An Overview of the Discrete Logarithm Problem in Cryptography

| Conference paper | First Online: 23 December 2024

| pp 129–143 | Cite this conference paper

Proceedings of Third International Conference on Advanced Computing and Applications

(ICACA 2024)

Abhiroop Sarkar, Deepsubhra Guha Roy & Piyali Datta

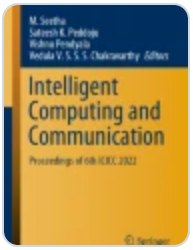
Part of the book series: Lecture Notes in Networks and Systems ((LNNS,volume 1045))

Included in the following conference series:
International Conference on Advanced Computing and Applications

Abstract

The discrete logarithm problem is a computationally hard problem that is widely employed in public-key cryptography, based on the assumption that there exists no general method to efficiently solve discrete logs. In this paper, we investigate the historical evolution, theoretical foundations, associated equations, implementation techniques, applications, and security aspects of the discrete logarithm problem. A timeline detailing the early development of discrete logarithms in cryptography is presented. The algorithms deployed to solve discrete logarithm problems, including Shanks' baby step–giant step algorithm, Pohling–Hellman's algorithm, Pollard's Rho algorithm, Pollard's Kangaroo algorithm, index calculus, and function field sieve, are discussed. Additionally, an overview of Shor's quantum algorithms is provided. The paper also offers concise discussions of schemes such as Diffie–Hellman key exchange, ElGamal encryption, and elliptic curve cryptography.

Supported by IEM Grant in Aid Project from Institute of Engineering and Management, Kolkata, India.



Technical history of discrete logarithms in small characteristic finite fields

Article | 24 November 2015

Quantum Cryptanalysis Landscape of Shor's Algorithm for Elliptic Curve Discrete...

Chapter | © 2021

Comparison of Pollard's rho Algorithm Based on Cycle Finding Methods

Chapter | © 2023

References

1. Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654

Google Scholar

2. Merkle R (1978) Secure communication over insecure channels. Commun ACM 21:294–299

Article Google Scholar

3. Paar C, Pelzl J (2010) Understanding cryptography: a textbook for students and practitioners. Springer

Google Scholar

4. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signature and public-key cryptosystems. Commun ACM 21(2), 120–126

Google Scholar

5. Kritsanapong S (2020) The new integer factorization algorithm based on Fermat's Factorization Algorithm and Euler's theorem. Int J Electr Comput Eng 10

Google Scholar

6. Andreas SS, Claudio T (2020) Integer factorization and Riemann's hypothesis: why two-item joint replenishment is hard. arXiv: Computational Complexity

7. Ralph Charles Merkle, Secrecy, authentication, and public key systems. Ph.D. Dissertation. Stanford University, Stanford, CA, USA. Order Number: AAI8001972 (1979)

Google Scholar

8. Lamport L (1979) Constructing digital signatures from a one way function. SRI International (CSL-98)

Google Scholar

9. Goldwasser S, Micali S, Rivest RL (1988) SIAM J Comput 17(2):281–308

Article MathSciNet Google Scholar

10. Coppersmith D (1984) Fast evaluation of logarithms in fields of characteristic two. IEEE Trans Inf Theory 30(4):587–594

Google Scholar

11. Adleman L (1979) A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In: 20th Annual Symposium on Foundations of Computer Science (sfcs 1979). San Juan, PR, USA, pp 55–60

Google Scholar

12. Elgamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31(4):469–472

Google Scholar

13. Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209

Article MathSciNet Google Scholar

14. Miller VS (1986) Use of elliptic curves in cryptography. In: Williams HC (eds) Advances in cryptology - CRYPTO '85 proceedings. CRYPTO 1985. Lecture notes in computer science, vol 218. Springer, Berlin, Heidelberg

Google Scholar

15. McCurley KS (1990) The discrete logarithm problem. Proc Symp Appl Math 22

Google Scholar

16. Leonard M, Adleman JD (1993) A subexponential algorithm for discrete logarithms over all finite fields. Math Comput 61(203):1–15

Article MathSciNet Google Scholar

17. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science, Santa Fe, NM, USA, pp 124–134

Google Scholar

18. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26(5):1484–1509

Article MathSciNet Google Scholar

19. Joux A (2000) A one round protocol for tripartite Diffie-Hellman. In: Bosma W (eds) Algorithmic number theory. ANTS 2000. Lecture notes in computer science, vol 1838. Springer, Berlin, Heidelberg

Google Scholar

20. Proos J, Zalka C (2003) Shor's discrete logarithm quantum algorithm for elliptic curves. Quant Inf Comput 3(4):317-344

Google Scholar

21. Childs A, Ivanyos G (2014) Quantum computation of discrete logarithms in semigroups. J Math Cryptol 8(4):405–416

Article MathSciNet Google Scholar

22. Battarbee C, Kahrobaei D, Perret L, Shahandashti SF (2022) A subexponential quantum algorithm for the semidirect discrete logarithm problem. Cryptology ePrint Archive, Paper 2022/1165

Google Scholar

23. Shanks D (1969) Class number, a theory of factorization and genera. Proc Symp Pure Math 20:415–440

Article Google Scholar

24. Stein A, Teske E (2005) Optimized baby step-giant step methods. 20:1–32

Google Scholar

25. Stephen C, Pohlig, Martin E, Hellman (1978) An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.). IEEE Trans Inf Theory, 24

Google Scholar

26. Pollard (2010) By J. M.. Monte Carlo methods for index computation (mod p). Math Comput 32(143):918–924

Google Scholar

27. Brent RP (1980) An improved Monte Carlo factorization algorithm. BIT 20:176–184

Article MathSciNet Google Scholar

28. Pollard JM (2000) . Kangaroos, monopoly and discrete logarithms. J Cryptol 13(4):437-447

Google Scholar

29. Kraitchik M (1922) Théorie des nombres, vol 1. Gauthier-Villars, Paris

Google Scholar

30. Padmavathy R, Bhagvati C (2012) Discrete logarithm problem using index calculus method. Math Comput Model 55(1-2)

Google Scholar

31. Adleman LM (1994) The function field sieve. In: Adleman LM, Huang MD (eds) Algorithmic number theory. ANTS 1994. Lecture notes in computer science, vol 877. Springer, Berlin, Heidelberg

Google Scholar

32. Adleman LM, Huang MA (1999) Function field sieve method for discrete logarithms over finite fields. Inf Comput 151: 5–16. Academic

Google Scholar

33. Joux A, Lercier R (2002) The function field sieve is quite special. ANTS-V, Sydney, Australia, July 7–12, 2002. Proceedings, LNCS, vol 2369, pp 431–445

Google Scholar

34. LaMacchia BA, Odllyzko AM (1991) Computation of discrete logarithms in prime fields. Des Codes Crypt 1(1):46–62

Article MathSciNet Google Scholar

35. Ekerå M (2021) Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. J Math Cryptol 15(1):359–407

Article MathSciNet Google Scholar

36. Ekerå M (2016) Modifying Shor's algorithm to compute short discrete logarithms, IACR ePrint Archive Report 2016/1128

Google Scholar

37. Huang Y, Su Z, Zhang F, Ding Y, Cheng R (2020) Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. Quant Inf Process 19:1–17

Article MathSciNet Google Scholar

38. Roy KS, Kalita HK (2019) A survey on post-quantum cryptography for constrained devices. Int J Appl Eng Res 14

Google Scholar

39. Khader AS, Lai D (2015) Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. 2015. In: 22nd international conference on telecommunications (ICT), pp 204–208

Google Scholar

40. Burmester M, Desmedt Y (1995) A secure and efficient conference key distribution system, EUROCRYPT 1994 (A. De Santis, ed.), LNCS, vol 950, Springer, pp 267–275

Google Scholar

41. Adrian D, Bhargavan K, Durumeric Z, Gaudry P, Green M, Halderman JA, Heninger N, Springall D, Thomé E, Valenta L, VanderSloot B (2018). Imperfect forward secrecy: how Diffie-Hellman fails in practice. Commun ACM 62(1): 106–114

Google Scholar

42. Abdalla M, Pointcheval D (2005) Simple password-based encrypted key exchange protocols. In: Menezes A (eds) Topics in cryptology - CT-RSA 2005. Lecture notes in computer science, vol 3376. Springer, Berlin, Heidelberg

Google Scholar

43. Mikhail M, Abouelseoud Y, Elkobrosy G (2004) Extension and application of El-Gamal encryption scheme. In: World congress on computer applications and information systems (WCCAIS), Hammamet, Tunisia, 2014, pp 1–6

Google Scholar

44. NIST (2003) Special Publication 800-57: recommendation for key management. Part 1: general guideline, Draft

Google Scholar

45. Vivek K, Vivek S, Abraham, Ramesh S (2008) Elliptic curve cryptography. ACM Ubiquity, 9, 7

Google Scholar

46. Bos, J.W., Halderman, J.A., Heninger, N., Moore, J., Naehrig, M., Wustrow, E. Elliptic Curve Cryptography in Practice. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg (2014)

Google Scholar

47. M. E. Hellman, An overview of public key cryptography, in IEEE Communications Magazine, vol. 40, no. 5, pp. 42-49, May (2002)

Google Scholar

48. Steven D (2012) Galbraith. Mathematics of Public Key Cryptography, Cambridge University Press

Google Scholar

49. Nielsen M, Chuang I (2010) Quantum Computation and Quantum Information: 10th, Anniversary. Cambridge University Press, Cambridge

Google Scholar

Acknowledgements

We would like to express our heartfelt gratitude to the IEM Centre of Excellence for Cloud Computing and IoT for invaluable support and resources from IEM Grant-in-Aid project of Dr. Deepsubhra Guha Roy, which have enabled us to conduct this review. We are also deeply thankful to the IEDC-CSE of the Institute of Engineering & Management, Kolkata, for providing us the work space that made this work possible.

Author information

Authors and Affiliations

Institute of Engineering and Management, University of Engineering and Management, Kolkata, India
Abhiroop Sarkar

IEM Centre of Excellence for Cloud Computing and IoT, Department of CSE(AIML), Institute of Engineering and Management, University of Engineering and Management, Kolkata, India
Deepsubhra Guha Roy

IEM Centre of Excellence for Data Science, Department of CSE(AIML), Institute of Engineering and Management, University of Engineering and Management, Kolkata, India
Piyali Datta

Corresponding author

Correspondence to Deepsubhra Guha Roy .

Editor information

Editors and Affiliations

Depart. of IT, Maulana Abul Kalam Azad Univ. of Tech., Kolkata, West Bengal, India
Debasis Giri

Electronics and Communication Sci. Unit, Indian Statistical Institute, Kolkata, West Bengal, India
Swagatam Das

BISITE Research Group, University of Salamanca, Salamanca, Spain
Juan Manuel Corchado Rodríguez

Tech, Dept of Comp Sci and Engineering, Maulana Abul Kalam Azad University of, Kolkata, West Bengal, India
Debashis De

Rights and permissions

Copyright information

About this paper

Cite this paper

Sarkar, A., Guha Roy, D., Datta, P. (2024). An Overview of the Discrete Logarithm Problem in Cryptography. In: Giri, D., Das, S., Corchado Rodríguez, J.M., De, D. (eds) Proceedings of Third International Conference on Advanced Computing and Applications. ICACA 2024.

Lecture Notes in Networks and Systems, vol 1045. Springer, Singapore.
https://doi.org/10.1007/978-981-97-4799-3_10

.RIS .ENW .BIB

DOI
https://doi.org/10.1007/978-981-97-4799-3_10

Published
23 December 2024

Publisher Name
Springer, Singapore

Print ISBN
978-981-97-4798-6

Online ISBN
978-981-97-4799-3

eBook Packages
Intelligent Technologies and Robotics
Intelligent Technologies and Robotics (R0)

Publish with us

Policies and ethics