

一种关于分组密码的新的统计检测方法

陈 华¹⁾ 冯登国¹⁾ 范丽敏^{1),2)}

¹⁾(中国科学院软件研究所信息安全国家重点实验室 北京 100190)

²⁾(中国科学院研究生院 北京 100039)

摘 要 统计检测在分组密码安全性评估的过程中发挥着重要的作用,许多密码标准组织纷纷把对分组密码的统计检测作为评估过程中的重要环节来实施.文中提出了一种有效、实用的统计检测方法,该统计检测方法以分组长度为统计单位,将一个分组的某一字节取遍所有的值而其它字节固定不变,经过密码变换后,将256个输出值进行异或,通过检测输出异或值每一位为0(或1)的概率是否为1/2来判断分组密码是否随机.该检测方法可以一定程度地反映出分组密码抵抗积分攻击的能力.与此同时,基于推广的积分攻击方法,文中在已有方法的基础上提出了更一般的统计检测方法.另外,文中分别对Rijndael算法、Camellia算法和SMS4算法进行了统计检测,这3种算法分别从第4轮、第5轮和第7轮开始呈现出良好的统计性能.

关键词 统计检测;分组密码;安全性评估;积分攻击

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.00595

A New Statistical Test on Block Ciphers

CHEN Hua¹⁾ FENG Deng-Guo¹⁾ FAN Li-Min^{1),2)}

¹⁾(State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190)

²⁾(Graduate University of Chinese Academy of Sciences, Beijing 100039)

Abstract Statistical tests are playing very important part in the security evaluation on block ciphers, which have been applied by many cryptographic standard organizations in the evaluation process. In this paper, an effective and practical statistical test is proposed, which takes block size as the statistics unit. In the test, one state byte of a block is taken all possible values while other bytes are fixed, and after cryptographic transformation 256 output values are applied XOR(exclusive-or) operation. By testing whether every output bit of XORed value is 0 with probability 1/2, the randomness of block ciphers can be judged. The method can also somewhat reflect the resistance ability of a block cipher to integral attack. Meanwhile, based on the generalized integral attack, a more generalized statistical test is proposed on the basis of the given method. Moreover, the proposed statistical test is applied on Rijndael, Camellia and SMS4 algorithm, and good statistical property begins to behave respectively after 4 round, 5 round and 7 round operation.

Keywords statistical test; block cipher; security evaluation; integral attack

1 引 言

分组密码是现代密码学中的一个重要研究分

支,它因具有速度快、易于标准化和便于软硬件实现等特点而在计算机通信和信息系统安全领域中有着极其广泛的应用.分组密码主要由加密算法、解密算法和密钥编排算法三部分组成.对于分组密码而言,

安全性是其最重要的特性,只有在安全性得到保证的基础上,才能考虑其它因素.在分组密码的安全性评估中,密码分析发挥着重要的作用,通过它可以判断算法能否抵抗现有的各种可能的密码攻击.目前已存在大量的密码分析方法,如分组密码的线性分析方法、差分分析方法、相关密钥分析方法等等^[1].这些分析方法的实施过程往往比较复杂,并严重依赖于具体的密码结构,因而对每一种密码算法进行具体实施时都需要由密码专家进行专门的分析.

除了密码分析以外,统计检测在分组密码安全性评估的过程中同样发挥着重要的作用.与密码分析相比,统计检测具有自动化程度高、检测模型通用化等诸多优点,因此许多密码标准组织纷纷把对密码算法的检测作为评估过程中的重要环节来实施.目前关于分组密码的统计检测方法主要是将分组密码作为一个伪随机数发生器进行检测,即检测分组密码输出序列的随机性能的好坏.目前已出现了十余种随机性检测算法,如频数检测、重叠子序列检测、扑克检测、游程检测、线性复杂度检测、近似熵检测以及离散傅立叶变换检测等等^[2-3]①.在 AES 的评选过程中,算法评估组选择了 16 种随机性检测算法对候选算法输出的随机性能进行了统计检测,任何一个不能通过随机性检测的算法都会被淘汰^[3-4].除此以外,还有一类统计检测方法是与分组密码的分组长度、密码结构等有关的,如明文雪崩检测、密钥雪崩检测、明密文独立性检测、仿射特性检测以及互补特性检测等等^[1,5-7].

本文提出了一种新的统计检测方法,它属于第二类统计检测方法.该统计检测方法以分组长度为统计单位,将一个分组的某一字节取遍所有的值而其它字节固定不变,经过密码变换后,将 256 个输出值进行异或,通过检测输出异或值每一位为 0(或 1)的概率是否为 1/2 来判断分组密码是否随机.该统计检测方法还可以一定程度地反映出待测分组密码抵抗积分攻击的能力.利用该统计检测方法,我们对三种具有不同密码结构的流行分组密码算法进行了统计分析,它们分别是 Rijndael 算法^[8]、Camellia 算法^[9]和 SMS4 算法^②.检测结果表明,这 3 种算法分别从第 4 轮、第 5 轮和第 7 轮开始呈现出良好的统计性能.与此同时,基于推广的积分攻击方法,我们在已有方法的基础上提出了更一般的统计检测方法.

2 背景知识

一个 n 元布尔函数可以表示为 $f(x):F_2^n \rightarrow F_2$, 则所有 n 元布尔函数的总个数为 2^{2^n} . 对于任意的 $x \in F_2^n$, 共有 2^{2^n-1} 个 n 元布尔函数的取值为 1. 因此对于一个随机选取的 n 元布尔函数 f , $P(f(x)=1) = \frac{1}{2}$. 不难证明,若对 f 的所有输出进行异或,则异或值取 1 的概率应该为 $\frac{1}{2}$. 令 $\delta(f(x)) = \bigoplus_{x=0}^{2^n-1} f(x)$, 则

$$P(\delta(f(x))=1) = \frac{1}{2}.$$

$F(x):F_2^n \rightarrow F_2^m$ 表示一个多输出的布尔函数,也称为一个 (n,m) 布尔函数. $F(x)$ 也可表示为多个布尔函数的组合,即 $F(x) = [f_1(x), f_2(x), \dots, f_m(x)]$. 显然,对于一个随机选取的 $F(x)$, $f_i(x)$ ($1 \leq i \leq m$) 也是随机的并且相互独立,所以

$$P(\delta(f_i(x))=1) = \frac{1}{2}.$$

对于 $F(x):F_2^n \rightarrow F_2^m$, $C \in F_2^t$, $1 \leq i_1 < i_2 < \dots < i_t \leq n$, $1 \leq j_1 < j_2 < \dots < j_{n-t} \leq n$, $(i_1, i_2, \dots, i_t) \cap (j_1, j_2, \dots, j_{n-t}) = \emptyset$, 定义 $G_{[C, F, (i_1, i_2, \dots, i_t)]}(x):F_2^{n-t} \rightarrow F_2^m$, 令 $G_{[C, F, (i_1, i_2, \dots, i_t)]}(x) = [g_1(x), g_2(x), \dots, g_m(x)]$, $g_l(x)$ ($1 \leq l \leq m$) 为 n 元布尔函数,其中 $g_l(x) = f_l((x_{i_1}, x_{i_2}, \dots, x_{i_t}) = C, (x_{j_1}, x_{j_2}, \dots, x_{j_{n-t}}) = x)$. 在这里称 $G_{[C, F, (i_1, i_2, \dots, i_t)]}(x)$ 为 $F(x)$ 的衍生函数. 显然,对于一个随机选取的 $F(x)$, $G_{[C, F, (i_1, i_2, \dots, i_t)]}(x)$ 同样也是随机的. 所以 $g_l(x)$ 随机并且相互独立,从而

$$P(\delta(g_l(x))=1) = \frac{1}{2}.$$

以上背景知识为后面提出的统计检测方法奠定了基本的理论基础. 接下来简单介绍一下皮尔逊假设检验^[10],它在后面提出的统计检测中会被使用.

假设总体 ξ 是一个离散型随机变量,其可能的取值为 x_1, x_2, \dots, x_l . 为了检验假设:

$$H_0: P\{\xi=x_i\} = p_i, i=1, 2, \dots, l.$$

抽取容量为 n 的样本得到 n 个样本数据,将样本数据按不同的取值进行分组整理,列成如表 1 所示的频数分布表.

① Marsaglia G. DIEHARD statistical Tests. <http://sta.fsu.edu/~geo/diahard.html>

② 国家商用密码管理办公室. 无限局域网中使用的 SMS4 密码算法. <http://www.oscca.gov.cn/UpFile/200621016-423197990.pdf>

表 1 样本频数分布表

ξ	频数
x_1	n_1
x_2	n_2
x_3	n_3
...	...
x_l	n_l

其中, $n_i \geq 0, i = 1, 2, \dots, l$, 且 $\sum_{i=1}^l n_i = n$.

若 H_0 为真, 则 ξ 的概率分布如表 2 所示.

表 2 样本频数分布表

ξ	概率
x_1	p_1
x_2	p_2
x_3	p_3
...	...
x_l	p_l

由大数定律可知, 当 n 充分大时, 事件 $\{\xi = x_i\}$ 发生的频率 $\frac{n_i}{n}$ 与理论概率 p_i 的差应该很小. 于是, 可以构造反映这一差异的一个统计量:

$$\chi^2 = \sum_{i=1}^k \frac{n((n_i/n) - p_i)^2}{p_i} = \sum_{i=1}^k \frac{(n_i - np_i)^2}{np_i},$$

其中, $k \leq l$, 称为实际分组数. 这个统计量是实测频数 n_i 与理论组频数 np_i 离差平方的加权和. 它反映了样本实测组频数 $n_i (i = 1, 2, \dots, k)$ 与理论组频数 $np_i (i = 1, 2, \dots, k)$ 之间差异的大小, 称这个统计量为皮尔逊 χ^2 统计量. 当 H_0 为真时, χ^2 统计量的值应该小. 所以, 如果皮尔逊统计量的值大到超过某个界限 λ 时, 就怀疑 H_0 的正确性而拒绝接受 H_0 . 因此, 拒绝假设 H_0 的拒绝域为 $\chi^2 > \lambda$. λ 的确定依赖于皮尔逊 χ^2 统计量的分布, 而它的精确分布难以求得, 皮尔逊给出了它的一个近似分布. 不论 ξ 是什么分布, 当假设 H_0 为真时, 则统计量 χ^2 的极限分布就是自由度为 $k - r - 1$ 的 χ^2 分布. 其中, k 为实际分组数, r 为统计量 χ^2 中未知参数的个数.

3 一种新的统计检测方法

3.1 检测方法描述

我们知道, 在通常情况下, 分组密码实际上就是一族 (n, n) 布尔函数, 每一个密钥对应着一个 (n, n) 布尔函数. 在密钥 k 的作用下, 分组密码可以表示为 $F_k(x): F_2^n \rightarrow F_2^n$. 对于一个安全的分组密码来说, $F_k(x)$ 应该是一个随机的 (n, n) 布尔函数. 因此, 若我们固定明文输入的一些比特, 则得到的衍生函数

仍然是随机的. 根据前面介绍的背景知识, 本节提出一种针对分组密码的新的统计检测方法. 以下是对检测过程的详细描述.

对于一个分组长度为 n 比特的分组密码, 首先随机生成 F 个明文分组和 1 个密钥, 第 i 个明文分组表示为 $P_i = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, p_{i_{m-1}}\}$, 其中 $m = n/8, p_{i_j} \in F_2^8, 0 \leq j \leq m-1, 0 \leq i \leq F-1$. 现令 $p_{i_j} = 0, 1, \dots, 255$, 其它字节不变, 得到以下 256 个明文分组:

$$\begin{aligned} P_i^0 &= \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 0, p_{i_{j+1}}, \dots, p_{i_{m-1}}\}, \\ P_i^1 &= \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 1, p_{i_{j+1}}, \dots, p_{i_{m-1}}\}, \\ &\vdots \\ P_i^{255} &= \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 255, p_{i_{j+1}}, \dots, p_{i_{m-1}}\}. \end{aligned}$$

对以上 256 个明文分组分别加密, 得到相应的 256 个密文分组:

$$\begin{aligned} C_i^0 &= \{c_{i_0}^0, c_{i_1}^0, c_{i_2}^0, \dots, c_{i_{m-1}}^0\}, \\ C_i^1 &= \{c_{i_0}^1, c_{i_1}^1, c_{i_2}^1, \dots, c_{i_{m-1}}^1\}, \\ &\vdots \\ C_i^{255} &= \{c_{i_0}^{255}, c_{i_1}^{255}, c_{i_2}^{255}, \dots, c_{i_{m-1}}^{255}\}. \end{aligned}$$

将以上 256 个密文进行异或操作, 得到 $C'_i = C_i^0 \oplus \dots \oplus C_i^{255}$. 由第 2 节的背景知识得知, 若分组密码可看作是一个随机的多输出布尔函数, 则 C'_i 应服从二项分布 $B(n, 1/2)$. 令 $D_i = W(C'_i)$, 在这里 W 统计了 C'_i 的汉明重量 (即 C'_i 中 1 的个数). 然后统计 $D_i (0 \leq i \leq F-1)$ 中汉明重量为 $w (0 \leq w \leq n)$ 的分组数, 记为 H_w . 将 H_w 与期望数 $E_w = C_n^w \times F/2^n$ 进行皮尔逊拟合 χ^2 检验, 将计算结果与显著性水平为 α 的 χ^2 阈值相比较, 来判断 H_w 是否服从二项分布 $B(n, 1/2)$. 显然, 随着被遍历字节位置的不同, 共有 $m = n/8$ 个检测结果, 只有当所有 m 个检测结果都服从二项分布 $B(n, 1/2)$ 时, 才表明分组密码通过该项统计检测, 否则说明分组密码存在明显的统计弱点.

3.2 与积分攻击的关系

积分攻击是一种非常重要的面向字节的分组密码分析方法^[11]. 该分析方法是一种选择明文攻击方法, 其基本思想是: 通过分析一些中间状态的“和”经过几轮密码变换后的演变来恢复某些密钥比特.

设分组密码的分组长度为 n 比特, $m = n/8$. 在积分攻击中, 让一组明文在 $m-1$ 个字节上都取相同的值, 另外 1 个字节上遍历 256 个所有的可能取值, 这样得到的一个结构称做一个 Δ -集合. 更一般地, 如下定义 Δ -集合:

设 λ 是一个由元素 i 组成的索引集合, 其中 $0 \leq i \leq m-1$. 定义 $\Lambda(\lambda)$ 是一个含有 256 个状态的集合, 满足

$$\forall x, y \in \Lambda \Rightarrow \begin{cases} x_i \neq y_i, & i \in \lambda \\ x_i = y_i, & i \notin \lambda \end{cases}.$$

在这里, 若 $i \in \lambda$, 则称位置为 i 的字节状态为活动的 (active), 否则就是非活动的 (passive). 一个 Λ -集合经过几轮密码变换后, 输出集合中字节状态分为 4 种, 第 1 种是活动的, 第 2 种是非活动的, 第 3 种就是平衡的 (即异或值为 0), 最后一种是未知状态. 显然, 若字节状态是活动的或非活动的, 它们实际也是平衡的. 在积分攻击中, 会寻找这样的 Λ -集合, 在经过 r 轮密码变换后 (在这里 r 要尽可能大, 以便增加攻击轮数), 其输出集合中含有状态为平衡的字节. 在这种情况下, 称分组密码存在一个 r 轮积分特征, 积分攻击会利用这种积分特征抛弃大量错误的猜测密码, 从而恢复某些密钥比特. 那么积分攻击与我们提出的统计检测方法有什么关系呢? 定理 1 给出了它们之间存在的关系.

定理 1. 设 Λ -集合中仅第 k 个字节是活动的, 若经过 r 轮密码变换, 其输出集合中含有状态为平衡的, 则 r 轮密码变换不会通过 3.1 节提出的统计检测方法.

证明. 按照 3.1 节提出的统计检测方法, 随机生成 F 个明文分组和 1 个密钥, 第 i 个明文分组表示为 $P_i = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, p_{i_{m-1}}\}$, 其中 $m = n/8$, $p_{i_j} \in F_2^8$, $0 \leq j \leq m-1$, $0 \leq i \leq F-1$. 现令 $p_{i_k} = 0, 1, \dots, 255$, 其它字节不变, 得到以下 256 个明文分组:

$$P_i^0 = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 0, p_{i_{k+1}}, \dots, p_{i_{m-1}}\},$$

$$P_i^1 = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 1, p_{i_{k+1}}, \dots, p_{i_{m-1}}\},$$

\vdots

$$P_i^{255} = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, 255, p_{i_{k+1}}, \dots, p_{i_{m-1}}\}.$$

显然这是一个 Λ -集合, 其中仅第 k 个字节是活动的. 经过 r 轮密码变换后, 得到相应的 256 个密文分组:

$$C_i^0 = \{c_{i_0}^0, c_{i_1}^0, c_{i_2}^0, \dots, c_{i_{m-1}}^0\},$$

$$C_i^1 = \{c_{i_0}^1, c_{i_1}^1, c_{i_2}^1, \dots, c_{i_{m-1}}^1\},$$

\vdots

$$C_i^{255} = \{c_{i_0}^{255}, c_{i_1}^{255}, c_{i_2}^{255}, \dots, c_{i_{m-1}}^{255}\}.$$

将以上 256 个密文进行异或操作, 得到

$$C'_i = \{c_{i_0}^0 \oplus c_{i_1}^1 \oplus \dots \oplus c_{i_0}^{255}, c_{i_1}^0 \oplus c_{i_1}^1 \oplus \dots \oplus c_{i_1}^{255}, \dots, c_{i_{m-1}}^0 \oplus c_{i_{m-1}}^1 \oplus \dots \oplus c_{i_{m-1}}^{255}\},$$

因为经过 r 轮密码变换, 集合 $\{C_i^0, C_i^1, \dots, C_i^{255}\}$ 中含有状态为平衡的字节, 不妨设其中某一平衡字节的位置为 t , 则 $c_{i_t}^0 \oplus c_{i_t}^1 \oplus \dots \oplus c_{i_t}^{255} = 0$. 令 $C'_{i,j}$ 表示 C'_i 的第 j 比特, 则 $P(C'_{i,s} = 0) = 1 \neq \frac{1}{2}$, $8t \leq s \leq 8t+7$. 显然, C'_i 不服从二项分布 $B(n, 1/2)$. 因此, r 轮密码变换不会通过 3.1 节提出的统计检测方法. 证毕.

定理 1 给出了积分攻击与本文提出的统计检测方法之间的关系, 但其逆命题不一定成立. 也就是, 当 r 轮分组密码没有通过统计检测时, 则仅第 k 个字节是活动的 Λ -集合, 经过 r 轮密码变换, 其输出集合中不一定含有状态为平衡的元素, 后面第 4 节的实验结果也验证了这一点.

3.3 推广的统计检测方法

3.2 节介绍了一种最常见的积分攻击方法. 除此之外, 积分攻击还可以推广为更一般的情形. 首先, 明文 Λ 集合的选取不一定是针对某一个字节, 可以推广为更一般的几个比特; 其次, 针对密文集合的运算可以考虑比较特殊的任意几个比特, 运算可以是异或操作或者是其它的一些操作. 基于推广的积分攻击方法, 我们可以在 3.1 节的基础上提出一种更为一般的统计检测方法. 为了便于描述, 在这里密文的运算还是考虑异或运算. 以下是对检测过程的详细描述.

对于一个分组长度为 n 比特的分组密码, 首先随机生成 F 个明文分组和 1 个密钥, 第 i 个明文分组表示为 $P_i = \{p_{i_0}, p_{i_1}, p_{i_2}, \dots, p_{i_{n-1}}\}$, 其中 $p_{i_j} \in F_2$, $0 \leq j \leq n-1$, $0 \leq i \leq F-1$. 现令 P_i 的第 j_1, j_2, \dots, j_t 位取遍所有可能的值 (其中 $0 \leq j_1 < j_2 < \dots < j_t \leq n-1$), 其它位保持不变, 得到以下明文分组:

$$P_i^0 = \{p_{i_0}, p_{i_1}, \dots, 0, p_{i_{j_1+1}}, \dots, 0, p_{i_{j_t+1}}, \dots, p_{i_{n-1}}\},$$

$$P_i^1 = \{p_{i_0}, p_{i_1}, \dots, 0, p_{i_{j_1+1}}, \dots, 1, p_{i_{j_t+1}}, \dots, p_{i_{n-1}}\},$$

\vdots

$$P_i^{2^t-1} = \{p_{i_0}, p_{i_1}, \dots, 1, p_{i_{j_1+1}}, \dots, 1, p_{i_{j_t+1}}, \dots, p_{i_{n-1}}\}.$$

对以上 2^t 个明文分组分别加密, 得到相应的 2^t 个密文分组:

$$C_i^0 = \{c_{i_0}^0, c_{i_1}^0, c_{i_2}^0, \dots, c_{i_{n-1}}^0\},$$

$$C_i^1 = \{c_{i_0}^1, c_{i_1}^1, c_{i_2}^1, \dots, c_{i_{n-1}}^1\},$$

\vdots

$$C_i^{2^t-1} = \{c_{i_0}^{2^t-1}, c_{i_1}^{2^t-1}, c_{i_2}^{2^t-1}, \dots, c_{i_{n-1}}^{2^t-1}\}.$$

现在我们只考虑密文分组中第 k_1, k_2, \dots, k_r 比

特的情况 (其中 $0 \leq k_1 < k_2 < \cdots < k_r \leq n-1$), 令 $C_i^s[k_1, k_2, \cdots, k_r] = \{c_{i_{k_1}}^s, c_{i_{k_2}}^s, \cdots, c_{i_{k_r}}^s\}, 0 \leq s \leq 2^t-1$. 将 $C_i^s[k_1, k_2, \cdots, k_r]$ 进行异或操作, 得到 $C_i'[k_1, k_2, \cdots, k_r] = C_i^0[k_1, k_2, \cdots, k_r] \oplus \cdots \oplus C_i^{2^t-1}[k_1, k_2, \cdots, k_r]$. 令 $D_i = W(C_i'[k_1, k_2, \cdots, k_r])$, 然后统计 $D_i (0 \leq i \leq F-1)$ 中汉明重量为 $w (0 \leq w \leq r)$ 的分组数, 记为 H_w . 将 H_w 与期望数 $E_w = C_r^w \times F/2^r$ 进行皮尔逊拟合 χ^2 检验, 将计算结果与显著性水平为 α 的 χ^2 阈值相比较, 来判断 H_w 是否服从二项分布 $B(r, 1/2)$.

4 典型分组密码的统计分析

本节我们将利用 3.1 节提出的统计检测方法对目前几个流行的具有不同密码结构的分组密码算法进行统计分析, 它们分别是 Rijndael、Camellia 和 Sms4 分组密码算法. Rijndael 算法是由美国国家标准技术研究所评选出来的高级数据加密标准^①, 采用了 SPN 结构, 分组长度为 128 比特, 密钥长度

为 128、192 和 256 比特, 对应的加密轮数分别为 10、12 和 14. Camellia 算法是欧洲密码标准计划 NESSIE^② 和日本 CRYPTREC^③ 计划的建议标准算法, 采用了 Feistel 结构, 分组长度为 128 比特, 密钥长度为 128、192 和 256 比特, 对应的加密轮数分别为 18 和 24 (192/256 比特). Sms4 算法是用于 WAPI 的分组密码算法, 它是国内官方公布的第一个商用密码算法, 它的分组长度和密钥长度均为 128 比特, 加密算法与密钥扩展算法都采用 32 轮非线性迭代结构.

在对上面 3 个分组密码算法进行统计检测之前, 我们将检测样本的长度设为 10000×128 比特, 即 $F=10000$, 检测样本的个数设为 100, 显著性水平设为 0.05. 表 3~5 分别给出了针对 Rijndael、Camellia 和 Sms4 算法的统计分析结果. 限于篇幅, 在这里我们只对 128 比特密钥的密码算法进行统计分析, 并且加密轮数均不超过 10 轮. 表中数据记录了 100 次检测实验的通过比率.

表 3 Rijndael 算法统计分析结果

轮数	通过比率/%															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	97	97	93	99	94	94	94	96	92	93	97	96	98	93	95	96
5	96	97	90	97	99	95	94	96	98	97	93	95	98	94	99	92
6	95	94	94	99	96	97	96	91	93	94	96	95	95	93	93	100
7	99	97	95	96	96	95	98	95	97	97	95	90	91	97	94	97
8	93	94	97	96	94	90	98	88	97	95	95	93	92	91	94	94
9	98	94	95	95	94	95	97	91	92	94	94	92	97	94	96	98
10	97	94	93	99	93	95	96	97	97	95	96	99	93	94	96	90

表 4 Camellia 算法统计分析结果

轮数	通过比率/%															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	96	93	94	97	98	95	96	95	0	0	0	0	0	0	0	0
5	95	95	97	94	95	91	96	93	95	97	94	97	92	97	94	93
6	96	97	96	96	96	94	94	96	97	95	94	99	93	95	88	94
7	95	95	94	94	98	96	94	93	89	97	92	99	95	93	98	99
8	97	96	93	95	93	97	92	96	94	97	94	95	97	98	98	98
9	95	97	97	99	95	96	94	93	93	97	98	95	91	94	93	94
10	95	98	92	95	94	95	95	98	93	94	96	97	91	98	94	95

① AES website: <http://www.nist.gov/aes/>

② NESSIE website: <https://www.cosic.esat.kuleuven.ac.be/nessie/>

③ CRYPTREC website: <http://www.ipa.go.jp/security/enc/CRYPTREC/indexe.html>

表 5 Sms4 算法统计分析结果

轮数	通过比率/%															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	96	97	96	92	96	96	97	94	93	97	96	96
7	96	90	97	96	93	93	98	89	97	98	95	100	94	91	97	92
8	96	97	94	94	96	94	94	91	93	98	93	95	94	96	94	94
9	95	94	98	91	95	97	95	93	98	94	96	94	96	98	90	95
10	92	94	94	93	98	94	97	96	96	94	96	97	97	94	93	95

从表 3 可以看出 Rijndael 算法的前 3 轮密码变换的通过率均为 0,从第 4 轮开始算法开始呈现出良好的统计特性.而事实上是存在着这样的 Δ -集合(仅有一个字节是活动的,字节位置不限),经过 1~3 轮的密码变换,其输出集合中是含有状态为平衡的元素的,其分析结果可以参见文献[12],因此与我们的检测结果是吻合的.从表 4 可以看出 Camellia 算法的前 3 轮密码变换的通过率均为 0,第 4 轮的第 8~15 个的检测结果的通过率为 0,而第 4 轮的第 0~7 个的检测结果以及 5 轮之后的检测结果均呈现出了良好的统计特性.文献[13]对 Camellia 的积分分析结果表明,若输入为 Δ -集合(仅有一个字节是活动的),最多经过 4 轮变换,其输出集合中是含有状态为平衡的元素的.另外还证明了仅当输入 Δ -集合中活动字节的位置在明文的右半部分时,经过 4 轮变换才能保证输出集合中是含有状态为平衡的元素.这与我们的检测结果也是相吻合的.从表 5 可以看出 Sms4 算法的前 5 轮密码变换的通过率均为 0,第 6 轮的第 0~3 个的检测结果的通过率为 0,而第 6 轮的第 4~15 个的检测结果以及 7 轮之后的检测结果均呈现出了良好的统计特性.经过我们的验证,若输入为 Δ -集合(仅有一个字节是活动的),最多经过 5 轮变换,其输出集合中是含有状态为平衡的元素的.第 6 轮的第 0~3 个的检测结果的通过率虽然为 0,但经过 6 轮变换后,其输出集合中是不含有状态为平衡的元素的,从而验证了定理 1 的逆命题不一定成立.

5 结 论

本文提出了一种针对分组密码的新的统计检测方法,该统计检测以分组长度为统计单位,基本思想是将某一输入字节取遍所有的值而其它字节固定不

变,经过密码变换后,将 256 个输出值进行异或,最后检测输出异或值每一位为 0(或 1)发生的概率是否为 1/2.本文在提出统计检测方法的同时,也证明了它与积分攻击之间存在着一定的关系,这种关系可以帮助我们充分利用检测结果去进行更深入的密码分析.与此同时,基于推广的积分攻击方法,我们在已有方法的基础上提出了更一般的统计检测方法.最后本文分别对 Rijndael、Camellia 和 Sms4 算法进行了统计分析,统计结果表明,这 3 种算法分别从第 4 轮、第 5 轮和第 7 轮开始呈现出良好的统计性能.该检测结果同时也验证了新的统计检测方法

参 考 文 献

[1] Feng Deng-Guo, Wu Wen-Ling. Design and Analysis of Block Cipher. Beijing: Tsinghua University Press, 2000(in Chinese)
(冯登国, 吴文玲. 分组密码设计与分析. 北京: 清华大学出版社, 2000)

[2] Knuth D E. Seminumerical Algorithms, Volum 2 of the Art of Computer Programming. Massachusetts: Addison-Wesley, 1981

[3] Rukhlin A, Soto J et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report, NIST Special Publication 800-22, 2001

[4] Soto Juan, Bassham Lawrence. Randomness testing of the advanced encryption standard finalist candidates. Computer Security Division. NIST IR 6483, 2000

[5] Gustafson H, Dawson E, Nielsen L, Caelli W. A computer package for measuring the strength of encryption algorithms. Computers and Security, 1994, 13(8): 687-697

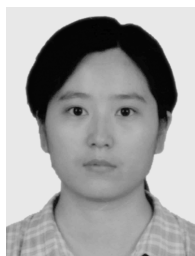
[6] Chen Hua. Security test on cryptographic algorithms and design of key cryptographic components[Ph. D. dissertation]. Institute of Software, Chinese Academy of Sciences, Beijing, 2005(in Chinese)

(陈华. 密码算法的安全性检测及关键组件的设计[博士学位论文]. 中国科学院软件所, 北京, 2005)

- [7] Chen Hua, Wu Chuan-Kun, Feng Deng-Guo. On statistical properties of S-boxes in block ciphers. *Journal of Electronics*, 2005, 14(4): 584-587
- [8] Daemen J, Rijmen V. *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin: Springer, 2002
- [9] Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J, Tokita T. Specification of Camellia—A 128-bit block cipher//*Proceedings of the Selected Areas in Cryptography (SAC' 2000)*. Canada, 2000, Berlin: Springer-Verlag, 2001: 183-191
- [10] Sheng Zhou, Xie Shi-Qian et al. *Probability and Statistics*. 2nd Edition. Beijing: Higher Education Press, 1989(in

Chinese)

- (盛骤, 谢式千等. 概率论与数理统计. 第2版. 北京: 高等教育出版社, 1989)
- [11] Knudsen L, Wagner D. Integral cryptanalysis//*Proceedings of the Fast Software Encryption (FSE'02)*. LNCS 2365. Belgium. Berlin: Springer-Verlag, 2002: 112-127
- [12] Daemen J, Rijmen V. The block cipher Rijndael//*Proceedings of the 1st AES Candidate Conference (AES1)*. Ventura, California, USA, 1998, NIST Journal of Research, 1998, 104(5)
- [13] He Ye-Ping, Qing Si-Han. Square attack on reduced Camellia cipher//*Proceedings of the Information and Communication Security (ICICS'01)*. LNCS 2229. Xian, 2001. Berlin: Springer-Verlag, 2001: 238-245



CHEN Hua, born in 1976, Ph. D., associate researcher. Her research interests include cryptography and information security.

FENG Deng-Guo, born in 1965, researcher. Ph. D. supervisor. His research interests include cryptography and information security.

FAN Li-Min, born in 1978, Ph. D. candidate. Her research interests include cryptography and information security.

Background

Cryptographic algorithms are playing core roles in information security, which can provide confidentiality, integrity and authenticity of information. During the design and analysis of cryptographic algorithms, how to evaluate the algorithms is becoming a key problem.

There have existed many avenues to evaluate cryptographic algorithms, among which the statistical test is very important. Compared with cryptographic analysis, statistical tests have many advantages including high automation, generic test models and so on. Currently, many cryptographic standard plans have applied statistical tests in the process of the evaluation on cryptographic algorithms. The standard plans contain AES (Advanced Encryption Standard), NES-SIE (New European Schemes for Signature, Integrity, and Encryption), ECRYPT (European Network of Excellence for Cryptology) and so on.

To sum up, there are two kinds of statistical tests on cryptographic algorithms. The first one is the pure randomness test on the output sequences of cryptographic algorithms, under which cryptographic algorithms are thought of

pseudorandom number generators. Up to now, there have existed a lot of randomness test methods such as frequency test, run test, poker test, autocorrelate test and so on. Besides the randomness test, another kind of statistical tests is based on the size and structure of cryptographic algorithms. Compared with the first one, the second one can detect the statistical weaknesses more easily. Unfortunately, the research on the second kind of statistical tests is still weak.

In this paper, an effective and practical statistical test on block ciphers is proposed, which belongs to the second kind of statistical tests. In the test, one state byte of a block is taken all possible values while other bytes are fixed, and after cryptographic transformation 256 output values are applied XOR (exclusive-or) operation. By testing whether every output bit of XORed value is 0 with probability 1/2, the randomness of block ciphers can be judged. The method can also somewhat reflect the resistance ability of a block cipher to integral attack. The research work in this paper can be used in the future practical cryptographic evaluation on block ciphers.