一类基于混沌函数的分组密码的安全性评估*

张文涛+, 卿斯汉, 吴文玲

(中国科学院 软件研究所,北京 100080)
(中国科学院 信息安全技术工程研究中心,北京 100080)

Security Evaluation for a Class of Block Ciphers Based on Chaotic Maps

ZHANG Wen-Tao+, QING Si-Han, WU Wen-Ling

(Institute of Software , The Chinese Academy of Sciences, Beijing 100080, China)
(Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)
+ Corresponding author: Phn: 86-10-62561197 ext 8004, E-mail: zhangwt@ercist.iscas.ac.cn
http://ercist.iscas.ac.cn
Received 2001-12-19; Accepted 2002-08-02

Zhang WT, Qing SH, Wu WL. Security evaluation for a class of block ciphers based on chaotic maps. *Journal of Software*, 2003,14(3):512~517.

Abstract: The security evaluation of a class of block ciphers based on chaotic maps against differential and linear attacks is studied. If the round function is bijective and its maximum differential and linear characteristic probabilities are p and q respectively, the upper bounds of maximum differential and linear characteristic probabilities for r rounds are $p^{r-1}$and q^{r-1} respectively.

Key words: block cipher; block cipher based on chaotic maps; differential cryptanalysis; linear cryptanalysis; security evaluation

摘 要: 评估了一类基于混沌函数的分组密码(generalized Feistel structure,简称 GFS)抵抗差分密码分析和线性密码分析的能力.如果轮函数是双射且它的最大差分特征概率和线性逼近概率分别是 p 和 q,则 r 轮 GFS 的最大差分特征和线性逼近的概率分别以 p^{r-1} 和 q^{r-1} 为其上界.

关键词: 分组密码;基于混沌函数的分组密码;差分密码分析;线性密码分析;安全性评估
中图法分类号: TP309 **文献标识码**: A

随着美国 AES(advanced encryption standard)活动的展开,分组密码成为近几年来密码学研究中非常活跃的一个研究方向.在对具体算法进行安全性分析的过程中,人们积累了大量的攻击方法,其中,差分密码分析和线性密码分析是最基本和最有效的两种攻击方法.估计一个分组密码抵抗差分密码分析和线性密码分析的能力也就成为评估这个密码的安全强度的重要指标.

把混沌函数应用于分组密码的设计是一个新的、有意义的尝试.文献[1]推出了一些基于混沌函数的分组密

* Supported by the National Natural Science Foundation of China under Grant Nos.60103023, 60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810 (国家重点基础研究发展规划(973))

第一作者简介: 张文涛(1977－),女,陕西丹凤人,博士生,主要研究领域为分组密码设计与分析.

码,它们都具有相同的整体结构,本文的主要目的就是评估具有这类结构的分组密码抵抗差分密码分析和线性密码分析的能力.

1 算法的结构描述

文献[1]推出的一些基于混沌函数的分组密码都采用了一种特殊的 Feistel 网络结构,分组长度为 64 比特,运算都是面向字节的,加密过程描述如下:以 $x_{i,0},...,x_{i,7}$ 表示第 i 轮的 8 个输入字节,迭代函数为 $x_{i,k+1}=x_{i-1,k}\oplus f_{k-1}[x_{i-1,1},...,x_{i-1,k-1},k_{i-1,k-1}]$,其中,$i=1,...,r,\ k=1,...,8,\ x_8\equiv x_0, x_9\equiv x_1, k_{i,0},...,k_{i,7}$ 表示第 i 轮子密钥 k_i 的 8 个字节.函数 $f_1,f_2,...,f_7$ 具有如下形式:

$$f_j=f(x_1,...,x_j,k_j)=g(x_1\oplus...\oplus x_j\oplus k_j),$$

其中,函数 g 是由一个混沌性质好的非线性映射离散化后得到的.文献[1]给出了函数 g 的两个设计方案,并声称对应的两个分组密码算法在迭代 20 轮以后,就没有比强力攻击更好的攻击方法了.

为了研究上的方便和易行,在此,我们简化一下这种结构,设轮函数是从 4 个模块到 4 个模块的变换,把这种简化后的广义 Feistel 结构的密码记为 GFS(generalized Feistel structure).需要指出的是,这样的简化从本质上并不影响对算法安全强度的评价.

如图 1 所示是 1 轮 GFS 的加密结构,(X_0,X_1,X_2,X_3) 表示轮输入,(Y_0,Y_1,Y_2,Y_3) 表示轮输出,(K_0,K_1,K_2,K_3) 是轮子密钥,轮函数表达式如下:

$$Y_0=X_3\oplus g(X_0\oplus X_1\oplus X_2\oplus K_3),$$
$$Y_1=X_0\oplus K_0,$$
$$Y_2=X_1\oplus g(X_0\oplus K_1),$$
$$Y_3=X_2\oplus g(X_0\oplus X_1\oplus K_2).$$

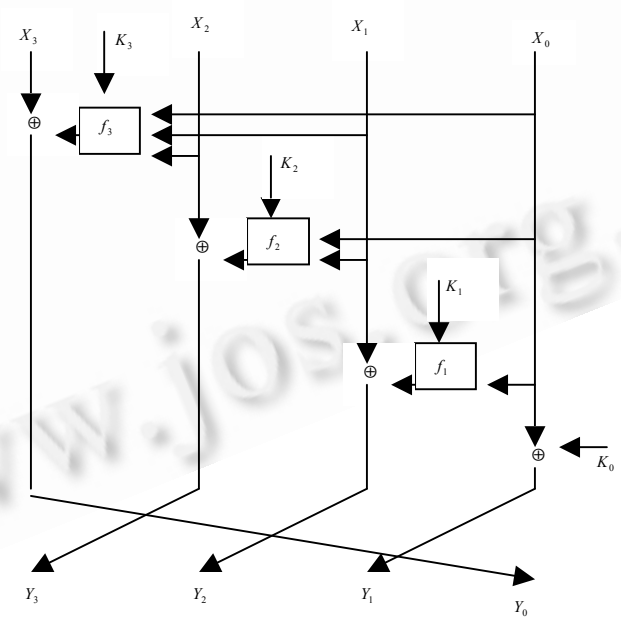

Fig.1 The structure of 1-round GFS

图 1 一轮 GFS 示意图

以下均假定函数 g 是双射,用 $(X_{i,3},X_{i,2},X_{i,1},X_{i,0})$ 和 $(\Delta X_{i,3},\Delta X_{i,2},\Delta X_{i,1},\Delta X_{i,0})$ $(0\le i\le r-1)$ 分别表示第 i+1 轮的输入和输入差分,r 是轮数.因为下面的讨论不需要用到具体的差分,我们用“1”表示不为 0 的差分,因此,输入非 0 的差分只有 15 种表示:1=(0 0 0 1),...,15=(1 1 1 1).

对分组密码抵抗差分密码分析和线性密码分析的能力的评估,现有的做法主要有下面几种:(a) 给出密码的最大的差分概率平均值和线性概率平均值的一个上界;(b) 给出密码的最大的差分特征和线性逼近的概

率;(c) 给出密码的最大的差分特征和线性逼近的概率的一个上界.因为差分概率平均值和线性概率平均值的概念比差分特征和线性逼近的概念更为准确地反映了密码抵抗差分和线性攻击的能力[2,3],因此,从理论上讲,方法(a)显得更为准确,更切入问题本质.然而,通常情况下,密码算法当轮数稍微增大一些时,找出它的能够利用的差分和线性包就非常困难了,鉴于此,Knudsen 在文献[4]中提出了实际安全的概念,即用最大的差分特征和线性逼近概率或其上界来估计算法的实际安全性.另外,对于大多数算法,当轮数增大时,密码的最大差分概率平均值和线性概率平均值要小于用方法(c)给出的最大差分特征和线性逼近概率的上界[5].因此,给出算法的最大差分特征和线性逼近概率的上界是很有意义的.

本文采用与文献[5,6]相同的方法,通过估计差分活动轮函数的最小个数,给出任意轮 GFS 类密码算法的最大差分特征和线性逼近概率的一个上界.

2 GFS 抵抗差分密码分析和线性密码分析的能力

2.1 2轮GFS

这一节中,我们用穷举的方法,列举出输入差分的每一种取值在经过两轮 GFS 后输出差分的所有可能的取值情况.

先来看输入差分为 1 时的情况:

$$1=(0\ 0\ 0\ 1)\rightarrow(1\ 1\ 1\ 1)\rightarrow\begin{pmatrix}\begin{Bmatrix}0\\1\end{Bmatrix}&\begin{Bmatrix}0\\1\end{Bmatrix}&1&\begin{Bmatrix}0\\1\end{Bmatrix}\end{pmatrix}.$$

因为轮函数是双射,所以输入差分非 0 时,输出差分一定非 0,因此第 1 轮比较清楚.对于第 2 轮,当 $\Delta X_{2,0}$ 和 $\Delta X_{2,1}$ 都不为 0 时, $g(\Delta X_{2,0})$ 和 $\Delta X_{2,1}$ 有可能相等,所以对应的 $\Delta X_{3,2}$ 有两种情况,以此类推,第 2 轮的输出应有 8 种情况.

下面我们给出输入差分的每一个取值经过 2 轮 GFS 后输出差分的所有取值情况.其中,箭头上边的数字 $u(v)$ 表示迭代 u 轮后,总共有 v 个轮函数的输入差分非 0,用后边的 $\Delta I_{i,j}$ 表示第 i 轮的第 j 个 f 函数的输入非 0:

$$1\begin{cases}\xrightarrow{2(4)}2\\ \xrightarrow{2(4)}3\\ \xrightarrow{2(4)}6\\ \xrightarrow{2(4)}7\\ \xrightarrow{2(4)}10\\ \xrightarrow{2(4)}11\\ \xrightarrow{2(4)}14\\ \xrightarrow{2(4)}15\end{cases}\Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1},\quad 2\begin{cases}\xrightarrow{2(4)}6\\ \xrightarrow{2(4)}7\\ \xrightarrow{2(4)}14\\ \xrightarrow{2(4)}15\end{cases}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2},$$

$$4\begin{cases}\xrightarrow{2(4)}14\\ \xrightarrow{2(4)}15\end{cases}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3},\quad 6\begin{cases}\xrightarrow{2(3)}6 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(3)}7 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}8 & \Delta I_{1,2}\Delta I_{2,3}\\ \xrightarrow{2(2)}9 & \Delta I_{1,2}\Delta I_{2,3}\\ \xrightarrow{2(3)}14 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(3)}15 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\end{cases},$$

$$3\begin{cases}\xrightarrow{2(2)}2 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}3 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}4 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}5 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}6 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}7 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}10 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}11 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}12 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}13 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}14 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}15 & \Delta I_{1,1}\Delta I_{2,1}\end{cases},\quad 5\begin{cases}\xrightarrow{2(3)}2 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}3 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}4 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}5 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}6 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}7 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}10 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}11 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}12 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}13 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}14 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}15 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\end{cases},\quad 7\begin{cases}\xrightarrow{2(2)}2 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}3 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}4 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}5 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}6 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}7 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}10 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}11 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}12 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}13 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}14 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}15 & \Delta I_{1,1}\Delta I_{2,1}\end{cases},\quad 11\begin{cases}\xrightarrow{2(2)}2 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}3 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}4 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}5 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}6 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}7 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}10 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}11 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}12 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}13 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}14 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}15 & \Delta I_{1,1}\Delta I_{2,1}\end{cases},$$

$$8\xrightarrow{2(3)}15\quad \Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3},$$

$$10\begin{cases}\xrightarrow{2(4)}6 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(4)}7 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(3)}8 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,3}\\ \xrightarrow{2(3)}9 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,3}\\ \xrightarrow{2(4)}14 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(4)}15 & \Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\end{cases},\quad 14\begin{cases}\xrightarrow{2(3)}6 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(3)}7 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}8 & \Delta I_{1,2}\Delta I_{2,3}\\ \xrightarrow{2(2)}9 & \Delta I_{1,2}\Delta I_{2,3}\\ \xrightarrow{2(3)}14 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\\ \xrightarrow{2(3)}15 & \Delta I_{1,2}\Delta I_{2,1}\Delta I_{2,2}\end{cases},\quad 12\begin{cases}\xrightarrow{2(1)}1 & \Delta I_{1,3}\\ \xrightarrow{2(4)}14 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3},\\ \xrightarrow{2(4)}15 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\end{cases}$$

$$9\begin{cases}\xrightarrow{2(4)}2 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}3 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}4 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,2}\\ \xrightarrow{2(4)}5 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,2}\\ \xrightarrow{2(4)}6 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}7 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}10 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}11 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}12 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,2}\\ \xrightarrow{2(4)}13 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,2}\\ \xrightarrow{2(4)}14 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\\ \xrightarrow{2(4)}15 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{1,3}\Delta I_{2,1}\end{cases},\quad 13\begin{cases}\xrightarrow{2(3)}2 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}3 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}4 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}5 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}6 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}7 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}10 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}11 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}12 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}13 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,2}\\ \xrightarrow{2(3)}14 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\\ \xrightarrow{2(3)}15 & \Delta I_{1,1}\Delta I_{1,2}\Delta I_{2,1}\end{cases},\quad 15\begin{cases}\xrightarrow{2(2)}2 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}3 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}4 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}5 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}6 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}7 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}10 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}11 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}12 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}13 & \Delta I_{1,1}\Delta I_{2,2}\\ \xrightarrow{2(2)}14 & \Delta I_{1,1}\Delta I_{2,1}\\ \xrightarrow{2(2)}15 & \Delta I_{1,1}\Delta I_{2,1}\end{cases}.$$

以上面 2 轮 GFS 的结果为基础,下面我们考虑更多轮 GFS 的情况.

2.2 4轮GFS

这一节我们以输入差分 4=(0 0 1 0)为例,来讨论 4 轮 GFS 的情况.

$$4\begin{cases}\xrightarrow{2(4)}14\begin{cases}\xrightarrow{2(3)}6 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,1}\Delta I_{4,2}\\ \xrightarrow{2(3)}7 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}8 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,3}\\ \xrightarrow{2(2)}9 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,3}\\ \xrightarrow{2(3)}14 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,1}\Delta I_{4,2}\\ \xrightarrow{2(3)}15 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,2}\Delta I_{4,1}\Delta I_{4,2}\end{cases}\\ \xrightarrow{2(4)}15\begin{cases}\xrightarrow{2(2)}2 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,1}\\ \xrightarrow{2(2)}3 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,1}\\ \xrightarrow{2(2)}4 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}5 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}6 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}7 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}10 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}11 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}12 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}13 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}14 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\\ \xrightarrow{2(2)}15 & \Delta I_{1,3}\Delta I_{2,1}\Delta I_{2,2}\Delta I_{2,3}\Delta I_{3,1}\Delta I_{4,2}\end{cases}\end{cases}.$$

为表示简单起见,如果对于集合 S 的任何一个元素 S,都有 $a\xrightarrow{u(v)}s$ 成立,就记为 $a\xrightarrow{u(v)}S$.

记集合 $C=\{2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$, $E=\{2,3,4,5,6,7,10,11,12,13,14,15\}$.

类似上面的讨论,我们可以得到

$$1\xrightarrow{4(6)}C\quad 2\xrightarrow{4(6)}C\quad 4\xrightarrow{4(6)}C\quad 6\xrightarrow{4(5)}C\quad 8\xrightarrow{4(5)}E\quad 10\xrightarrow{4(6)}C$$

$$3\begin{cases}\xrightarrow{4(3)}1\\ \xrightarrow{4(4)}C\end{cases}\quad 5\begin{cases}\xrightarrow{4(4)}1\\ \xrightarrow{4(5)}C\end{cases}\quad 7\begin{cases}\xrightarrow{4(3)}1\\ \xrightarrow{4(4)}C\end{cases}\quad 9\begin{cases}\xrightarrow{4(5)}1\\ \xrightarrow{4(6)}C\end{cases}\quad 11\begin{cases}\xrightarrow{4(3)}1\\ \xrightarrow{4(4)}C\end{cases}\quad 13\begin{cases}\xrightarrow{4(4)}1\\ \xrightarrow{4(5)}C\end{cases}$$

$12 \begin{cases} \xrightarrow{4(5)} \{2,3,6,7,10,11,14,15\} \\ \xrightarrow{4(6)} \{4,5,8,9,12,13\} \end{cases}$ $14 \xrightarrow{4(5)} C$ $15 \begin{cases} \xrightarrow{4(3)} 1 \\ \xrightarrow{4(4)} C \end{cases}$

由此,我们就可以得到下面的结论:

结论 1. 对于 4 轮 GFS,当函数 g 是双射时,至少有 3 个轮函数的输入差分非 0.

2.3 6轮GFS

首先,我们来看输入差分为 1=(0 0 0 1)的 6 轮 GFS 的情况.

当输入差分为 1 时,第 4 轮的输入差分可以是 2~15 这 14 个数字中的任何一个.从第 1 节的讨论可知,对于两轮 GFS,除过差分特征 $12 \xrightarrow{2(1)} 1$ 仅有 1 个轮函数的输入差分非 0,其他情况下至少都有两个轮函数的输入差分非 0.

存在下面的差分特征:

$1 \xrightarrow{4(6)} 12 \xrightarrow{2(1)} 1$, $1 \xrightarrow{4(6)} 3 \xrightarrow{2(2)} E$, $1 \xrightarrow{4(6)} 6 \xrightarrow{2(2)} \begin{cases} 8 \\ 9 \end{cases}$

这样,我们就可以得到

$1 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$

输入差分为其他值的情况如下:

$2 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$ $3 \begin{cases} \xrightarrow{6(5)} 1 \\ \xrightarrow{6(6)} C \end{cases}$ $4 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$ $5 \begin{cases} \xrightarrow{6(6)} 1 \\ \xrightarrow{6(7)} C \end{cases}$ $6 \begin{cases} \xrightarrow{6(6)} 1 \\ \xrightarrow{6(7)} C \end{cases}$ $7 \begin{cases} \xrightarrow{6(5)} 1 \\ \xrightarrow{6(6)} C \end{cases}$

$8 \begin{cases} \xrightarrow{6(6)} 1 \\ \xrightarrow{6(7)} C \end{cases}$ $9 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$ $10 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$ $11 \begin{cases} \xrightarrow{6(5)} 1 \\ \xrightarrow{6(6)} C \end{cases}$ $12 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(7)} C \end{cases}$ $13 \begin{cases} \xrightarrow{6(6)} 1 \\ \xrightarrow{6(7)} C \end{cases}$

$14 \begin{cases} \xrightarrow{6(6)} 1 \\ \xrightarrow{6(7)} C \end{cases}$ $15 \begin{cases} \xrightarrow{6(5)} 1 \\ \xrightarrow{6(6)} C \end{cases}$

由此,我们得到下面的结论:

结论 2. 对于 6 轮 GFS,当函数 g 是双射时,至少有 5 个轮函数的输入差分非 0.

2.4 2r轮和2r+1轮GFS

有了前 3 节的准备,我们现在可以证明下面的结论:

定理 1. 对于 2r 轮(r 是自然数)GFS,当函数 g 是双射时,至少有 2r–1 个轮函数的输入差分非 0.

证明:当 r=1,2,3 时,由前 3 节的结论可知,定理成立.当 $r \geq 4$ 时,首先,我们注意 2 轮 GFS 的以下事实:

(1) $12 \xrightarrow{2(1)} 1$,并且,除了这样的差分特征,2 轮 GFS 在其他情况下至少都有两个轮函数的输入差分非 0;

(2) 以 1 为输入差分的 2 轮 GFS,都有 4 个轮函数的输入差分非 0;

(3) $3 \xrightarrow{2(2)} \{2,3,4,5,6,7,10,11,12,13,14,15\}$, $6 \xrightarrow{2(2)} \{8,9\}$.

这样,由上面的事实,我们从 $1 \begin{cases} \xrightarrow{6(7)} 1 \\ \xrightarrow{6(8)} C \end{cases}$ 出发,对于 $r \geq 4$,可以归纳得到下面的结论:

$1 \begin{cases} \xrightarrow{2r(2r+1)} 1 \\ \xrightarrow{2r(2r+2)} C \end{cases}$

同理有

$2 \begin{cases} \xrightarrow{2r(2r+1)} 1 \\ \xrightarrow{2r(2r+2)} C \end{cases}$ $3 \begin{cases} \xrightarrow{2r(2r-1)} 1 \\ \xrightarrow{2r(2r)} C \end{cases}$ $4 \begin{cases} \xrightarrow{2r(2r+1)} 1 \\ \xrightarrow{2r(2r+2)} C \end{cases}$ $5 \begin{cases} \xrightarrow{2r(2r)} 1 \\ \xrightarrow{2r(2r+1)} C \end{cases}$ $6 \begin{cases} \xrightarrow{2r(2r)} 1 \\ \xrightarrow{2r(2r+1)} C \end{cases}$

$7 \begin{cases} \xrightarrow{2r(2r-1)} 1 \\ \xrightarrow{2r(2r)} C \end{cases}$ $8 \begin{cases} \xrightarrow{2r(2r)} 1 \\ \xrightarrow{2r(2r+1)} C \end{cases}$ $9 \begin{cases} \xrightarrow{2r(2r+1)} 1 \\ \xrightarrow{2r(2r+2)} C \end{cases}$ $10 \begin{cases} \xrightarrow{2r(2r+1)} 1 \\ \xrightarrow{2r(2r+2)} C \end{cases}$ $11 \begin{cases} \xrightarrow{2r(2r-1)} 1 \\ \xrightarrow{2r(2r)} C \end{cases}$

12 $\begin{cases}\xrightarrow{2r(2r)}1\\ \xrightarrow{2r(2r+1)}C\end{cases}$ 13 $\begin{cases}\xrightarrow{2r(2r)}1\\ \xrightarrow{2r(2r+1)}C\end{cases}$ 14 $\begin{cases}\xrightarrow{2r(2r)}1\\ \xrightarrow{2r(2r+1)}C\end{cases}$ 15 $\begin{cases}\xrightarrow{2r(2r-1)}1\\ \xrightarrow{2r(2r)}C\end{cases}$

可见,当 $r\geq 4$ 时,$2r$ 轮 GFS 也至少有 $2r-1$ 个轮函数的输入差分非 0. □

推论. 对于 $2r+1$ 轮(r 是自然数)GFS,当函数 g 是双射时,至少有 $2r$ 个轮函数的输入差分非 0.

证明:当输入差分为 8 时,所有(3 个)轮函数的输入差分都为 0.然而,当输入差分为 8 时,2 轮 GFS 有 3 个轮函数的输入差分非 0,4 轮 GFS 有 5 个轮函数的输入差分非 0,对任何 $r\geq 4$,都有 8 $\begin{cases}\xrightarrow{2r(2r)}1\\ \xrightarrow{2r(2r+1)}C\end{cases}$ 成立,而 $2r+1$ 轮 GFS 的非 0 轮函数的个数总是不小于 $2r$ 轮 GFS 的非 0 轮函数个数,因此,当输入差分为 8 时,推论成立.

当输入差分为其他值时,1 轮 GFS 至少有 1 个轮函数的输入差分非 0,由定理 1,推论成立.

由于差分密码分析和线性密码分析两种方法的对称性和联系,对于 GFS 抵抗线性密码分析的讨论有类似的结果成立. □

由定理 1 及其推论,可得如下结果:

定理 2. 如果函数 g 是双射且它的最大差分特征和线性逼近的概率分别是 p 和 q,则 r 轮 GFS 的最大的差分特征和线性逼近的概率分别以 p^{r-1} 和 q^{r-1} 为其上界.

3 小结和讨论

差分密码分析和线性密码分析是目前对分组密码最有效的攻击方法,因此,每个分组密码设计者都要想办法估计算法抵抗差分和线性密码分析的能力.本文对一类基于混沌函数的分组密码(GFS)抵抗差分密码分析和线性密码分析的能力作了估计:如果轮函数是双射且它的最大差分特征和线性逼近的概率分别是 p 和 q,则 r 轮 GFS 的差分和线性特征概率的上界为 p^{r-1} 和 q^{r-1}.这样,对于该类结构的密码,只需确定轮函数的密码特性就能估计出整个算法抵抗差分密码分析和线性密码分析的能力.

进一步地,在 GFS 结构中,如果轮函数采取 S-P 网络,对这种结构的密码算法抵抗差分密码分析和线性分析的能力进行评估,我们发现,采取类似的方法非常困难.那么,是否存在其他方法,可以对这类结构的密码算法的安全性进行很好的评估?这可以留待今后进一步加以研究和分析.

References:

[1] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems-1: Fundamental Theory and Applications, 2001,48(2):163~169.

[2] Lai X, Massey JL, Murphy S. Markov ciphers and differential cryptanalysis. In: Rueppel RA, ed. Advances in Cryptology——EUROCRYPT'91. LNCS 547, Berlin: Springer-Verlag, 1991. 17~38.

[3] Nyberg K. Linear approximation of block ciphers. In: De Santis A, ed. Advances in Cryptology——EUROCRYPT'94. LNCS950, Berlin: Springer-Verlag, 1995. 439~444.

[4] Knudsen LR. Practically secure Feistel ciphers. In: Anderson R, ed. Fast Software Encryption. LNCS 809, New York: Springer-Verlag, 1994. 211~221.

[5] Kanda M. Practical security evaluation against differential and linear attacks for Feistel ciphers with SPN round function. In: Stinson DR, ed. Proceedings of the 7th Annual Workshop on Selected Areas in Cryptography. New York: Springer-Verlag, 2000. 168~179.

[6] Hong S, Lee S, Lim J, Sung J, Cheon D. Provable security against differential and linear cryptanalysis for the SPN structure. In: Schneier B, ed. Fast Software Encryption 2000. LNCS 1978, New York: Springer-Verlag, 2000. 273~283.