Second Preimage Attack on a Chaos-Based Hash Function Construction and Its Improvement

Zahra Hajibabaei and Mohammad Dakhilalian

Abstract Hash functions play an important role in cryptography. Recently, Hash functions based on chaotic map are attracting more and more attention. In 2005, Kwok and Tang proposed a chaos-based cryptographic hash function. Five years later, Deng and Xiao showed that this algorithm has low collision resistance and it does not have good diffusion and confusion property. Then, based on the weakness of this algorithm, they improved it and introduced the second version of the original algorithm. In this paper, we show that both algorithms: the first algorithm and the second version of the algorithm have the same weaknesses and they are not second preimage resistance. Then, we improve the second version of the algorithm and show that this algorithm has good confusion and diffusion property such as the second version of the original algorithm.

1 Introduction

Hash functions take a message as input with arbitrary length and produce an output with fixed length as hash value. Most widely used hash functions are dedicated hash functions such as MD5 [1], SHA1 [2], RIPEMD [3] and HAVAL [4] which are derived from MD4 [5]. Recently, it has been shown that these algorithms are not collision resistance [6–8]. Because of the weaknesses of these algorithms, researchers have been working to develop new and more secure hash functions. One direction is the development of chaos based hash function. Chaos based hash function is attracting more and more interest due to the characteristics of chaos such as sensitivity to initial value, random-like behavior [9], and some hash functions based on chaotic maps such as tent map [10], piecewise linear map [11], logistic map [12] are proposed.

Z. Hajibabaei (✉) · M. Dakhilalian
Isfahan University of Technology, P.O. Box: 84156-83111, Isfahan, I.R. Iran
e-mail: z.hajibabaei@ec.iut.ac.ir

S.G. Stavrinides et al. (eds.), *Chaos and Complex Systems*,
DOI 10.1007/978-3-642-33914-1_17, © Springer-Verlag Berlin Heidelberg 2013