# Spongy-Gift: A New Lightweight Message Authentication Code

Cuauhtemoc Mancillas-López[1] and Mridul Nandi[2]

[1]Laboratoire Hubert Curien, University of Lyon at St-Etienne, France
[2]Applied Statistics Unit, Indian Statistical Institute, India

Abstract

In the recent years Internet of Things (IoT) has been a hot topics, at the same time its security issues have gained a lot of attention. The intrinsic characteristics of IoT make the design of security modules for it a very difficult task, mainly the restrictions in memory, energy and physical resources. One of the important security requirements are data authentication and data integrity, Message Authentication Codes (MACs) are primitives of symmetric cryptography used to provide them. In this work we introduce Sopongy-Gift which is a MAC constructed as a sponge function using a permutation based on the round of block cipher Gift [1]. The design decisions, security aspects and implementation issues are discussed. Final implementation results show Sopongy-Gift can be implemented using very low resources and matches the speed requirements for IoT applications.

[1]Banik et al, CHES 2017