

Landau-Ramanujan keyed hash functions for message authentication

A. Suganya*

N. Vijayarangan†

SETS

No. 21, Mangadu Swamy street

Nungambakkam

Chennai 600 034

India

Abstract

An algorithm is newly developed for keyed hash functions using Landau-Ramanujan constant. It is tested well for message authentication and digital signatures. The security analysis on this algorithm is compared with [1] and then the algorithm passes validation tests.

Keywords : HMAC, Hash functions, keying hash functions, Landau-Ramanujan constant.

1. Introduction

When two parties exchange information each other over insecure channel, keyed hash function used to avoid for tampering information. For that, many algorithms like keyed hash functions [1], hash based message authentication codes (HMAC) [2], keyed-MD5 [8], Keyed/Unkeyed RIPEMD [13], etc., are used for message authentication. Apart from these algorithms, in this paper a new keyed hash function is based on Landau-Ramanujan constant [9] and hyperbolic function which are efficient in security analysis. For validation, the proposed algorithm passes 3 primary

*E-mail: asuganya@sets.org.in

†E-mail: vijayarangan_n@rediffmail.com, vijayarangan_2005@yahoo.com