Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

The CiliPadi Family of Lightweight Authenticated Encryption, v1.2

Z'aba, M. R.[1,*], Jamil, N.[2], Rohmad, M. S.[3], Rani, H. A.[4], and Shamsuddin, S.[4]

[1]*Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Malaysia*
[2]*College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia*
[3]*Faculty of Electrical Engineering, Universiti Teknologi MARA, Malaysia*
[4]*CyberSecurity Malaysia*

E-mail: reza.zaba@um.edu.my
[*]*Corresponding author*

Received: 8 January 2020
Accepted: 4 August 2021

Abstract

This article describes the specification and analysis of the CiliPadi family of lightweight authenticated encryption v1.2. An earlier version, dubbed v1.0, was accepted as one of the Round 1 candidates in the US NIST lightweight cryptography project. CiliPadi is designed based on the Sponge construction which is also used in the SHA-3 hash function. CiliPadi supports 128- and 256-bit keys and is offered in four variants or flavours. The flavours differ in the length of tag, message block and the number of rounds of the internal permutation.

Keywords: authenticated encryption; sponge construction; lightweight cryptography; symmetric encryption; generalized Feistel network.