# 一种结合离散混沌映射和 Feistel 网络的分组加密算法

彭 军[①②] 廖晓峰[②] 岡本栄司[③] 张 伟[④] 李学明[②]
[①](重庆科技学院电子信息工程学院 重庆 400050)
[②](重庆大学计算机科学与工程学院 重庆 400044)
[③](日本筑波大学系统与情报工学研究科 日本 305-8573)
[④](重庆教育学院计算机与现代教育技术系 重庆 400067)

**摘 要** 论文提出了一种新颖的结合一维离散混沌映射与Feistel网络结构的分组密码算法(CFCEA)。分组长度为 64 bit，密钥长度为 128bit，并使用了一个 128bit长的辅助密钥。在轮函数中用Logistic混沌映射和 3 个代数群算子进行混合运算，此外还特别设计了子密钥生成算法。对CFCEA的密码学特性进行了分析，结果表明该算法具有严格的雪崩效应，扩散性能和扰乱性能理想。并且算法在 64bit分组长度下差分概率和线性概率的理论上界分别近似为 $2^{-52.92}$和 $2^{-49.206}$，具备抵抗一定强度的差分和线性密码分析的能力。

**关键词** 分组密码，Logistic 混沌映射，Feistel 网络，差分和线性密码分析
**中图分类号**：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2006)04-0707-05

# A Block Encryption Algorithm Combined with the Discrete Chaotic Map and Feistel Network

Peng Jun[①②] Liao Xiao-Feng[②] Okamoto Eiji[③] Zhang Wei[④] Li Xue-Ming[②]
[①](*Department of Electronic Information Engineering, Chongqing University of Science and Technology, Chongqing* 400050, *China*)
[②](*Department of Computer Science and Engineering, Chongqing University, Chongqing* 400044, *China*)
[③](*Graduate School of Systems and Information Engineering, University of Tsukuba, Ibaraki* 305-8573, *Japan*)
[④](*Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing* 400067, *China*)

**Abstract** In this paper a novel block encryption algorithm, which is called CFCEA, is proposed by combining the one dimensional discrete chaotic map and Feistel network. The algorithm operates on 64bit plaintext blocks, and the master key is 128 bit long, and an auxiliary key with size of 128 bit is exploited. Within the round function, the logistic chaotic map and three algebraic group operations are mixed. Moreover, the subkeys schedule is specially designed for the consideration of the security. The cryptographic properties of the algorithm are analyzed, and the results indicate that this algorithm satisfies the strict avalanche criterion and as a result, the diffusion and confusion properties of the algorithm are very ideal. Furthermore, when the block length is 64bit, the approximately upper bound of differential probability and linear probability of CFCEA is $2^{-52.92}$ and $2^{-49.206}$, respectively. This shows that the algorithm can resist differential and linear cryptanalysis with some strength.

**Key words** Block cipher, Logistic chaotic map, Feistel network, Differential and linear cryptanalysis

## 1 引言

混沌理论已经在物理、数学、化学、生物、经济和工程等众多领域得到了广泛的深入研究。从 90 年代初期开始，混沌理论在保密通信和密码学中的应用研究也逐渐展开并引起了普遍关注。由于混沌信号是由确定性方程产生的，具有类随机、宽频谱、对初值条件极端敏感等固有特性，表现出复杂的动力学行为并且对混沌信号难以长期预测。这些特性使得混沌系统具有非常广阔的应用前景。90 年代初期Pecora和Carroll[1,2]首次使用混沌自同步理论实现了两个相同混沌系统之间的保密通信，而几乎是同一时期Matthews[3] 首次报道了混沌序列密码方面的研究成果。此后相继出现了许多基于混沌的加密算法或系统，如基于混沌同步的加密系统[4,5]、混沌序列密码[6-8]、混沌分组密码[9-11]和混沌图像加密[12-14]等。

我们知道，在设计加密算法时有几类网络结构被经常使用，它们是 Feistel 网络(如 DES，FEAL，TWOFISH，LOKI97，GOST)，变型 Feistel 网络(如 RC5，MISTY2，CAST-256)以及 SP 网络(如 IDEA，Rijndael，SAFER)。本文则给出一个基于 Logistic 混沌映射并采用 Feistel 网络结构的分组加密算法，分组长度为 64bit，主密钥长度为 128bit，此外还使用了一个长度为 128bit 的辅助密钥，算法共有 16 轮。简要地讲，此类结构的加密算法就是通过一个轮函数 $F$ 多次作用于明

2004-08-23 收到，2005-01-04 改回
国家自然科学基金(60573047)，重庆市科委自然科学基金(GSTC，2005BB2050)和重庆市教委科学技术研究项目基金(KJ051402)资助课题

文分组而得到相应的密文分组。设一个 $r$ 轮的 Feistel 结构加密算法，分组长度为 $2n$ bit，每轮的操作可形式地定义如下：

$$\text{Round}_i : L_{i-1} \| R_{i-1} \mapsto R_i \| F(Z_i, R_{i-1}) \oplus L_{i-1}$$

其中 $i = 1,2,\cdots,r$ ， $L_i$ 和 $R_i$ 分别是分组的左右两个部分，长度均为 $n$ bit。 $Z_i$ 为第 $i$ 轮使用的子密钥，由主密钥 $Z$ 按照某种算法产生。函数 $F$ 为加密算法的核心部件，应该是非线性的，一般有两个长度为 $n$ bit 的参数。在函数 $F$ 中我们加入了混沌机制，由于混沌具有如前所述的固有特性，因此将导致 $F$ 的非线性行为更加复杂和难以预测。

Logistic映射是研究得最多的一维离散映射，虽然形式简单，但其动力学行为却是很复杂的[15]。Logistic映射定义如下：

$$y_{i+1} = \mu y_i (1 - y_i), \quad 0 \le y_i \le 1 \tag{1}$$

式中 $\mu$ 为系统参数，当 $\mu$ 取不同值时将表现出不同的动力学行为，如 $3 < \mu < 4$ 时出现倍周期分叉和奇数周期等现象，而 $\mu = 4$ 时则处于完全混沌状态。在我们的加密算法中则利用了参数 $\mu = 4$ 时的混沌映射。

据我们所知，同时结合离散混沌映射和 Feistel 网络结构的分组加密算法还少有报道，本文在这方面则进行了一些有意义的研究工作。

## 2 加密算法描述

为便于叙述，本文算法简称为CFCEA(Chaotic Map and Feistel Network Combined Block Encryption Algorithm)。在设计该算法时，我们遵循了如下一些准则：(1) 在函数 $F$ 中使用 3 个代数群算子进行混合运算，它们分别是 16 位“异或”，模 $2^{16}$加，模 $2^{16}$+1 乘(这个思想类似于IDEA[16]，但我们用的是Feistel网络，而非SP网络)；(2) 每轮中的 4 个子密钥都要直接或间接地与两个输入子分组进行某种运算，以达到每个子密钥都将显著地影响输出子分组的效果；(3) 加入混沌机制，提高加密系统复杂性；(4) 算法能支持 128bit长度的密钥；(5) 由子密钥推测出主密钥是困难的。

图 1 给出了我们设计的CFCEA算法的整体描述。整个算法共有 16 轮，每轮都使用了一个子密钥 $Z_{(i)}$ (含有 4 个分量，均由主密钥导出)。此外，为了增强算法的安全性能，我们还采用了辅助密钥的概念[17]，设( $AZ_H$ , $AZ_L$ )为长度为 128bit 的辅助密钥，先用 $AZ_H$ 与明文分组进行“异或”，然后开始 16 轮迭代，迭代输出后的分组再与 $AZ_L$ 进行“异或”。

### 2.1 函数 $F$ 结构

函数 $F$ 的内部结构如图 2 所示。该函数将 2 个 16bit输入子分组 $X_1$ 和 $X_2$ 变换为 2 个 16bit输出子分组 $Y_1$ 和 $Y_2$，4 个长度为 16bit的子密钥 $Z_{k(r)}$ 分别与函数的输入值或中间运算结果进行 16bit“异或”或者 16bit模 $2^{16}$加，其中第 $r$ 轮子密钥 $Z_{k(r)}$ 由主密钥 $Z = Z_1 Z_2 \cdots Z_{16}$ 按照 2.2 节的算法生成。我们注意到，基于Logistic混沌映射的变换函数 $G$ 两次参与了函数 $F$ 的内部运算，目的是增加扰乱(Confusion)和扩散

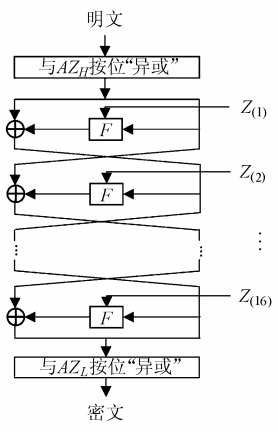


图 1 CFCEA 算法

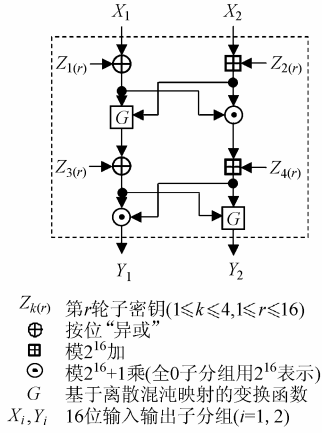


图 2 函数 $F$

(Diffusion)效果。变换函数 $G$ 定义如下：

(1) 输入参数 $p_1$ 和 $p_2$ (均为 16bit 整数)；

(2) 计算 $X_s = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_{16}$ 和 $N_s = \left(Z_1 + Z_2 + \cdots Z_{16}\right) \bmod 256 + C$ ，其中 $C$ 是一个任意选定的固定常数；

(3) 计算 $N = N_s + \tilde{p}_1$ ， $y_0 = ((X_s + p_2) \bmod 2^{16})/(2^{16}+1)$ ，$\tilde{p}_1$ 由 $p_1$ 右移 8bit 得到；

(4) 以 $y_0$ 为初值，对式(1)迭代 $N$ 次(参数 $\mu = 4$ )；

(5) 输出 $y_N \leftarrow \text{floor}(y_N 2^{16})$ (16bit 整数)。

### 2.2 子密钥生成算法

子密钥和主密钥之间的关系应该是复杂的，也就是说试图从子密钥猜测出主密钥是很困难的，为此我们对主密钥进行了特定的变换。设主密钥 $Z = Z_1 Z_2 \cdots Z_{16}$ ，用图 3 所示的函数 $R$ 对 $Z$ 连续迭代 8 次，输出仍为 128bit，记为 $Z^*$ 。CFCEA 算法有 16 轮，总共需要 64 个子密钥，每一轮使用 4 个，子密钥的长度为 16bit。第 1 轮子密钥的产生方式如下：将 $Z^*$ 循环左移 13bit 得到 $Z_{(1)}$ ，按从高位到低位的顺序依次选取 4 个长度为 16bit 的子密钥 $Z_{1(1)}$ ， $Z_{2(1)}$ ， $Z_{3(1)}$ 和 $Z_{4(1)}$ 。对 $Z_{(1)}$ 作类似处理就可以得到第 2 轮的子密钥 $Z_{k(2)}$ ( $k = 1,2,3,4$ )，如此进行下去就可以生成所有 16 轮子密钥。

下面对函数 $R$ 进行说明。输入为 $S_i$ ($i = 1,2,\cdots,16$) ， $S_i$ 与 $S_i \oplus S_{i+1}$ (当 $i = 16$ 时为 $S_{16} \oplus S_1$ )作为 2 个参数输入到另外一个函数 $H$ 中(与混沌映射有关)，于是可以得到 16 个值，再经过第 $k$ 个置换函数的作用，输出为 $T_i$ ($i = 1,2,\cdots,16$) ，其中 $k$ 取值与函数 $R$ 的迭代顺序号相同。这 8 个置换函数可参考文献[18]，实际上他们是大小为 16×16 的 S 盒。函数 $H$ 类似

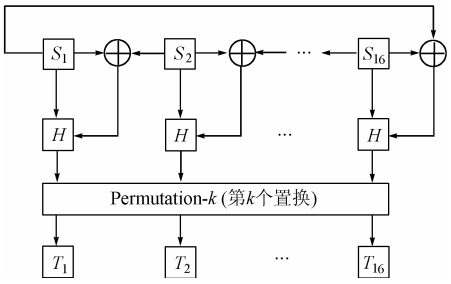


图 3 函数 $R$

于函数 $G$，都是基于离散混沌映射的。此处只给出不同之处：函数 $H$ 处理的均是 8bit 整数情形，即

$$N = N_s + p_1, \quad y_0 = ((X_s + p_2) \bmod 2^8)/(2^8+1),$$
$$y_N \leftarrow \text{floor}(y_N 2^8)$$

并且用 $S_i$ 替换了函数 $G$ 中的 $Z_i$。

### 2.3 解密过程

采用 Feistel 结构的分组密码有一个特性，就是加密解密可以使用相同的算法结构，并且函数 $F$ 可以设计得非常复杂甚至不要求它是可逆的，因为 Feistel 网络的结构特点保证了分组加密算法的可逆性，即

$$R_i \oplus F(L_i, Z_{(i)}) = (L_{i-1} \oplus F(R_{i-1}, Z_{(i)})) \oplus F(R_{i-1}, Z_{(i)}) = L_{i-1}$$

唯一不同的是子密钥的使用顺序与加密时相反。

## 3　实验结果

我们采用 MATLAB V6.1 对 CFCEA 算法进行了实验，实验数据如下：

明文 $m_1$ =The applications of chaotic map to secure communications have received a great deal of attention

明文 $m_2$ =Uhe applıcations!of chaouic map uo securf communjcations!have redeived a!great dfal of autention

辅助密钥 $az$ =Kai$sbHR4kaEtb7Q　　主密钥 $mz_1$ = Hd2%t5^bfe3&nwYe

主密钥 $mz_2$ =Hd2%t5^bfe3&nwYf　　主密钥 $mz_3$ = Gd2%t5^bfe3&nwYe

其中明文 $m_2$ 与 $m_1$ 只在每个分组的首字符不同( $m_2$ 比 $m_1$ 的 ASCII 码值大 1，并用下划线标记)，3 个主密钥之间也只是在首字符或尾字符不同(ASCII 码值相差 1)。实验时辅助密钥都取相同值，结果见图 4 所示。

我们用符号 $f(m,mz)$ 表示用主密钥 $mz$ 对明文 $m$ 进行加密得到的密文，并考察他们之间的 ASCII 码值的差。图 4(a)为 $f(m_1,mz_1)$ 与 $m_1$ 之差，可看出密文与明文之间的差异是巨大的；图 4(b)为 $f(m_1,mz_1)$ 与 $f(m_1,mz_2)$ 之差，而图 4(c)为 $f(m_1,mz_1)$ 与 $f(m_2,mz_1)$ 之差，表明密钥或明文的微小差异将导致密文的显著变化，体现了算法对密钥和明文的敏感性。同时这种敏感性会使得唯密文攻击变得非常困难，例如使用与 $mz_1$ 有微小差异的密钥 $mz_3$ (只有首字符不同) 对密文 $f(m_1,mz_1)$ 进行解密，从图 4(d) (为解密明文与原文之差)可看出，解密得到的明文与原文 $m_1$ 是完全不同的。

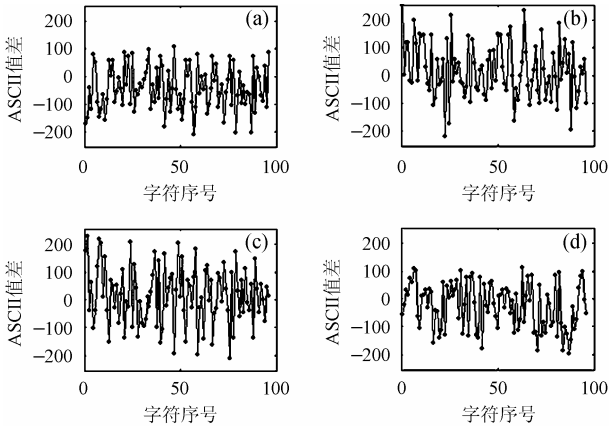


图 4　实验结果

## 4　讨论

### 4.1 扩散和扰乱特性

Shannon在其经典文章[19]中曾提出了两个用于指导密码设计的基本原则，即扩散(diffusion)和扰乱(confusion)。扩散就是将明文冗余度分散到密文中使之分散开来，以便隐藏明文的统计结构，实现方式是使得明文的每一位影响密文中多位的值。扰乱则是用于掩盖密钥和密文之间的关系，使密钥和密文之间的统计关系变得尽可能复杂，导致密码攻击者无法从密文推出密钥。

Kocarev等人指出[20]，混沌的轨道混合特性对应于传统加密系统的扩散特性，而混沌信号的类随机特性和对系统参数的敏感性则相当于传统加密系统的扰乱特性。因此，我们在轮函数 $F$ 和子密钥生成算法中都引入了混沌映射，有望获得与传统加密算法一样好的扩散和扰乱效果。

“雪崩效应”由Feistel提出[21]，可以用来表达加密算法所蕴涵的扩散和扰乱性能。一个严格的“雪崩效应”应是：当有一位输入位发生改变时，输出位将有一半要发生改变。

**定义 1**　称一个分组中 bit1 的个数为该分组的汉明权重，记为 HW 。

**定义 2**　$e_i^n$ 代表第 $i$ 个位置为 1(其余位置全为 0)的 $n$ bit 长度的单位向量($1 \le i \le n$)。

为考察 CFCEA 算法的“雪崩效应”，我们计算如下 4 个值(在不同执行轮数下)：

(1) 明文分组为 $e_i^{64}$，设 $f(e_i^{64}, mz_t)$ 的汉明权重为 $\text{HW}_i^1$，其中 $f(e_i^{64}, mz_t)$ 表示对 $e_i^{64}$ 使用主密钥 $mz_t$ 进行加密得到的密文(以下解释相同)，$mz_t$ 随机选取，$1 \le t \le T$，$T$ 为主密钥个数。计算平均值

$$\text{HW}^1 = \frac{1}{64}\sum_{i=1}^{64}\text{HW}_i^1 \tag{2}$$

(2) 任意选定一个非零的明文分组 $m_1$，设 $f(m_1, mz_t) \oplus f(m_1 \oplus e_i^{64}, mz_t)$ 的汉明权重为 $\text{HW}_{i,t}^2$。计算平均值：

$$\text{HW}^2 = \frac{1}{64}\sum_{i=1}^{64}\left(\frac{1}{T}\sum_{t=1}^{T}\text{HW}_{i,t}^2\right) \tag{3}$$

(3) 明文分组 $m_1$ 为全零，主密钥 $mz_1$ 也为全零，设 $f(m_1, mz_1) \oplus f(m_1, mz_1 \oplus e_i^{128})$ 的汉明权重为 $\text{HW}_i^3$。计算平均值：

$$\text{HW}^3 = \frac{1}{128}\sum_{i=1}^{128}\text{HW}_i^3 \tag{4}$$

(4) 明文分组 $m_1$ 为全零，但主密钥 $mz_1$ 非零，设 $f(m_1,mz_1)\oplus f(m_1,mz_1\oplus e_i^{128})$ 的汉明权重为 $\mathrm{HW}_i^4$。计算平均值

$$\mathrm{HW}^4=\frac{1}{128}\sum_{i=1}^{128}\mathrm{HW}_i^4 \tag{5}$$

计算时 $T$ 取值200(即考虑随机选取200个主密钥时的统计结果)，执行轮次从 1 到 16，4 个汉明权重平均值 $\mathrm{HW}^i(1\le i\le 4)$ 的计算结果如图 5 所示。我们对结果进行分析，发现算法在执行 3 轮之后汉明权重均值就非常接近于 32 了，并且 $\max_{1\le i\le 4}|\mathrm{HW}^i/64-0.5|$ 的值为 0.0075 (3 轮之后)，也就是说如果改变明文或主密钥的一位都将导致密文近一半的位发生变化，表明 CFCEA 算法具有严格的“雪崩效应”。由此可知算法对明文和密钥的扩散和扰乱性能是非常理想的。

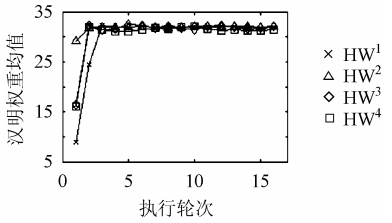


图 5 雪崩效应

CFCEA算法的内部细节可以公开，其安全性完全依赖于密钥的安全，足够长的密钥可提供算法抵抗穷举攻击的能力。CFCEA算法的主密钥有 128bit，辅助密钥也是 128bit，密钥的组合达到 $2^{256}\approx 1.16\times 10^{77}$种可能，因此以当前的计算能力还暂时无法对CFCEA算法成功实施诸如密钥穷举攻击、字典攻击和密钥匹配等类型的强力攻击。但自从Biham-Shamir[22,23]引入差分密码分析和Matsui[24]引入线性密码分析之后，攻击像DES之类的密码使用上述两种分析方法比穷举攻击等更为有效。从算法的分类上看，我们的算法属于DES之类的迭代型密码(主要区别是在 $F$ 函数中用 3 个代数群算子的混合运算和混沌映射组件替换了DES中相应的S-盒)，因此对CFCEA算法进行差分和线性密码分析是很有必要的。

**定义 3** 设函数 $F:\mathrm{GF}(2)^m\to\mathrm{GF}(2)^n$，对给定的 $\Delta x,\Gamma x\in\mathrm{GF}(2)^m$ 和 $\Delta y,\Gamma y\in\mathrm{GF}(2)^n$，函数 $F$ 的差分概率和线性概率分别定义如下：

$$\mathrm{DP}^F(\Delta x\to\Delta y)=\#\{x\in\mathrm{GF}(2)^n\mid F(x)\oplus F(x\oplus\Delta x)=\Delta y\}/2^n \tag{6}$$

$$\mathrm{LP}^F(\Gamma x\to\Gamma y)=(\#\{x\in\mathrm{GF}(2)^n\mid x\Gamma x=F(x)\Gamma y\}/2^{n-1}-1)^2 \tag{7}$$

其中 $\#\{S\}$ 表示集合 $S$ 中的元素个数，而 $xy=\oplus_{i=0}^{n-1}(x_iy_i)$，即 $xy$ 表示 $x$ 与 $y$ 按位相乘后得到的数的奇偶(奇为 1，偶为 0)。

**定义 4** 函数 $F$ 的最大差分概率和最大线性概率分别定义如下：

$$p=\max_{\Delta x\ne 0,\Delta y}\mathrm{DP}^F(\Delta x\to\Delta y),\quad q=\max_{\Gamma x,\Gamma y\ne 0}\mathrm{LP}^F(\Gamma x\to\Gamma y) \tag{8}$$

Nyberg 和 Knudsen 在文献[25]中已经证明：如果一个基于 Feistel 结构的分组加密算法具有 $\mathrm{GF}(2)^m\to\mathrm{GF}(2)^n$ 的轮函数 $F$，并且每轮的输入都是独立随机分布的，那么 $r$ 轮($r\ge 4$)算法的最大差分概率 $\le 2p^2$；同样地 $r$ 轮($r\ge 4$)算法的最大线性概率 $\le 2q^2$。实际上这给出了理论上可证明的算法差分概率和线性概率的上界(一个保守的上界)，如果 $2p^2$ 或 $2q^2$ 足够小，则算法可以抵抗差分攻击和线性攻击。

我们对 CFCEA 算法在不同分组长度下进行了差分和线性密码分析，结果如表 1 所示(表中带*号的数据为预测值)。当分组长度取为 16，24 和 32bit 时，需要对函数 $G$ 和子密钥生成算法作局部微小的改动以适应较短的分组长度(此处略)。由表 1，当分组长度为 64bit 时，CFCEA 算法的差分概率上界近似为 $2^{-52.928}$，而线性概率上界近似为 $2^{-49.206}$，表明该算法具备了抵抗一定强度的差分攻击和线性攻击的能力。

**表 1 最大差分和最大线性概率**

| 概率 | 分组长度（bit） | | | |
|---|---|---|---|---|
| | 16 | 24 | 32 | 64 |
| $p$ | $2^{-4.415}$ | $2^{-6.245}$ | $2^{-9.328}$ | $2^{-26.964}$(*) |
| $2p^2$ | $2^{-7.830}$ | $2^{-11.490}$ | $2^{-17.656}$ | $2^{-52.928}$(*) |
| $q$ | $2^{-3.678}$ | $2^{-5.445}$ | $2^{-8.219}$ | $2^{-25.103}$(*) |
| $2q^2$ | $2^{-6.356}$ | $2^{-9.890}$ | $2^{-15.438}$ | $2^{-49.206}$(*) |

## 5 结束语

本文提出了一种新颖的结合离散混沌映射和Feistel网络结构的分组加密算法，在轮函数 $F$ 的设计中我们使用了一维离散 Logistic 混沌映射和 3 个代数群算子进行混合运算，并提供了对 128bit 长度主密钥的支持。对算法的密码学特性进行了分析和讨论，结果表明该算法具有严格的雪崩效应，算法的扩散性能和扰乱性能非常理想，在轮函数和子密钥生成算法中均引入混沌映射，这使得密文的复杂性和不可预测性得到了很大程度的提高。此外算法具备抵抗一定强度的差分密码分析和线性密码分析的能力。

本文研究内容表明，将离散混沌映射与传统密码学结合起来去尝试新的加密算法是可行的。同时我们也发现，如何更深层次地将混沌理论用于传统密码学仍然是一项非常艰巨的工作，基于混沌的加密算法的安全性评估方法也有待进一步研究。

## 参 考 文 献

[1] Pecora L M, Carroll T L. Synchronization in chaotic systems. *Phys. Rev. Lett*., 1990, 64(8): 821−824.

[2] Pecora L M, Carroll T L. Driving systems with chaotic signals. *Phys. Rev.* A, 1991, 44(4): 2374−2383.

[3] Matthews R. On the derivation of a chaotic encryption algorithm. *Cryptologia*, 1989, XIII (1): 29−42.

[4] Yang T, Wu C W, Chua L O. Cryptography based on chaotic systems. *IEEE Trans. on CAS-I*, 1997, 44(5): 469−472.

[5] Sivaprakasam S, Shore K A. Message encoding and decoding using chaotic external-cavity diode lasers. *IEEE Journal of Quantum Electronics*, 2000, 36(1): 35−39.

[6] Habutsu T, Nishio Y, Sasase I, *et al*.. A secret cryptosystem by iterating a chaotic map. Advance in cryptology – EUROCRYPT'91, Berlin, Springer-Verlag, 1991, LNCS 547: 127−140.

[7] Erdmann D, Murphy S. Henon stream cipher. *Electronics Letters*, 1992, 28(9): 893−895.

[8] Chen H C, Yen J C. A new cryptography system and its VLSI realization. *Journal of Systems Architecture*, 2003, 49(7-9): 355–367.

[9] Kocarev L, Jakimoski G. Logistic map as a block encryption algorithm. *Phys. Lett. A*, 2001, 289 (4-5): 199−206.

[10] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Trans. on CAS-I*, 2001, 48(2): 163−169.

[11] Pareek N K, Patidar V, Sud K K. Discrete chaotic cryptography using external key. *Phys. Lett. A*. 2003, 309 (1-2): 75−82.

[12] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation and Chaos*, 1998, 8(6): 1259−1284.

[13] Salleh M, Ibrahim S, Isnin I F. Enhanced chaotic image encryption algorithm based on Baker's map. ISCAS'03, Bangkok Thailand, May 2003, Vol.2: 25−28.

[14] Chen G R, Mao Y B and Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, 2004, 21(3): 749−761.

[15] Feigenbaum M J. Quantitative universality for a class of nonlinear transformations. *Journal of Statistical Physics*, 1978, 19(1): 25−52.

[16] Lai X, Massey J L. A proposal for a new block encryption standard. Advances in Cryptology - EUROCRYPT'90, Berlin Springer-Verlag, 1991, LNCS 473, 389−404.

[17] Merkle R C. Fast software encryption functions. Advances in Cryptology - CRYPT0'90, Springer-Verlag, Berlin 1991, LNCS 537: 476−501.

[18] GOST R 34.11-94, Gosudarstvennyi Standard of Russian Federation. Information technology, cryptographic data security, hashing function. Government Committee of the Russia for Standards, 1994.

[19] Shannon C E. Communication theory of secrecy system. *The Bell System Technical Journal*, 1949, 28(4): 656−715.

[20] Kocarev L. Chaos-based cryptography: A brief overview. *IEEE Trans. on CAS-I*, 2001, 1(3): 6−21.

[21] Feistel H. Cryptography and computer privacy. *Scientific American*, 1973, 228(5): 15−23.

[22] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Advances in Cryptology - CRYPTO'90, Berlin Springer-Verlag, 1991, LNCS 537: 2−21.

[23] Biham E, Shamir A. Differential cryptanalysis of the data encryption standard. Berlin Springer-Verlag, 1993.

[24] Matsui M. Linear cryptanalysis method for DES cipher. Advances in Cryptology-EUROCRYPT'93, Berlin Springer-Verlag, 1994, LNCS 765: 386−397.

[25] Nyberg K, Knudsen L. Provable security against a differential attack. *Journal of Cryptology*, 1995, 8(1): 27−37.

彭　军：男, 1970 年生, 副教授, 博士, 研究方向为混沌保密通信、密码学、网络安全.

廖晓峰：男, 1964 年生, 教授, 博士后, 博士生导师, 研究方向为混沌保密通信、神经网络.

岡本栄司：男, 1950 年生, 教授, 博士, 研究方向为密码学.