IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 6, May 2023

A New Lightweight Symmetric Encryption Scheme for String Identification

Vengadesh K[1], Vishwa Kumar K[2], Sriram M[3],Grace Mary S[4]

Students, Department of Computer Science Engineering[1,2,3]

Assistant Professor, Department of Computer Science Engineering[4]

Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract: *In this paper, We present an efficient and simple-to-implement symmetric encryption scheme for string search that requires just one round of communication and O(N) computations across N documents. Unlike previous schemes, we use hash-chaining for index generation rather than a chain of encryption operations, making it suitable for lightweight applications. Unlike Previous String Search Schemes, Our Scheme Learns Nothing About The Frequency And Relative Positions Of The Words Being Searched Except What It Can Learn From History. We are the first to propose probabilistic trapdoors In String Symmetric Encryption Scheme we provide concrete proof of our scheme's non-adaptive security against an honest-but-curious server. Provides some protection against trapdoor leakage. We have demonstrated that our scheme is secure according to the Pattern Indistinguishable Definition. We demonstrate why symmetric encryption schemes for string searches fail to meet adaptive indistinguishable criteria. We also propose changes to our scheme that will allow it to be used against active adversaries at the expense of more communication rounds and memory space. We validate our scheme using two commercial data sets.*

Keywords: Cloud storage, Symmetric key, Encryption Scheme, lightweight cryptography

REFERENCES

[1]. D. J. Wheeler and R. L. Schroeppel, "Optimizing SHA-1 in Assembly Language," in Proceedings of the Second International Workshop on Fast Software Encryption, Springer-Verlag, 1995, pp. 261-277.

[2]. P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Springer-Verlag, 2004, pp. 371-388.

[3]. R. C. Merkle, "A certified digital signature," in Advances in Cryptology: Proceedings of CRYPTO '89, Springer-Verlag, 1990, pp. 369-378.

[4]. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[5]N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

[6]. C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, 2010.

[7]. D. Stinson, Cryptography: Theory and Practice, CRC Press, 2019.

[8]. W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2017.

[9]. H. Wang, D. Zhu, and X. Hu, "A new lightweight symmetric encryption scheme for Internet of Things," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 3, pp. 1271-1281, 2019.

[10]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology: Proceedings of CRYPTO '01, Springer-Verlag, 2001, pp. 213-229.

DOI: 10.48175/IJARSCT-10114