Automated Proof Techniques for Assessing the Security of Chaos-Based Encryption Algorithms

Fatih Özkaynak[1,2*]
[1] Fırat University Department of Software Engineering 23119 Elazig Turkey
[2] Kriptarium Ar-Ge Yazılım 23350 Elazig, Turkey
ozkaynak@firat.edu.tr, fatih@kriptarium.com

Abstract

Chaos-based encryption systems have been extensively studied in the cryptographic literature since the early 1990s. These studies have garnered attention, particularly in cryptographic applications, due to their complexity and unpredictability; however, they have often not found a complete place in mainstream cryptographic literature. This deficiency is associated with a series of criticisms asserting that such encryption algorithms are not secure. In particular, security analyses of chaos-based image encryption algorithms often focus solely on specific statistical analyses. While these analyses include measurements such as histogram analysis, NPCR, UACI, and correlation, they are often insufficient to assess the security of the algorithms. This approach, providing a limited perspective, does not accurately reflect the reliability of chaos-based encryption algorithms. Chaos-based encryption systems, especially in recent years with increased computing power and technological advancements, face new security challenges. In this context, the scope of research in this field encompasses a wide range of aspects, from the mathematical foundations of algorithms to practical applications. The detection of security vulnerabilities and weaknesses forms the focal point of studies aimed at making chaos-based encryption algorithms more reliable. The significance of the subject, particularly in the context of digital security and data protection, lies in the need to enhance the reliability and robustness of chaos-based encryption systems in potential areas of application. These studies aim not only to highlight the shortcomings of existing algorithms but also to develop more effective solutions against future security threats. Therefore, comprehensive research on chaos-based encryption systems plays a crucial role in the field of information security and is influential in shaping future security standards.

The primary research question of this study is how to leverage automatic proof techniques systematically to address the security issues of chaos-based image encryption algorithms, systematically tackling the deficiencies and challenges in this field and

[*] Masterminded EasyChair and created the first stable version of this document

evaluating the security of these algorithms. The goal is to establish a network, utilizing the knowledge and experience of researchers within the scope of this action, to create a solution-oriented roadmap.

.