学术论文

演化密码与 DES 密码的演化设计

张焕国[1]，冯秀涛[1]，覃中平[2] 刘玉珍[1]

（1. 武汉大学计算机学院 软件工程国家重点实验室，湖北 武汉 430072；2. 华中科技大学数学系，湖北 武汉 430074）

摘 要：本文提出演化密码的概念和用演化计算设计密码的方法。演化密码在理论和应用中都有重要意义。本文对 DES 的核心部件 S 盒进行了实际演化，得到一种用演化计算设计 S 盒的方法，并获得了一批安全性能优异的 S 盒。用演化方法设计出一族安全性能渐强的 S 盒或其他部件，分别以这些 S 盒或其他部件构造 DES，就可使 DES 密码体制本身进行演化，而且安全性能愈来愈强。

关键词：信息安全；密码；演化计算；演化密码

中图分类号：TP309 **文献标识码：**A **文章编号：**1000-436X（2002）05-0057-08

Evolutionary cryptosystems and evolutionary design for DES

ZHANG Huan-guo[1], FENG Xiu-tao[1], QIN Zhong-ping[2], LIU Yu-zhen[1]

(1. State Key Laborary of Software Engineering, College of Computer, Wuhan University, Wuhan 430072, China;
2. Dept. of Math., Huazhong University of Sci. & Tech., Wuhan 430074, China)

Abstract: This paper proposes the concept of evolutionary cryptosystems and an evolutionary method for designing cryptosystems. With the evolutionary computing we can fast generate a group of S-boxes of DES which are more secure than the old ones of DES. The evolutionary computing can also be used in designing the general cryptosystems (for example AES). In other aspect using a group of increasingly secure S-boxes we can construct the evolutionary cryptosystem of type DES. Generally the evolutionary cryptosystems have the more powerful secure function than usual ones

Key words: information security; cryptology; evolutionary computing; evolutionary cryptosystem

收稿日期：2001-12-10；**修订日期：**2002-03-29

基金项目：国家自然科学基金重点资助项目（90104005）；国家自然科学基金资助项目（66973034）

作者简介：张焕国（1945-），男，河北元氏人，武汉大学教授，博士生导师，研究方向为信息安全、容错计算；冯秀涛（1978-），男，湖北云梦人，武汉大学硕士生，研究方向为信息安全；覃中平（1949-），男， 湖北武汉人，华中科技大学教授，研究方向为密码学、算法设计；刘玉珍（1963-），女，湖北宜昌人，武汉大学副教授，研究方向为信息安全。

1 引言

密码是一种重要的信息安全技术。安全强度高是对密码的基本要求。而密码的设计却十分复杂困难。如何设计出高安全强度的密码和使密码设计自动化是人们长期追求的目标。

大自然是人类获得灵感的源泉。几百年来，将生物界所提供的答案应用于实际问题已被证明是一种成功的方法，并且已经形成仿生学这个专门的科学分支。我们知道，自然界所提供的答案是经过漫长的演化过程，而获得的结果。除了演化过程的最终结果，我们还可以利用这一过程去解决一些复杂问题。于是，我们不必非常明确地描述问题的全部特征，只需要根据自然法则来产生新的更好的解。演化计算正是基于这种思想而发展起来的一种通用的问题求解方法。它具有高度并行、自适应、自学习等特征。它通过优胜劣汰的自然选择和简单的遗传操作使演化计算能够解决许多复杂的问题。

我们将密码学与演化计算结合起来，借鉴生物进化的思想，提出演化密码的概念和密码算法的演化设计方法。这些研究工作无论对于密码学还是对演化计算是十分有意义的。

2 演化密码的概念

迄今为止的分组密码都是一种加解密算法固定而密钥随机可变的密码。如 DES、IDEA、AES、RSA 等都是如此。设 E 为加密算法，$K_0\,K_1\cdots K_i\cdots K_n$ 为密钥，M 为明文，C 为密文，则把 $M_0\,M_1\cdots M_i\cdots M_{n\text{-}1}\,M_n$ 加密成密的过程可表示为

$$C_0=\mathrm{E}(M_0,K_0),\ C_1=E(M_1,K_1),\cdots C_i=E(M_i,K_i),\cdots C_n=E(M_n,K_n) \tag{1}$$

在这一过程中加密算法固定不变。

如果能够使上述加密过程中加密算法 E 也不断变化，即

$$C_0=E_0(M_0,K_0),\ C_1=E_1(M_1,K_1),\cdots C_i=E_i(M_i,K_i),\cdots C_n=E_n(M_n,K_n) \tag{2}$$

则称为加密算法可变的密码。

由于加密算法在加密过程中可受密钥控制而不断变化，显然可以极大地提高密码的强度。更进一步，若能使加密算法朝着越来越好的方向发展变化，密码就成为一种渐强的密码。

另一方面，密码的设计是十分复杂的、困难的。密码设计自动化是人们长期追求的目标。能否找到一种密码设计自动化的方法呢？我们提出一种模仿自然界的生物进化，通过演化来设计密码的方法。在这一过程中，密码算法不断演化变化，而且越变越好。设 $E_{-\tau}$ 为始加密算法，则演化过程从 $E_{-\tau}$ 开始，经历 $E_{-\tau+1}$，$E_{-\tau+2}$，$\cdots E_{-1}$，最后变为 E_0。由于 E_0 的安全强度达到实际使用的要求，可以实际应用。我们称这一过程成为“十月怀胎”，$E_{-\tau}$ 为“初始胚胎”，E_0 为“一朝分娩”的新生密码。

设 $S(E)$ 为加密算法 E 的强度函数，则这一演化过程可表为

$$E_{-\tau}\to E_{-\tau+1}\to E_{-\tau+2}\to\cdots\to E_{-1}\to E_0 \tag{3}$$

$$S(E_{-\tau})<S(E_{-\tau+1})<S(E_{-\tau+2})\cdots<S(E_{-1})<S(E_0) \tag{4}$$

综合以上两个方面，可把加密算法 E 的演化过程表示为

$$E_{-\tau}\to E_{-\tau+1}\to E_{-\tau+2}\to\cdots\to E_{-1}\to E_0\to E_1\to E_2\to\cdots\to E_n \tag{5}$$

$$S(E_{-\tau})<S(E_{-\tau+1})<\cdots<S(E_{-1})<S(E_0)\le S(E_1)\le S(E_2)\le\cdots\le S(E_n) \tag{6}$$

其中，$E_{-\tau}\to E_{-\tau+1}\to\cdots\to E_{-1}$ 为加密算法的设计演化阶段，即“十月怀胎”阶段。在一阶段中，加密算法的强度尚不够强，不能实际使用。这是密码的演化设计阶段，这一过程在实验室进行。E_0 为“一朝分娩”的新生密码，它是密码已经成熟的标志。$E_0\to E_1\to E_2\to\cdots\to E_n$ 为密码

的工作阶段，而且在工作过程中仍不断演化，密码的安全性越变越好。这就是演化密码。

3　DES 类分组密码的抗差分分析

许多分组密码采用 feistel 结构，并以 S 盒作为其核心部件。对分组密码强度的评估，主要是看其抵抗各种攻击的能力。目前，对 DES 类分组密码的主要攻击方法有穷举攻击、差分分析和线性分析等。而差分分析和线性分析便直接针对 S 盒组和密码的迭代结构。因此，演化 DES 的核心就是演化 S 盒组，使之符合某种安全准则。S 盒的安全准则主要有：a) 非线性准则；b) 差分准则；c) 雪崩准则；d)扩散准则。下面主要讨论演化 DES 的差分准则。

3.1　DES 差分分析原理

首先我们给出几个重要的概念：

定义 1　对一对明文 m_1、m_2，定义差分 $\Delta=m_1 \oplus m_2$，而将这样一组差分 Ω：Δ_0、Δ_1、…、Δ_r 称之为一个 r-轮特征，其中 Δ_j 为第 j 轮的输出差分；其概率是指在初始差分为 Δ_0 下，使得第一轮差分等于 Δ_1，第二轮差分等于 Δ_2、…第 r 轮差分等于 Δ_r 时的概率。

在明文，密钥均匀独立下，r-轮特征概率近似等于各单轮概率的乘积。

定义 2　测试集 $test$（m_1，m_2，Δ），即可能密钥集，我们将之定义为

$$\{key \mid key = m_1 \oplus m, m \in IN(D_{\text{in}}, D_{\text{out}}) \text{ 其中 } D_{\text{in}} = m_1 \oplus m_2,\ D_{\text{out}} = D\} \tag{7}$$

对 DES 进行差分攻击主要是基于弱轮函数，即若我们可以准确的或者很高概率地知道某一轮的输入差分，输出差分以及输入明文或者输出密文，则我们根据以下定理对 DES 攻击可以获得成功。

定理 1　若我们能够准确的知道某轮的输入明文对以及 S 盒的输出差分，则密钥 key 一定满足 $key \in test$（m_1，m_2，Δ）[2]。

根据定理 1，只需一个计数器，将可将密钥计数，若某一个计数器的值已经明显比其他任何一个计数器的值要高，则其对应的子密钥一定是所求的子密钥。我们将能够正确的区分出正确子密钥所需要的各计数器的最小差值（即正确子密钥和错误子密钥的计数器之间的最小差值）称之为显具水平 a。

定理 2　设显具水平为 a，r-弱轮特征概率为 P，k 个可能密钥计数器，则攻击 r+2-轮 DES 所需要的最小明文对 N，由下式决定

$$N \approx a \times P^{-1} \times \frac{k}{k-1} \tag{8}$$

在确定性攻击中，a=1。

证明　由于在 N 对明文中，可能正确的明文对有 $N \times P$ 对，可能错误的明文对有 $N \times (1-P)$对，在密钥，文明对均匀随机的条件下，这些明文对对各个可能密钥计数器的贡献是一致的，即每个可能密钥计数器大致可以得到 N/K 次计数，而正确子密钥的计数器可以得到：$N \times p + N \times (1-p)/k$ 计数，故

$$(N \times p + N \times (1-p)/k) - N/k = a$$

即 $N = a \times p^{-1} \times \frac{k}{k-1}$，命题得证。

3.2 DES 的 r+2 / 3 轮攻击

如图 1，当我们攻击 r+2 轮 DES 时，考虑最后一轮，我们已经知道 S 盒的输入明文的差分 $E(L_{r+2} \oplus L_{r+2}^{*})$，以及输入明文 L_{r+2}，因此我们只需知道 S 盒的输出差分 Δ_{r+2} 即可。而

$$\Delta_{r+2} = P^{-1}(\Delta R_{r+2} \oplus \Delta L_{r+1}) = P^{-1}(\Delta R_{r+2} \oplus \Delta R_r) \qquad (9)$$

因此，我们对 r+2 轮 DES 攻击，只要能够正确的或者很高概率地知道第 r 轮的输出差分 ΔR_r 即可。此外，若我们只能正确的或者很高概率的知道第 r-1 轮的输出差分 Δ_{r-1}，并且可以正确的得到第 r 轮部分 S 盒的输出差分，那么我们也可以得到第 r 轮部分 S 盒的输出差分，因此，我们此时只能得到部分 S 盒的子密钥[2]。于是可以得到如下结论：

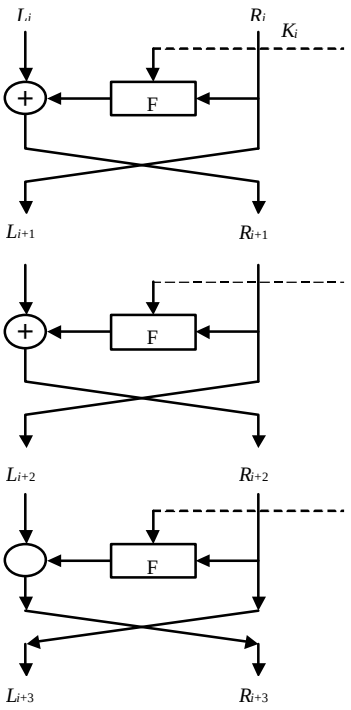

图 1 DES 圈结构

定理 3 如果我们可以得到一个高概率的 r 轮特征，那么我们可以对 r+2 轮 DES 进行攻击，可以得到 8 个 S 盒全部子密钥；并且可以对 r+3 轮 DES 进行攻击，但只能得到部分 S 盒的子密钥。证明略。

3.3 轮特征构造

对 DES 进行差分攻击时关键在于能够找到一个高概率的差分轮特征，本文给出了一种寻找最大轮特征的上下对称的轮特征结构，利用这种结构，在搜索差分特征时可以减少一半的工程量。

在图 2 的上下对称的轮特征构造结构中，两种轮特征结构是等价的，这是因为在图 2（a）中

$$\Delta R_{I+1} \overset{P}{=} \Delta L_I \oplus DESFUN(\Delta R_I)$$

在图 2(b)中

$$\Delta L_I \overset{P}{=} \Delta R_{I+1} \oplus DESFUN(\Delta R_I)$$

容易发现上面两式完全等价，因此由其中的一个结构可以完全以同等概率推出另外一个结构。于是可以选择如图 3 所示的轮特征结构，在这种结构中我们有一个好处，那就是我们只需在一个方向上构造概率最大的轮特征，那么我们就可以朝另外一个方向延伸，能够得到两倍长的概率最大轮特征。根据上面讨论的结果，我们对 r+2/3 轮 DES 攻击时只需将精力集中在图 3 的结构上。

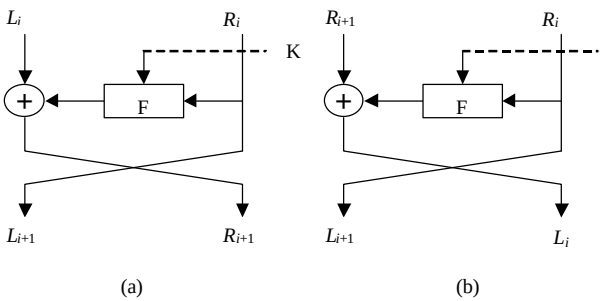

图 2 差分的对称性

3.4 差分特征自动搜索算法

利用差分对 DES 进行攻击，由于关键在于找到一个高概率的差分轮特征，因此差分的自动分析算法的目的就在于

通过一个有效的策略，将其轮特征找出来。我们定义：

定义 3　攻击度 cr 是一个反映攻击难易程度的指标，其数学定义为 $cr=-\ln f_{\max}/\ln 2$，其中 $f_{\max}$ 为最大 r-轮概率。攻击度 cr 反映了攻击的难易程度。

由定理 2，我们很容易得到下面结论

定理 4　设 r+2（或者 r+3）DES 的攻击度为 cr，则其所需要的最小的明文对 N 为

$$N\approx a\times 2^{cr}\times\frac{k}{k-1}$$

其中，a 为显具水平，k 为可能密码计数。

因此攻击度可以作为 DES 抗差分攻击的一个定量指标。此外，我们定义 S 盒差分的输入权重 W 为该差分经扩展置换后输入到不同的 S 盒中差分不为零的个数。对 $r\leq 4$ 时,其搜索最大概率差分算法如下。

r 轮差分自动搜索算法：

（1）根据 S 盒组生成差分统计表

（2）对输入权重≤4 的差分进行穷举搜索：

a）对输入差分非零的 S 盒，查找概率≥$LIMIT$ 的输出差分，计算该轮概率。

b）如果该轮轮特征概率≥P_0，则直接返回（2）。

c）否则，将输出差分经过置换变换后作为下一轮的输入差分。

d）如果不是最后一轮，则转到 a）。

e）否则，判断最终概率，如果≤P_0，则交换 P_0。

f）转到（2）。

（3）返回查到的差分值，以及攻击指数。

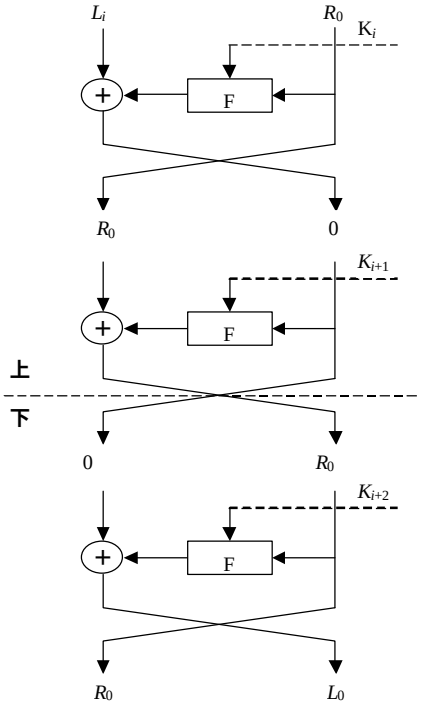

图 3　上下对称的差分圈特征结构

在上述算法中，P_0 为我们预先定义的概率值，这个值可以较大一些，对我们要搜索的差分轮特征没用任何影响。$LIMIT$ 称为截断概率，可以人为设定，主要是过滤掉那些概率很小，不太可能选得高概率轮特征的差分对。在上述算法中，我们一定可以得到不超过 12 轮的上下对称轮特征结构的最大概率的轮特征，证明如下。

证明　由于我们只是在对权重小于等于 4 的情况下通过穷举搜索得到一半轮特征差分（此时搜索的范围很狭窄了），因此可以断定，该一半轮特征差分一定是最大的。于是我们只需证明对于全局概率最大的上下对称轮特征差分必然落在这个区域中即可。对权重大于等于 5 的差分，其攻击度

$$cr=-\ln(p_1\cdot p_2\cdots p_r)/\ln 2=\sum_{i=1}^{r}-\ln p_i/\ln 2=\sum_{i=1}^{r}cr_i \qquad (10)$$

对于单轮特征，我们有如下关系式：$cr_i\geq 2\times w_i$，其中 w_i 为权重，当输入差分不为零时，有 $w_i\geq 1$。而 $w_i\geq 5$，因此，我们有

$$cr=\sum_{i=1}^{r}cr_i\geq cr_1+\sum_{i=2}^{r}2\times w_i\geq 2\times 5+2\times\sum_{r=2}^{r}1=8+2\times r \tag{11}$$

在我们对权重小于等于 4 的处理中，我们得到 6 轮 DES：$cr\leq 2$，8 轮：$cr<7$，10 轮：$cr\leq 13.5$，12 轮：$cr<16$。这与上式所给出的下界还要小，所以，概率最大的上下对称的轮特征差分必然落在权重小于等于 4 的区域中，命题得证。

4 演化 DES 以及差分分析

通过上面的分析，我们将攻击指标 cr 作为演化 DES 的评估标准，对 DES 作了演化试验，并同 DES 在抗差分攻击方面作了对比，得到了许多抗差分攻击能力更强的 S 盒组。

4.1 基本的演化算法

在 DES 演化过程中，我们采用了 $u+\lambda$ 重叠种群的演化结构，由于该结构简洁、实现简单，容易保留较好的个体。其基本算法如下。

S 盒演化算法

(1) 化 DES 群体 $p(t)=\{p_1、p_2、\ldots、p_N\}$，$t=0$，$p_1$=DES；

(2) 群体进行评估，计算每个个体的概率指标 cr；

(3) 得到最差个体的指标，如果其大于我们预先定义的指标，则转到 (8)；

(4) 否则，根据各个体的概率指标计算其选择概率；

(5) 然后随机选择两个个体进行杂交操作；

(6) 再随机选择一个个体进行变异操作；

(7) 将产生的后代加入到群体中，计算后代的概率指标 cr，转到 (2)

(8) 输出演化的各个个体；

(9) 结束。

4.2 演化目标及策略

演化的最终目标就是要得到比DES在抗差分方面更强的S盒组。为此我们采取如下策略：

(1) 选择策略：选择策略即是如何进行优胜劣汰的自然选择。在 DES 演化过程中，为了确保：1) 演化能够在整个 S 盒空间搜索；2) 较优个体具有较高的选择概率；3) 演化过程整体上符合优胜劣汰的自然选择，我们采取了如下的策略：

a) 对较优的个体赋予较高的存活概率；

b) 对新生个体，虽然初期比较弱小，但有较强的生命力，同样给予较高的存活概率；

c) 总是淘汰适应值最差的个体；

(2) 评估策略：评估策略即如何评定个体的适应能力。我们将采取了如下评估策略：

a) 对个体的评估　将以 DES 8 轮、10 轮以及 12 轮指标作为参考标准，进行个体抗差分攻击能力的评估；

b) 对 S 盒的评估，主要集中在一下几个指标：

(i) 雪崩规则，即要求输入变一位，输出至少变换两位；

(ii) 对输入差分为 001100，要求输出差分至少含有两个 1；

(iii) 差分均匀性；

(iv) 线性均匀性；

(3) 杂交策略：杂交策略即随机选择两个父体后，如何进行交配因子产生下一代。目前

采用的杂交方法主要有：对 father1 和 father2 进行交换和运算。

（4）繁殖策略：即如何控制由两个父体共同产生一个子代。繁殖策略要求满足：

a）对较优的 S 盒具有较高的选择概率；

b）能够较高概率地消除上次的攻击点；

（5）变异策略：变异策略即如何控制单个个体经过变异操作得到另一个体。变异要求满足：1) 对较差的个体具有较高的选择概率；2) 对整体而言能够较高概率的消除上次的攻击点；3) 对局部 s 盒而言，能够较高概率的选择可能消除其弱点的变异方法。变异方法有：

a）交换个体中两个 S 盒的位置；

b）随机产生一个新的 S 盒来替换其中某一个 S 盒；

（6）定期补充新个体：每隔一定代数，定期随机产生一个全新个体，参与演化。

下面是我们演化得到的一组 S 盒，表 1 数据是演化 S 盒与 DES S 盒的对比，表 2 是演化 S 盒的多项式的项数和最高次数统计。

1	8	2	4	14	13	7	11	12	3	5	15	9	10	0	6	S1
10	13	15	8	5	2	9	4	3	14	12	1	0	7	6	11	
14	7	11	13	4	8	2	1	3	9	12	0	15	6	5	10	
9	14	0	4	15	11	12	8	5	2	10	13	6	1	3	7	
12	15	0	5	9	6	10	3	2	1	7	11	14	13	4	8	S2
11	6	13	3	7	12	0	10	5	8	14	4	2	1	9	15	
0	4	15	3	10	8	5	14	9	13	12	6	7	1	2	11	
5	10	6	13	0	7	3	4	12	11	2	1	9	14	15	8	
5	6	12	9	15	10	0	3	11	8	7	2	1	13	14	4	S3
11	1	7	10	2	12	13	6	4	14	8	5	15	0	3	9	
10	13	5	3	9	4	6	14	0	1	12	15	7	2	11	8	
0	8	9	5	7	2	10	11	15	13	6	3	1	14	12	4	
14	8	5	15	0	3	11	4	9	7	12	2	10	13	6	1	S4
11	5	14	3	7	12	2	15	10	1	6	8	9	4	0	13	
3	15	9	0	12	5	6	10	14	4	2	13	1	11	8	7	
4	0	7	5	1	15	13	6	9	14	12	2	10	8	3	11	
7	10	1	12	13	0	2	9	4	15	11	6	8	5	14	3	S5
0	9	12	6	10	15	5	3	14	4	7	11	1	2	8	13	
10	0	12	5	7	14	9	3	11	4	6	1	13	2	8	15	
12	15	9	10	0	5	3	6	2	1	13	7	8	14	11	4	
11	0	2	12	13	10	7	9	1	6	8	15	14	5	4	3	S6
5	11	9	2	3	4	0	14	7	12	13	6	1	10	8	15	
0	13	12	10	7	4	9	3	6	11	1	5	8	2	15	14	
12	6	0	5	9	3	15	8	11	1	7	10	14	13	2	4	
13	3	7	4	10	9	0	15	1	14	12	2	6	5	11	8	S7
7	8	11	14	4	2	13	1	6	9	0	5	15	10	12	3	
6	0	8	15	5	12	3	10	7	1	2	11	9	14	4	13	
1	6	7	0	11	5	8	15	12	2	9	14	10	13	3	4	
1	7	11	14	2	4	12	9	8	13	6	0	5	10	15	3	S8
4	1	2	13	11	8	7	14	15	10	0	9	3	6	5	12	
14	0	7	9	4	15	11	5	1	10	13	3	2	12	8	6	
1	15	11	2	7	4	12	9	8	6	14	5	13	0	3	10	

表 1 演化 S 盒与 DES S 盒的对比

轮 数	差分分析			差分均匀性	线性均匀性
	8 轮	10 轮	12 轮		
DES	6.60768	13.2852	15.7147	16	20
演化 S 组	6.87072	14.0000	17.5424	16	16

表 2 演化 S 盒的多项式的项数和最高次数统计

比特位	0	1	2	3	4	5	6	7
项数	31	32	32	32	32	32	31	31
最高次数	6	6	6	5	5	5	5	6
比特位	8	9	10	11	12	13	14	15
项数	31	32	31	32	31	31	32	31
最高次数	5	5	6	5	5	6	6	5
比特位	16	17	18	19	20	21	22	23
项数	31	32	32	32	31	31	32	31
最高次数	6	5	6	6	5	5	6	5
比特位	24	25	26	27	28	29	30	31
项数	31	32	31	31	31	32	32	32
最高次数	5	5	6	5	5	6	5	6

此外，我们对 8 个 S 盒全相同的情况做了演化试验，发现它们可以提供更高的安全指数，并且具有设计简单，演化速度快等明显优点。就此将另文发表。

5 结论

本文提出了演化密码的概念和用演化计算设计密码的方法。具体对 DES 分组密码的核心部件 S 盒组进行了实际演化，得到一种用演化方法设计 S 盒组的方法，并获得了一批抗差分攻击能力优异的 S 盒组。据此可知，通过演化的方法设计密码是获得高强度密码的一种有效方法。再者，若用演化方法构造出一族安全性能渐强的 S 盒组或其它部件，分别以这些 S 盒组或其它部件构造 DES，从而就可使 DES 密码体制本身进行演化，这一族安全性能愈来愈强的 DES 密码体制便是本文所提出的演化密码的一个具体实例。演化密码由于其安全性能愈来愈强且结构同一，在实际应用中有重要意义。

参考文献：

[1] 张焕国等. 计算机安全保密技术[M].北京：机械工业出版社，1995.

[2] 康立山等. 演化计算[M].北京：清华大学出版社，1999.

[3] 冯登国等. 分组密码的设计与分析[M].北京：清华大学出版社，2000.

[4] 王育民等. 通信网的安全技术与理论[M]. 西安：西安电子科技大学出版社，1999.

[5] 陈克非. 门限 RSA 密码体制[J]. 电子学报，1999，27(6): 134-135.