New Hash Function Based on Chaos Theory (CHA-1)

**Mahmoud Maqableh, Azman Bin Samsudin and Mohammad A. Alia** *mahmoud\_m@cs.usm.my azman@cs.usm.my mohahmadalia.cod05@student.usm.my*

School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia

# Summary

Cryptographic hash function has been used extensively in many cryptographic protocols. Many of the hash functions generate the message digest thru a randomizing process of the original message. Subsequently a chaos system also generates random behavior, but at the same time a chaos system is completely deterministic. In this paper, we propose a new hash function (CHA-1) based on chaos, which produces 160-bit hash digest, accepts message length less than 280 bits, and has a security factor 280 of brute-force attack.

***Key words:***

Hash Functions, SHA-1, Chaos Theory, Logistic Map and Collision Search Attacks.

# Introduction

Secure Hash Algorithm (SHA-1) was issued by the National Institute of Standards and Technology in 1995 as a FIPS [1]. Hash functions such as SHA-1 are normally used as data integrity primitive in more complicated cryptographic protocols. SHA-1 is one of the most popular hash functions, which accepts message with length less than 264 bits and generates 160-bit message digest. SHA-1 has been adopted by many institutions, deployed as an important component in various cryptographic schemes, as well as being implemented in most commercial security systems and products.

Lately there has been significant advancement in the analysis of hash function. In February 2005 SHA-1, has been compromised when a new way of finding collisions in [SHA-1](http://en.wikipedia.org/wiki/SHA-1) was discovered [2]. From the report, collisions in SHA-1 can be found with less than 269 hash operations. Later, in August 2005, another group of cryptanalysis scientists discovered an improved attack on SHA-1; this time the complexity of the new attack is claimed to be 263

[3].

Many studies on digital chaotic cryptographic have been proposed [4-8]. Chaos system has attracted much attention in the field of cryptography due to its properties such as deterministic and sensitive to the initial values. As indicated earlier in previous paragraphs, researchers are urgently looking for new hash function that might be able to replace SHA-1. In this paper, we are proposing a new hash function, Chaos Hash Algorithm 1 (CHA-1), which is based on chaos theory. CHA-1 accepts message with length less than 280 bits and produces unique message digest of length 160-bit.

The new proposed hash function appears to have benefited from the chaotic nature of the chaos system. One glaring benefit of chaos based crypto primitives is that the ordinary cryptanalysis methods are not applicable anymore. The current state of the art in cryptanalysis employs many different methods such as statistical analysis and brute force exhaustive search. However, such cryptanalysis methods cannot be applied to chaos cryptosystem, because of the random nature and the unpredictability of chaos functions. Brute force will not work either if the chaos based crypto primitives employ a huge key space in its implementation.

# Logistic Map

Hash function is almost similar to a pseudo random number generator in terms of the randomized output required. Therefore, a dynamic system like chaos is very suitable to be used as the engine for a hash function. However, not all chaotic maps are suitable for cryptographic purposes. Among the promising chaotic maps that can be used for cryptographic purposes is the Logistic Map which we had used in our implementation.

|  |
| --- |
|  02 |

Logistic Map is simple, fast, sensitive to the initial conditions, unpredictable and it is a one-way-function. Logistic Map is a recursive function which takes a real