Available online at www.sciencedirect.com
SCIENCE DIRECT®
Chaos, Solitons and Fractals 23 (2005) 413–419
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

A novel method for designing S-boxes based on chaotic maps

Guoping Tang [a,b], Xiaofeng Liao [a,*], Yong Chen [a]

[a] Department of Computer Science and Engineering, Chongqing University, Chongqing 400030, China
[b] Logistical Engineering University of PLA, Chongqing 400016, China

Accepted 5 April 2004

Abstract

A method for obtaining cryptographically strong 8×8 S-boxes based on chaotic maps is presented and the cryptographical properties such as bijection, nonlinearity, strict avalanche criterion, output bits independence criterion and equiprobable input/output XOR distribution of these S-boxes are analyzed in detail. The results of numerical analysis also show that the S-boxes proposed are of the above properties and can resist the differential attack. Furthermore, our approach is suitable for practical application in designing cryptosystem.

1. Introduction

The substitution boxes (S-boxes) have been extensively used in almost all conventional cryptographic systems, such as the Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and the Advanced Encryption Standard (AES), and so on, which are core component of a DES-like cryptosystem and provide the cryptosystem with the confusion property described by Shannon in his classic paper [1]. They are the only nonlinear component of these ciphers and determined the strength of these cryptosystems. Therefore, the construction of cryptographically strong S-boxes is an important concern in design of secure cryptosystems and the study of S-box has also accelerated the development of block ciphers to a great extent. Mathematically, an $n \times m$ S-box is a nonlinear mapping from V_n to V_m, where V_n and V_m represent the vector spaces of n and m tuples of elements from GF(2) respectively. There are a number of papers published by researchers from around the world over the past decade. The significance of researching into S-boxes is also indicated in this papers [2–8].

In [6], Adams and Tavares proposed a design methodology for $n \times n$ S-boxes. It is an exhaustive search method. With the increase of n, the performance of such a procedure will become very difficult. After the appearance of differential cryptanalysis [11], Detombe and Tavares [4] made use of near-bent Boolean functions of five variables to create 5×5 S-boxes so as to resist the differential attack. Their algorithm is useful only to constructing S-boxes whose input bit number is odd. Yi et al. show a method for obtaining cryptographically strong S-boxes, which is based on a "mini version" of a block cipher with block size 8 bits and can be easily and efficiently performed on computer. To the best of our knowledge, there is only one approach for obtaining S-boxes based on chaos [9]. By using chaotic map, Jakimoski and Kocarev have proposed a four-step method to create S-box. Their approach includes the choosing a chaotic map, the discretizing the chaotic map, key scheduling and cryptanalysis and an example is presented.

All previous methods for obtaining S-boxes severely rely on finding m appropriate Boolean functions of n bits and setting them as the output bits of the $m \times n$ S-box.

* Corresponding author. Tel.: +86-23-65103190; fax: +86-23-65104570.
E-mail address: xfliao@cqu.edu.cn (X. Liao).

0960-0779/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2004.04.023

In this paper, a new method for obtaining cryptographically strong 8×8 S-boxes based on iterating chaotic maps is presented. According to the perfect properties of sensitive dependent on initial condition and system parameter of the chaotic system, it is easy and convenient to obtain a class of "good" S-box with changing the initial or system parameter slightly. The method is composed of two steps: First, by iterating a chaotic map, a 8-bit sequence of binary random variables is generated from a real value trajectory obtained and turn it to a decimal integer on the range of 0–2^n, then a integer table can be obtained. Second, a key-dependent permuting is used to shuffle the table nonlinear by a Bake map. The shuffled table is the desirable S-box.

The remaining part of this paper is as follows. In Section 2, the approach to generate a random binary sequence from iterating a chaotic map, which can be seen as a Boolean function is introduced. The criteria for a "good" $n \times n$ bit S-box and the proposed method for obtain strong S-box is described in Sections 3 and 4, respectively while the properties analysis are made in Section 5. Finally, conclusions are drawn in Section 6.

2. The Boolean function based on chaotic map

Boolean function is function that returns values 0 or 1. Generally, one takes a sequence of bits as input, produces 1 bit as output. In [10], Three approaches to generate a sequence of independent and identically distributed (i.i.d.) binary random variables from a class of ergodic chaotic maps were proposed, which can be seen as a Boolean function. Moreover, the statistical properties of the generated binary sequences and the sufficient condition for this class of chaotic maps were discussed. By the results of Kohda and Tsuneda [10], the Logistic map

$$\tau(x) = \mu x(1-x), \quad x \in I = [0,1] \tag{1}$$

is an ergodic chaotic map with many perfect properties, such as absolutely continuous invariant (ACI) measure property, equidistributivity property, symmetric property. These properties are significant in generating a sequence of independent and identically distributed binary random variables. In this paper, we use the following method to obtain a random binary sequence:

Denoting the a floating point number x as

$$x = 0.b_1(x)b_2(x)\ldots b_i(x)\ldots, \quad x \in [0,1], \;\; b_i(x) \in \{0,1\}. \tag{2}$$

The ith bit $b_i(x)$ can be expressed as

$$b_i(x) = \sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{(r/2^i)}(x), \tag{3}$$

where $\Theta_t(x)$ is a threshold function which is defined as

$$\Theta_t(x) = \begin{cases} 0 & x < t \\ 1 & x \geqslant t. \end{cases} \tag{4}$$

As a result, a binary sequence $B_i^n = f(x) = \{b_i(\tau^n(x))\}_{n=0}^{\infty}$ (where n is the length of the sequence and $\tau^n(x)$ is the nth iteration of the Logistic map) can be obtained, which it is composed of independent and identically distributed binary random variables [10]. The map f can be seen as a Boolean function. Therefore, when a real value x is input, a truth value 0 or 1 can be obtained correspondingly.

3. Criteria for a "good" $n \times n$ bit S-box

In [6], some important properties, which are necessary for cryptographically "good" S-boxes, are chosen as design criteria for a $n \times n$ S-box. In order to resist the differential attack, an expanded S-box design criteria that equiprobable input/output XOR distribution is introduced. So, we have chosen five properties that are necessary for general cryptographically "good" S-boxes. They include:

i. bijective;
ii. nonlinearity;
iii. strict avalanche criterion (SAC);
iv. output bits independence criterion (BIC);
v. equiprobable input/output XOR distribution.