A Linear Chaotic Function with Dynamic Constants for Rapid Chaos

P. Karthik, P. Shanthi Bala

Department of Computer Science, Pondicherry University, Puducherry

ABSTRACT

The generation of unique random numbers for the distinct inputs continues a forever research problem. The modern cryptographic applications like Modification Detection Code (MDC) and Message authentication code (MAC) provide an edge to the Chaotic function to provide a security-centric integrity solution. This is because, the chaotic function is a strong one-way function and it involves massive computational power to produce an unpredictable sequence of output symbols for a given input. It recursively applies the logistic map function on every independent element of the input data to generate a significant random sequence. The chaotic function is extremely sensitive to the initial conditions, and it demands backbreaking efforts to find hash collisions. The changes recorded in the output bits between any two consecutive iterations are minimal. Therefore, the chaotic function demands more iterations to foresee the random behavior in its output. The current work poses an effort to maximize the avalanche responses of any two successive chaotic iterations. It performs the task by drastically increasing the chaotic behavior through the application of dynamic constants. It helps the novel design to exhibit an identical Random behavior with reduced iterations. The experimental analysis on Avalanche and Near-collision proves the fact that the novel design will provide a security-centric data integrity solution.

© 2020 Copyright held by the author(s). Published by AIJR Publisher in Book of Abstracts for "TEQIP - III Sponsored First International Conference on Innovations and Challenges in Computing, Analytics and Security" (ICICCAS-2020) July 29-30, 2020. Organized by the Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India. Series: AIJR Abstracts; ISBN: 978-81-942709-3-5 (eBook); DOI: 10.21467/abstracts.90