl.com/NSA and ECC, 2005.
72. Neal koblitz A course in number theory and cryptography, Graduate Texts In math. no 114 , Springer verlag , New York, 1987 second edition,pp. 94, 1994.
73. Neal koblitz and Victor miller.
74. Nissa Mehibel et al. : A new enhancement of elliptic curve digital Signature algorithm Jr. of Discrete mathematical Sciences and cryptography,vol. 23, issue 3, pp. 743-757, 2020

75. P. Gaudry , index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem , J. Symbolic computers , available from http://www.loria.fr/gaudry/papers.en.html
76. P.K.S. wah & M.Z. Wang : Realization and application of the Massey . Omura lock. , Proc. Internet , Zurich Seminar , march 6-8 , pp. 175-182, 1984
77. Pholing Hellman "An improved Algorithm for computing Logarithms over GF (p) and its cryptographic singnificance . 1978 . http://www.ee.standard.edu/hellman/publications/28.pdf.

# REFRENCES

78. Rivest, R.L , Shamir ,A. , and Adleman , L. , A method for obtaining Digital signatures and public key crypto systems. Communications of the ACM , vol 21 , No.2 , pp 120-126 , 1978.
79. S. choof ,R: Elliptic curves over finite fields and the computation of square roots . Mathematics of computation. vol. 44. pp. 483-494 (1985)
80. S. Galbraith and P. Gaudry : Recent progress on the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography 78, pp. 51-72, 2016.
81. S. Galbraith and S. Gebregiyorgis : Summation polynomial algorithms for elliptic curves in characteristic two progress on cryptology-INDOCRYPT 2014, LNCS 8885, Springer-verlag, pp.402-427, 2014.
82. S. Pohling, M. Hellman , An improved algorithm for computing logarithms over GF (p) and its cryptographic significances ,IEEE trans. Inform. Theory 24 , pp. 106-110 1978
83. S. Tayal , N. Gupta, P. Gupta, S. Vijay "Review Network Security and Cryptography Advances in Computational Sciences and Technology, vol. 10, no.5, pp. 768-770, 2017.
84. S. Vanstone and D. Brown: Elliptic curve random number generation, International patent application, WO 2006/076804A1, 2006.
85. S.S. Dhanda, Brahmjit Singh, Poonam Jindal, Demystifying elliptic curve cryptography curve Selection, Implementation and Countermeasures to attacks to Journal Interdisciplinary Mathematics, vol. 23, issue 2, pp. 463-470, 2020
86. Silverman , H.S. : An introduction to the theory of Elliptic curves ,University of Wyoming , 2006
87. Silverman , J.H. and Tate , J.T. : Rational points on Elliptic curves , New York, Springer-verlag,1992
88. Stinson, D.R. Cryptography theory and practice 3rd edition, Chapman &Hall/ CRC, New York. 2006.
89. V. miller , fast multiplication on elliptic curves over small fields of characteristic two . J . Cryptology 11,pp.219-234 ,1998

90. V. miller , uses of elliptic curves in cryptography , in :advances in cryptology –CRYPTO 85, in: Lecture Notes in computer Sci., vol218 ,pp.417-426 1986
91. William Stallings : Cryptography and Network Security prentic Hall , 4th Edition , 2000
92. Zhang, J., Chen B., Zhao, Y., Cheng. X., & HU, F., Data security and pricvacy preserving I edge computing paradigm: survey and open ISSUE Access, pp. 18237, 2018