第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 博士论文 •

文章编号：1000—3428(2012)03—0022—03 文献标识码：A 中图分类号：TP309

基于 Feistel 网络的十进制加密算法

崔 杰，仲 红

(安徽大学计算机科学与技术学院，合肥 230039)

摘 要：提出一种基于 Feistel 网络的十进制加密算法。针对十进制数运算的特点，在加密算法中定义 4 种新的运算，在密钥扩展算法和解密算法中定义 2 种新的运算，并设计十进制 S 盒。将该算法应用于短分组加密仿真系统中，实验结果表明，该算法具有较好的密码学特性，加解密的各项扩散率指标均较优，经 6 轮加密后，该算法达到完全扩散。

关键词：十进制；Feistel 网络；分组密码；扩散率；S 盒；密码学

Decimal System Encryption Algorithm Based on Feistel Network

CUI Jie, ZHONG Hong

(School of Computer Science and Technology, Anhui University, Hefei 230039, China)

【Abstract】This paper proposes a decimal system encryption algorithm based on Feistel network. Aiming at the characteristics of decimal system operations, four operations are defined in encryption algorithm, two operations are defined in key expansion algorithm and decryption algorithm, and the new decimal system substitution table is designed. The new encryption algorithm is applied to the short-block encryption simulation system, simulation results show that the proposed algorithm has excellent cryptographic properties, all diffusion rate targets reach desired impact, and the diffusion rate of key to ciphertext after 6-round encryption reaches full diffusion. The encryption algorithm can be applied to all areas of decimal system encryption.

【Key words】decimal system; Feistel network; block cipher; diffusion rate; S-box; cryptology

DOI: 10.3969/j.issn.1000-3428.2012.03.008

1 概述

信息安全技术包括加密技术、入侵检测技术、反病毒技术等方面，加密技术是信息安全最主要的安全技术之一。加密体制分为对称加密和非对称加密 2 种[1-2]。计算机适宜处理十六进制数(即二进制)，加密算法一般是针对十六进制数进行设计。人们习惯使用十进制数，在相当多的网络通信应用中需要对十进制数信息进行加密[3]。很多应用(如预付费表计、电信充值卡、电子货币等加密应用)要求十进制数的明文位数和加密后的十进制数的密文位数相等，基于十六进制的加密算法就不能满足上述要求。为此，对基于对称密码的十进制加密技术进行研究。

本文利用 Feistel 网络，提出一种新的十进制加密算法，并对该算法进行密码学分析实验。在此十进制分组密码中，其分组加密的每一轮采用 Feistel 网络结构。与 DES 等算法不同的是，加解密过程中的明文、密文及各个中间状态都是等长的十进制数分组。

2 Feistel 网络

Feistel 网络被广泛应用于分组密码的设计，典型的有 DES、Lucifer、FEAL、LOKI、GOST 和 Blowfish 等，其基本思想为[4]：取一个长度为 n 的分组，将它分成长度为 $n/2$ 的左右 2 个部分，记为 L 和 R。定义一个迭代型的分组密码算法，其第 i 轮的输出为：

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

其中，k_i 是第 i 轮的子密钥；F 可以是任意的轮函数。只要 F 能在每一轮中重新构造，Feistel 网络的结构特点就能保证该密码的可逆性，哪怕 F 是不可逆的[5-7]。这是因为：

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

因此，该网络可同时用于加密和解密[8]。

3 算法原理

由于异或运算对十进制数没有可逆性，因此要对 Feistel 网络中的运算进行重新设计，即设计新的 F 函数。考虑到加密算法对十进制数的可逆性，同时保证加密算法的性能，本文设计的 F 函数包括 DeciIP、模十加、DeciS 和 DeciP 4 种变换。

加密算法可以对 8 位、16 位、32 位和 64 位 4 种长度的十进制明文分组进行加解密，密钥长度取相应明文长度的一半。下面以 32 位长度的明文为例，讨论算法的实现原理。

3.1 加密算法中的 4 种运算

3.1.1 初始置换函数 DeciIP

32 位的十进制明文分组 P 首先经过一个初始置换函数 DeciIP 进行置换运算，产生一个 32 位的输出 $\tilde{P}$，如图 1 所示。该输出被分成 2 个分别为 16 位的左半部分 $L0$ 和右半部分 $R0$，用于 F 函数的 16 轮迭代的第 1 轮迭代的输入。

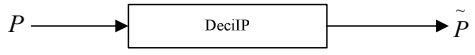

图 1 初始置换流程

基金项目：国家自然科学基金资助项目(61173187, 61173188)；安徽省高等学校优秀青年人才基金资助项目(2010SQRL017)；安徽大学“211 工程”基金资助项目

作者简介：崔 杰(1980－)，男，讲师、博士研究生，主研方向：网络与信息安全；仲 红，教授

收稿日期：2011-07-26 **E-mail：**cuijie@mail.ustc.edu.cn

设 $P = p_1 p_2 \cdots p_{32}$，$\tilde{P} = \tilde{p}_1 \tilde{p}_2 \cdots \tilde{p}_{32}$，则 $\tilde{P} = p_{26} p_{18} \cdots p_7$，即 $\tilde{p}_1 = p_{26}, \tilde{p}_2 = p_{18}, \cdots, \tilde{p}_{32} = p_7$。DeciIP 置换表如图 2 所示。DeciIP^{-1} 置换是 DeciIP 的逆置换。

26	18	10	2	28	20	12	4
30	22	14	6	32	24	16	8
25	17	9	1	27	19	11	3
29	21	13	5	31	23	15	7

图 2　DeciIP 置换表

3.1.2　模十加运算

在 Feistel 网络中，利用密钥与状态对应的字节做异或运算来加密。但是异或运算对于十进制数没有可逆性，为了实现十进制数的加密，需要引入模十加运算，记为 $\oplus_{\mathrm{mod}\ 10}$。对每一轮中 R_i 与密钥 k_i 的模十加可以表示成：

$$R_i \oplus_{\mathrm{mod}\ 10} k_i = \begin{cases} R_i + k_i & R_i + k_i < 10 \\ R_i + k_i - 10 & R_i + k_i \geqslant 10 \end{cases}$$

3.1.3　替换运算

由于替换运算是本文加密算法中唯一的非线性运算，其性能直接决定整个加密算法的安全性[9]。借鉴 AES S 盒的构造原理，设计一种新的十进制替换表 DeciS 盒，DeciS 盒是 2 位十进制数替换表，其运算空间为 $GF(100)$。DeciS 盒运算包括在有限域 $GF(100)$ 中的求乘法逆运算和在域 $GF(10)$ 下的仿射变换运算 2 个步骤。其中的求逆运算是将 2 位十进制数看作域 $GF(100)$ 的元素，求其在十进制不可化约多项式 $m(x) = x^2 + 1$ 下的逆，而仿射变换是求逆结果与 $GF(10)$ 上矩阵 $\boldsymbol{M}$ 相乘然后与向量 $\boldsymbol{I}$ 相加。其中，$\boldsymbol{M}$ 为：

$$\boldsymbol{M} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

向量 $\boldsymbol{I}$ 为 $\boldsymbol{I} = (2,3)^{\mathrm{T}}$。DeciS 盒运算的具体过程如下：

(1)在 $GF(10^2)$域，求乘法的逆运算，即对于 $\alpha \in GF(10^2)$，求 $\beta \in GF(10^2)$，使：

$$\alpha \cdot \beta = \beta \cdot \alpha \equiv 1 \bmod (x^2 + 1)$$

(2)在 $GF(10)$ 域作仿射变换：

$$\begin{pmatrix} y_1 \\ y_0 \end{pmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

通过计算得到 $GF(10^2)$域上各个元素的逆元。规定 0 元素的逆为它自身。经过仿射变换，得到的 DeciS 盒如图 3 所示，其中，X 代表十位；Y 代表个位。即用 23 替换 00，用 17 替换 12，以此类推。

X \ Y	0	1	2	3	4	5	6	7	8	9
0	23	34	39	20	26	92	11	54	64	52
1	13	63	17	60	94	32	33	89	93	00
2	68	37	98	87	81	79	31	99	14	90
3	83	69	49	96	56	21	58	71	01	95
4	85	38	70	74	61	12	55	30	07	19
5	91	45	27	50	06	02	24	75	62	66
6	08	51	41	35	86	88	15	80	40	18
7	77	53	46	22	47	05	67	76	59	48
8	09	78	36	43	57	03	04	42	97	29
9	73	44	84	72	82	25	65	10	16	28

图 3　DeciS 替换表

3.1.4　置换函数 DeciP

在 DeciS 替换之后进行 DeciP 置换，置换表如图 4 所示。

16	7	12	1	15	5	10	2
8	14	3	9	13	6	11	4

图 4　DeciP 置换表

DeciP 置换后的第 1 位是原来的第 16 位，第 2 位是原来的第 7 位，以此类推。

3.2　本文算法的加密和解密

3.2.1　加密过程

基于 Feistel 网络的十进制加密算法的加密流程由上述 4 种运算构成，首先进行初始置换 DeciIP，然后连续迭代 16 轮，最后进行逆初始置换 DeciIP^{-1} 便得到密文。整个加密算法的具体加密流程如图 5 所示。

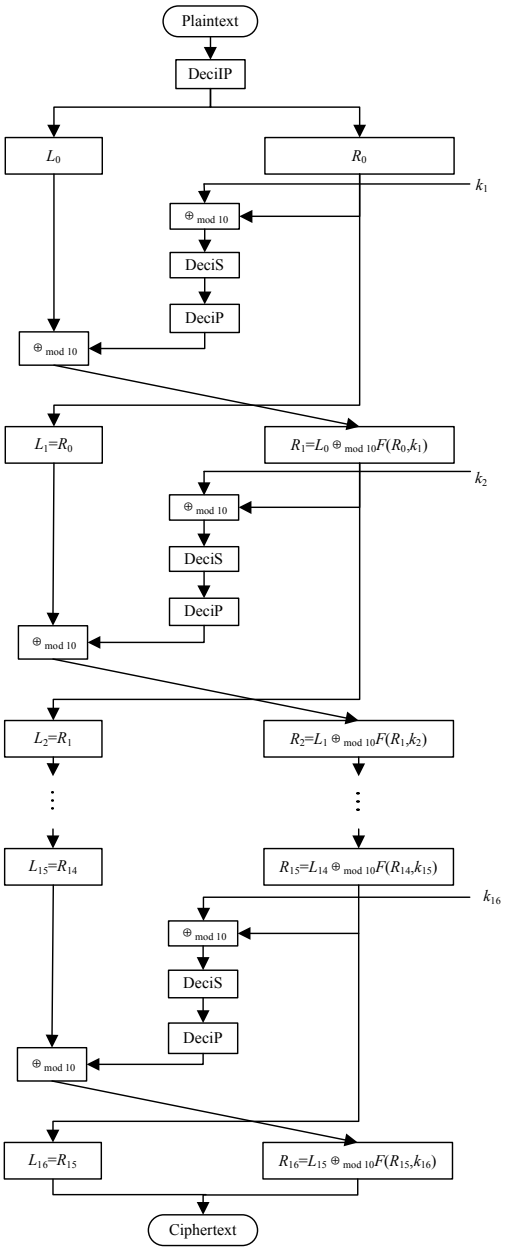

图 5　基于 Feistel 网络的十进制加密算法流程

由图 5 可知，加密算法中的 F 函数由 $\oplus_{\mathrm{mod}10}$、DeciS 和 DeciP 组合而成，即 $F(R_{i-1}, k_i) = DeciP(DeciS(R_{i-1} \oplus_{\mathrm{mod}10} k_i))$。输入的十进制明文分组经过上述变换便得到同样长度的十进制密文分组。

3.2.2 解密过程

本加密算法的解密过程是加密过程的逆过程，将密文按解密过程操作即可得到明文。解密过程还用到置换 DeciPC-1 和移位变换 Rsi。

(1)置换函数 DeciPC-1

DeciPC-1 置换表如图 6 所示。DeciPC-1 置换后，原来的第 2 位变为现在的第 1 位，原来的第 4 位变为现在的第 2 位，以此类推。

2	4	6	14	12	10	8	16
1	3	5	13	11	9	7	15

图 6 DeciPC-1 置换表

(2)循环右移 Rsi

Rsi 的移位规则如下：

迭代轮次	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
右移位数	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1	1

3.3 密钥扩展算法

加密过程中的各轮子密钥由原始密钥通过密钥扩展算法得到。每一轮密钥扩展中，首先要经过 DeciPC-1^{-1} 置换，然后进行移位操作。密钥扩展的具体过程如图 7 所示。

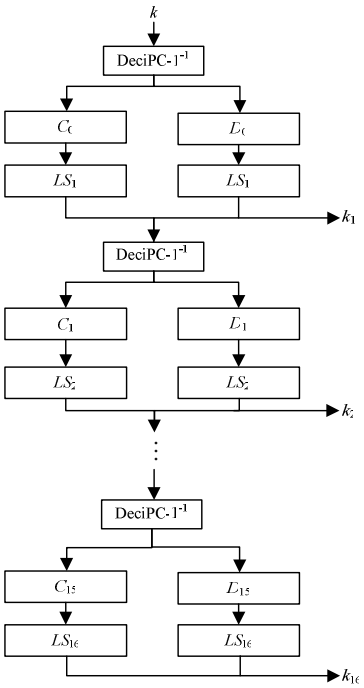

图 7 密钥扩展过程

(1)DeciPC-1^{-1} 置换

DeciPC-1^{-1} 置换的置换表如图 8 所示。

9	1	10	2	11	3	15	7
14	6	13	5	12	4	16	8

图 8 DeciPC-1^{-1} 置换表

(2)循环左移 Lsi

Lsi 是循环右移 Rsi 的逆操作，移位规则如下：

迭代轮次	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
右移位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

4 本文算法加密性能分析

定义 1 对于加密函数 $E_K(P)$ 中的参数 K 和 P(解密函数 $D_K(C)$ 中的参数 K 和 C)，每次加(解)密只改变其中某个参数的一位，另一个参数保持不变，把多次加(解)密得到的密(明)文相比较，每一位上相异的比率称为加密(解密)扩散率[10]。

由定义 1 可知，扩散率越大，相同的明文不同的密钥加密得到相同密文的概率就越小，可以更有效地防止攻击者已知部分密钥相关性攻击。扩散率越大，密码的雪崩效应越好，安全性也就越高。

定义 2 对于一个加密算法，若扩散率大于等于 0.5，则称该加密算法达到了完全扩散[10]。

对该算法的加密性能进行了软件仿真测试分析。分别以 8 位、16 位、32 位、64 位十进制数为加密分组，进行 4 轮~16 轮的加解密运算测试。下面是以 32 位十进制数为加密分组所得的测试结果。加密过程中明文对密文的扩散率、密钥对密文的扩散率如图 9 所示。

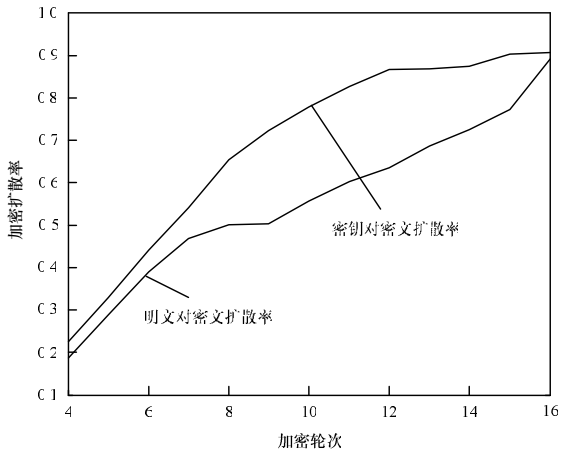

图 9 明文、密钥对密文的扩散率

解密过程中密文对明文的扩散率、密钥对明文的扩散率如图 10 所示。从图中可看出，加密轮数大于 8 有很好扩散性。加密过程中轮数大于 6，则密钥对密文就达到了完全扩散，解密过程中轮数大于 7，则密钥对明文就达到了完全扩散。

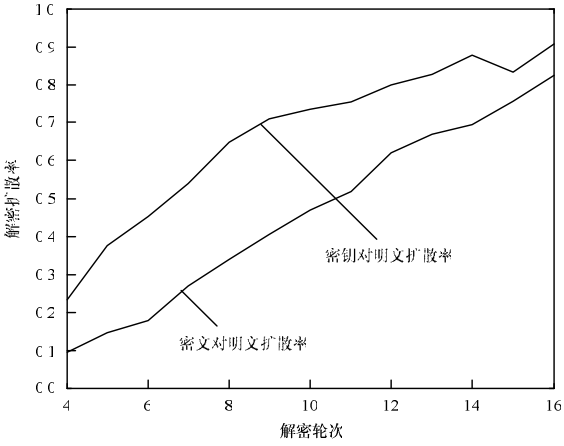

图 10 密文、密钥对明文的扩散率

5 结束语

本文提出的算法借鉴了 Feistel 密码结构的思想，并对其中的运算进行了重新定义，以适应十进制数加密/解密的要求。算法中定义了初始置换函数 DeciIP、模十加运算 $\oplus_{\bmod 10}$、替换运算 DeciS、置换函数 DeciP、置换函数 DeciPC-1 和循环移位等运算，其中十进制替换表 DeciS 的构造借鉴了 AES 中 S 盒的构造原理，并在十进制域 $GF(10^2)$ 内实现。算法对硬件要求低，实现容易，加密解密速度快，加密强度高，具有较高的安全性，该加密算法可广泛用于各种需要十进制数加密的领域。

(下转第 33 页)