对 8 轮 ARIA 算法的差分枚举攻击

陈少真 鲁林真*
(解放军信息工程大学信息工程学院 郑州 450002)

摘 要：给出了 ARIA 算法 4 轮差分性质，提出了对 ARIA 算法的差分枚举攻击。攻击了 7 轮和 8 轮 ARIA-256 算法，攻击的数据复杂度是 2^{56}，攻击 7 轮时预计算的复杂度为 $2^{238.2}$ 次加密 7 轮 ARIA 算法，恢复密钥的计算复杂度是 $2^{124.2}$ 次加密 7 轮 ARIA 算法；攻击 8 轮时预计算的复杂度为 2^{238} 次加密 8 轮 ARIA 算法，恢复密钥的计算复杂度是 $2^{253.6}$ 次加密 8 轮 ARIA 算法。

关键词：分组密码；ARIA；差分分析
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2011)07-1770-05
DOI: 10.3724/SP.J.1146.2010.01292

Differential Enumeration Attack on ARIA

Chen Shao-zhen Lu Lin-zhen
(*Institute of Information Engineering*, *PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: The 4-round ARIA differential property is given, and the differential enumeration attack on 7-round and 8-round ARIA-256 is presented in this paper. The attacks need 2^{56} chosen plaintexts. The attack on 7-round ARIA has the time complexity of $2^{238.2}$ 7-round ARIA encryptions in the preprocessing phase and $2^{124.2}$ 7-round ARIA encryptions in the processing phase. The attack on 8-round ARIA has the time complexity of 2^{238} 8-round ARIA encryptions in the preprocessing phase and $2^{253.6}$ 8-round ARIA encryptions in the processing phase.

Key words: Block cipher; ARIA; Differential cryptanalysis

1 引言

分组密码算法 ARIA[1]是 128 bit 分组长度的韩国标准密码算法，密钥长度分别为 128，192 和 256 bit，对应的轮数分别为 12, 14 和 16。设计者给出了对 ARIA 算法的一些基本攻击，如差分和线性攻击，截段差分攻击，不可能差分攻击，积分攻击，插值攻击等。随后文献[2]主要给出了截段差分攻击和线性攻击结果。设计者声称不存在 4 轮不可能差分区分，文献[3]给出一些 4 轮不可能差分区分并分析了 6 轮的 ARIA 算法。文献[4]提出了对 6 轮算法的飞去来器攻击，文献[5]发表了对 ARIA 算法的新飞去来器攻击。文献[6]给出了 4 轮积分区分。最近文献[7]给出了中间相遇攻击的结果，可以攻击 8 轮 ARIA-256 算法。

中间相遇攻击的思想由 Demirci 等人[8]提出，并利用该思想分析了 IDEA 分组密码算法。对 AES 算法的中间相遇攻击首先由 Demirci 等人[9]给出，随后 Dunkelman 等人[10]改进了这种攻击，给出复杂度更低的结果。

2010-11-22 收到，2011-02-28 改回
国家自然科学基金(60833008)资助课题
*通信作者：鲁林真 cipfytcx@yahoo.cn

在中间相遇攻击思想的基础上，本文提出了对 ARIA 算法的差分枚举攻击。这种攻击分为两部分：首先建立一个差分筛选集合，其次分析每个候选密钥并以筛选集合为标准来判断密钥的正误。利用差分枚举攻击的原理对 ARIA 算法进行分析，给出了 4 轮 ARIA 算法的差分性质，在此基础上实现了对 7 轮和 8 轮 ARIA-256 算法的攻击。

2 差分枚举攻击

中间相遇攻击的思想是首先建立特殊明文所对应的筛选集合，其次选出满足特殊明文要求的明密文对，接着猜测密钥，然后部分解密对应的密文得到所需值。所得的值与筛选集合中的元素相比较，如果猜测的密钥是正确的，那么计算值和集合中的一个元素是一致的；如果不一致，那么密钥是错误，这样就可以排除错误的候选密钥。本文首次提出差分枚举攻击，差分枚举攻击是对中间相遇攻击的进一步扩展。进行差分枚举攻击时，首先建立明文差分集合所对应的所有差分筛选集合，然后猜测密钥，再部分加解密满足明文差分的明密文对，如果得到的密文差分和差分筛选集合是一致的，那么密钥可能是正确的，否则猜测的是错误的密钥。选择合适的明文差分集合，差分枚举攻击所建立差分筛选集

合的规模相比中间相遇攻击的筛选集合要小，即预计算的复杂度较低。

设 N 轮分组密码算法 $C=E(P,K)$, P,K,C 分别是明文，密钥和密文。整个算法可以看成是两部分的级联，记 $E=E_2\circ E_1$，其中 E_1,E_2 分别是 N_1,N_2 轮，K_1,K_2 分别对应于 E_1,E_2 的密钥，记 $M=E_1(P,K_1)$，$C=E_2(M,K_2)$。

令 D 为所有的明文差分构成的集合，$\mathcal{A}$ 为 D 的幂集合，$A\in\mathcal{A}$ 为一个明文差分集合，经过 E_1 加密，由于非线性变换使得与集合 A 对应的差分集合有多种可能，将所有与差分集合 A 对应的差分集合记为 $\mathcal{B}=\{B_i \mid B_i$ 为 A 所对应的一个差分集合，$1\le i\le n\}$。如果只考虑差分集合 $B_i(1\le i\le n)$ 中元素的部分字节，则差分集合记为 b_i。如果集合规模 n 足够小，即这样的 $b_i(1\le i\le n)$ 都可以计算出，那么就可以构造一个差分筛选集合。

构造的筛选集合可以看作是密码体制的一个区分，在此基础上就可以成功分析密码体制。

首先选定一个差分集合 A，计算出集合 A 所对应的所有差分集合 $b_i(1\le i\le n)$，所有的 b_i 组成的集合记为 $\mathcal{B}$。这一步称为预计算。

其次选择满足差分集合 A 的明文集合 $\mathcal{P}$，加密得到对应的密文集合 $\mathcal{C}$，猜测密钥 K_2 的部分比特 k 解密密文，求出所对应中间值的差分集合 m。

最后比较差分集合 m 和集合 $\mathcal{B}$ 中的所有元素，如果与其中的一个元素 b_i 一致，那么猜测的密钥可能是对的，否则密钥是错误的。一个错误的密钥解密得到差分集合与集合 $\mathcal{B}$ 中的一个元素一致的概率是：$n\cdot 2^{-l\times|m|}$，其中 l 是集合 m 中差分值的比特长度。当 $|m|$ 足够大就可以以极大的概率排除所有的错误密钥。

3　ARIA 算法

分组密码算法 ARIA 是 SPN 型的密码体制，扩散层使用了 $\mathrm{GF}(2^8)$ 上 16×16 的对合矩阵。混乱层包含 16 个的 8×8 的 S 盒。128 bit 的明密文看作 $\mathrm{GF}(2^8)$ 上的元素组成的 4×4 矩阵：

x_0	x_4	x_8	x_{12}
x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}

整个算法的轮函数包含轮密钥加，混乱层和扩散层。N 轮算法迭代 $N-1$ 次轮函数，最后一轮是把轮函数的扩散层替换为轮密钥加，即包含轮密钥加，混乱层和轮密钥加。由于在攻击过程中，密钥扩展算法对攻击没有影响，所以下面对密钥扩展算法不作说明。

轮密钥加(AK)：128 bit 轮密钥与状态异或。轮密钥由密钥扩展算法产生。

混乱层(SL)：非线性代换，这个操作是对状态的每个字节执行 S 盒，它包含两种 S 盒。奇数轮和偶数轮的混乱层有区别。

扩散层(DL)：一个对合的线性变换 $P:\mathrm{GF}(2^8)^{16}\to\mathrm{GF}(2^8)^{16}$。即

$$(x_0,x_1,\cdots,x_{15})\to(y_0,y_1,\cdots,y_{15})$$

其中

$$\begin{aligned}
y_0&=x_3\oplus x_4\oplus x_6\oplus x_8\oplus x_9\oplus x_{13}\oplus x_{14}\\
y_1&=x_2\oplus x_5\oplus x_7\oplus x_8\oplus x_9\oplus x_{12}\oplus x_{15}\\
y_2&=x_1\oplus x_4\oplus x_6\oplus x_{10}\oplus x_{11}\oplus x_{12}\oplus x_{15}\\
y_3&=x_0\oplus x_5\oplus x_7\oplus x_{10}\oplus x_{11}\oplus x_{13}\oplus x_{14}\\
y_4&=x_0\oplus x_2\oplus x_5\oplus x_8\oplus x_{11}\oplus x_{14}\oplus x_{15}\\
y_5&=x_1\oplus x_3\oplus x_4\oplus x_9\oplus x_{10}\oplus x_{14}\oplus x_{15}\\
y_6&=x_0\oplus x_2\oplus x_7\oplus x_9\oplus x_{10}\oplus x_{12}\oplus x_{13}\\
y_7&=x_1\oplus x_3\oplus x_6\oplus x_8\oplus x_{11}\oplus x_{12}\oplus x_{13}\\
y_8&=x_0\oplus x_1\oplus x_4\oplus x_7\oplus x_{10}\oplus x_{13}\oplus x_{15}\\
y_9&=x_0\oplus x_1\oplus x_5\oplus x_6\oplus x_{11}\oplus x_{12}\oplus x_{14}\\
y_{10}&=x_2\oplus x_3\oplus x_5\oplus x_6\oplus x_8\oplus x_{13}\oplus x_{15}\\
y_{11}&=x_2\oplus x_3\oplus x_4\oplus x_7\oplus x_9\oplus x_{12}\oplus x_{14}\\
y_{12}&=x_1\oplus x_2\oplus x_6\oplus x_7\oplus x_9\oplus x_{11}\oplus x_{12}\\
y_{13}&=x_0\oplus x_3\oplus x_6\oplus x_7\oplus x_8\oplus x_{10}\oplus x_{13}\\
y_{14}&=x_0\oplus x_3\oplus x_4\oplus x_5\oplus x_9\oplus x_{11}\oplus x_{14}\\
y_{15}&=x_1\oplus x_2\oplus x_4\oplus x_5\oplus x_8\oplus x_{10}\oplus x_{15}
\end{aligned}$$

4　ARIA 算法的差分性质

本节首先介绍符号的记法，然后详细描述 ARIA 算法的 4 轮性质。

4.1 定义及符号记法

定义 1　集合 $\{a_i \mid a_i\in F_{2^n},0\le i\le 2^n-1\}$ 是活动的，如果对任意 $0\le i<j\le 2^n-1$，都有 $a_i\ne a_j$。

定义 2　集合 $\{a_i \mid a_i\in F_{2^n},0\le i\le 2^n-1\}$ 是非活动的，若对任意 $0\le i<j\le 2^n-1$，都有 $a_i=a_j$。

定义 3　明文集合 $\mathcal{P}=\{P^0,P^1,\cdots,P^{255}\}$，其中 $P^i(0\le i\le 255)$ 在第一个字节是活动的，其他字节是非活动的。

加密明文 $P^i(0\le i\le 255)$，设第 j 轮输入记为 X_j^i，字节记为 $X_{j,k}^i(0\le k\le 15)$；混乱层和扩散层的输入分别是 Y_j^i,Z_j^i，字节记为 $Y_{j,k}^i(0\le k\le 15)$ 和 $Z_{j,k}^i(0\le k\le 15)$。轮密钥为 k_j，字节记为 $k_{j,k}(0\le k\le 15)$；轮密钥加和扩散层可以交换顺序，记交换后的密钥为 k_j^*，字节记为 $k_{j,k}^*(0\le k\le 15)$。第 j 轮变换的字节记法如图 1 所示。

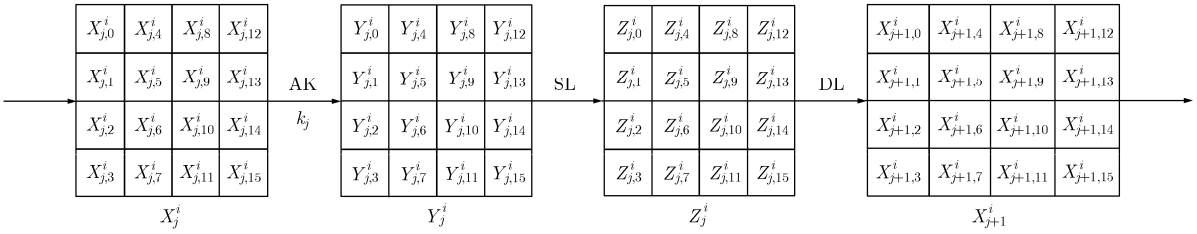

图 1 明文 P^i 的第 j 轮变换

4.2 ARIA 算法的 4 轮差分性质

性质 对定义 3 中的明文集合 $\mathcal{P}$ 加密 4 轮 ARIA 算法，差分集合 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$ 完全由以下 30 个字节确定：Y_2^0 的 7 个字节 $Y_{2,3}^0, Y_{2,4}^0, Y_{2,6}^0, Y_{2,8}^0, Y_{2,9}^0, Y_{2,13}^0, Y_{2,14}^0$，$Y_3^0$ 的 16 个字节和轮密钥 k_4 的 7 个字节 $k_{4,3}, k_{4,4}, k_{4,6}, k_{4,8}, k_{4,9}, k_{4,13}, k_{4,14}$。即差分集合 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$ 有 2^{240} 种取值(加密 4 轮后的其他字节也有类似的结论，即 $\{X_{5,k}^0 \oplus X_{5,k}^0, X_{5,k}^1 \oplus X_{5,k}^0, \cdots, X_{5,k}^{255} \oplus X_{5,k}^0\}$ $(1 \le k \le 15)$ 也是由 30 个字节确定)。当选取适当的 P^0，使得 $Y_{2,3}^0 = 0$，这样的差分集合 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$ 有 2^{232} 种取值。

证明 明文集合 $\mathcal{P} = \{P^0, P^1, \cdots, P^{255}\}$ 在第 0 字节互不相同，在其他字节全部相同，因此第 1 轮变换后，可以计算出差分集合 $\{Z_1^0 \oplus Z_1^0, Z_1^1 \oplus Z_1^0, \cdots, Z_1^{255} \oplus Z_1^0\}$，集合中元素在第 0 字节取遍所有值，在其他字节均为零。又因为扩散层和轮密钥加是线性操作，所以可以计算得到差分集合 $\{Y_2^0 \oplus Y_2^0, Y_2^1 \oplus Y_2^0, \cdots, Y_2^{255} \oplus Y_2^0\}$。由扩散层的运算可知这些差分除了第 3, 4, 6, 8, 9, 13 和 14 字节 $(Y_{2,j}^i \oplus Y_{2,j}^0 (0 \le i \le 255, j = 3,4,6,8,9,13,14))$ 以外都为零。

假设字节 $Y_{2,3}^0, Y_{2,4}^0, Y_{2,6}^0, Y_{2,8}^0, Y_{2,9}^0, Y_{2,13}^0, Y_{2,14}^0$ 作为参数，因此 $\{Y_2^1, Y_2^2, \cdots, Y_2^{255}\}$ 的第 3, 4, 6, 8, 9, 13 和 14 字节也可以得到，进一步可以计算出 $\{Z_2^0, Z_2^1, \cdots, Z_2^{255}\}$ 第 3, 4, 6, 8, 9, 13 和 14 字节，因此就得到差分集合 $\{Z_2^0 \oplus Z_2^0, Z_2^1 \oplus Z_2^0, \cdots, Z_2^{255} \oplus Z_2^0\}$ 的第 3, 4, 6, 8, 9, 13 和 14 字节的值，而除了第 3, 4, 6, 8, 9, 13 和 14 字节以外，$Z_2^i \oplus Z_2^0 (0 \le i \le 255)$ 的其他字节全部为零，这就得到差分集合 $\{Z_2^0 \oplus Z_2^0, Z_2^1 \oplus Z_2^0, \cdots, Z_2^{255} \oplus Z_2^0\}$。又因为扩散层和轮密钥加是线性操作，所以可以计算出 $\{Y_3^0 \oplus Y_3^0, Y_3^1 \oplus Y_3^0, \cdots, Y_3^{255} \oplus Y_3^0\}$。

假设 Y_3^0 的 16 个字节为参数，就可以计算出集合 $\{Y_3^0, Y_3^1, \cdots, Y_3^{255}\}$ 的值，经过混乱层和扩散层的变换就可以得到第 4 轮的输入状态 $\{X_4^0, X_4^1, \cdots, X_4^{255}\}$。

假设轮密钥 k_4 的 7 个字节 $k_{4,3}, k_{4,4}, k_{4,6}, k_{4,8}, k_{4,9}, k_{4,13}, k_{4,14}$ 也作为参数，因此就可以计算得到 $\{Y_{4,3}^i, Y_{4,4}^i, Y_{4,6}^i, Y_{4,8}^i, Y_{4,9}^i, Y_{4,13}^i, Y_{4,14}^i\} (0 \le i \le 255)$，在经过第 4 轮的混乱层变换就可以计算出 $\{Z_{4,3}^i, Z_{4,4}^i, Z_{4,6}^i, Z_{4,8}^i, Z_{4,9}^i, Z_{4,13}^i, Z_{4,14}^i\} (0 \le i \le 255)$，也就得到了差分集合 $\{Z_{4,k}^0 \oplus Z_{4,k}^0, Z_{4,k}^1 \oplus Z_{4,k}^0, \cdots, Z_{4,k}^{255} \oplus Z_{4,k}^0\} (k = 3,4,6,8,9,13,14)$，再经过扩散层置换就可以计算出差分 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$。4 轮变换过程如图 2 所示。

由上述分析，可知差分集合 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$ 由 30 个字节决定，因此最多有 2^{240} 种取值。而每个明文集合根据 P^0 的选择都可以表示成 2^8 个差分集合，因此可以通过选择 P^0，使得 $Y_{2,3}^0 = 0$ 来减少参数个数，这样差分集合 $\{X_{5,0}^0 \oplus X_{5,0}^0, X_{5,0}^1 \oplus X_{5,0}^0, \cdots, X_{5,0}^{255} \oplus X_{5,0}^0\}$ 由 29 个字节决定，共有 2^{232} 个差分取值。

5 对 7 轮和 8 轮 ARIA-256 的攻击

本节中，将利用第 4 节得到的 ARIA 算法的差分性质，对 ARIA 算法进行差分枚举攻击。对 7 轮 ARIA-256 算法的攻击，根据 4 轮差分性质构造的筛选集合对应第 2–5 轮，再选择明文集合 P 使得加密一轮后得到 4 轮差分性质中的明文集合 $\mathcal{P}$，然后解密对应的密文集合，计算出第 6 轮的输入差分，也即第 5 轮的输出差分，最后与筛选集合相比较，确定出正确密钥。攻击算法进一步扩展，在最后增加一轮，实现对 8 轮 ARIA-256 算法的分析。

对 7 轮 ARIA 算法的攻击算法如下：

(1)预计算，计算由 ARIA 算法的性质所确定的明文集合加密 4 轮后所对应的 2^{232} 个可能的差分筛选集合。

(2)猜测密钥 $k_{1,3}, k_{1,4}, k_{1,6}, k_{1,8}, k_{1,9}, k_{1,13}, k_{1,14}$，选择明文集合 P (包含 256 个明文)，这些明文除了第 3, 4, 6, 8, 9, 13 和 14 字节以外的其他字节均相同，且加密一轮后只有第 0 个字节是活动的，而其他字节是非活动的。

(3)解密部分要交换第 6 轮的扩散层和第 7 轮的轮密钥加的顺序，这样只猜测密钥 $k_{8,3}, k_{8,4}, k_{8,6},$

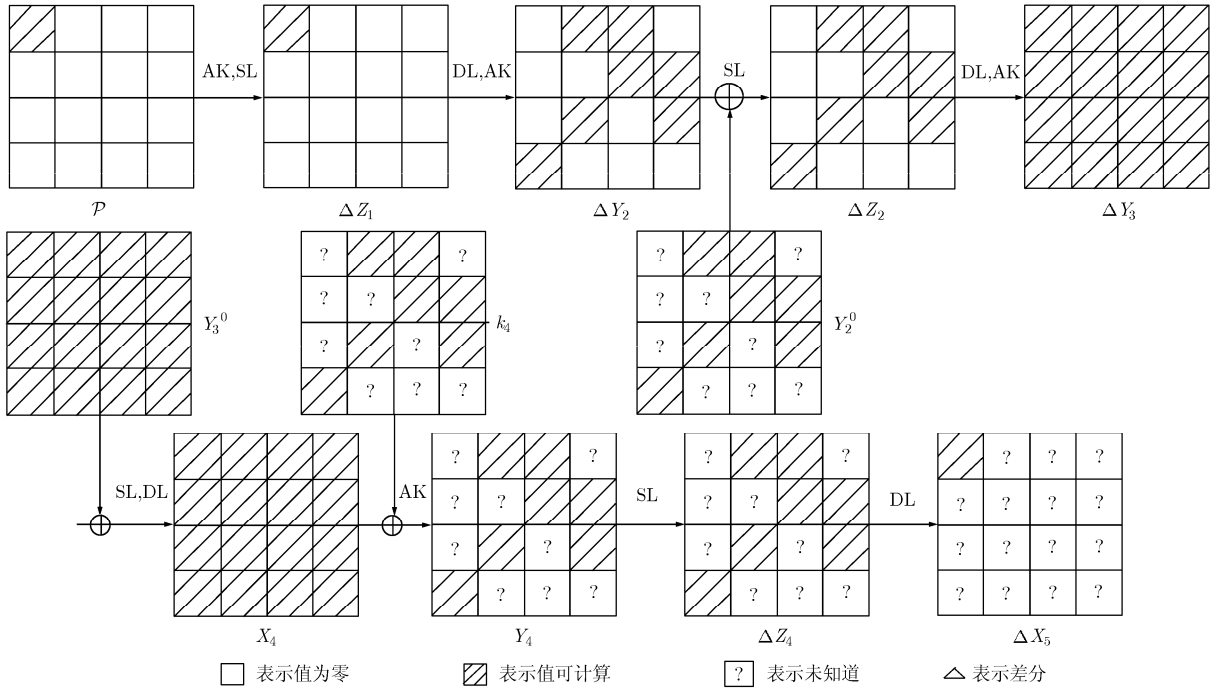

图 2 ARIA 算法 4 轮性质

$k_{8,8}, k_{8,9}, k_{8,13}, k_{8,14}$ 和 $k_{7,0}^*$，根据集合 P 中的明文所对应的密文计算 $Y_{6,0}^i$，由于轮密钥加不改变差分值，就可以求出差分集合 $\{X_{6,0}^0 \oplus X_{6,0}^0, X_{6,0}^1 \oplus X_{6,0}^0, \cdots, X_{6,0}^{255} \oplus X_{6,0}^0\}$。

(4)比较得到的差分集合和预计算中的所有差分集合，如果与预计算集合完全不一致，那么密钥是错误的。否则密钥是正确对，这是因为一个错误的密钥计算的差分集合与预计算中的差分集合相一致的概率是 $2^{232} \cdot 2^{-8\times 256} = 2^{-1816}$。

攻击的复杂度分析：由于密钥值的不同，在第 2 步需要从 2^{56} 个明文中选择明文，因此攻击时的数据复杂度是 2^{56} 个选择明文。预计算阶段需要计算 $2^{232} \times 2^8 = 2^{240}$ 个差分值。每个差分值计算相当于 2 轮加密，因此预计算的复杂度是 $(2^{240} \times 2)/7 \approx 2^{238.2}$ 次加密 7 轮 ARIA 算法。密钥猜测时需要猜测 15 个子密钥，部分解密相当于 1/2 加密，因此时间复杂度是 $256 \times 2^{8\times 15}/(2\times 7) \approx 2^{124.2}$ 次加密 7 轮 ARIA 算法。

对 8 轮 ARIA-256 的攻击，再猜测最后一轮的所有密钥，其他步骤与 7 轮的攻击相同。数据复杂度是 2^{56}。预计算阶段需要计算 $2^{232} \times 2^8 = 2^{240}$ 个差分值。每个差分计算相当于 2 轮加密，因此预计算的复杂度是 $2^{240}/4 = 2^{238}$ 次加密 8 轮 ARIA 算法。密钥猜测时需要猜测 31 个子密钥，部分解密相当于 3/2 加密，因此时间复杂度是 $256 \times 2^{8\times 31} \times 3/(2\times 8) \approx 2^{253.6}$ 加密 8 轮 ARIA 算法。与相同轮数的中间相遇攻击的攻击复杂度比较如表 1。

表 1 攻击复杂度比较

轮数	预计算复杂度	数据复杂度	计算复杂度	攻击方法	文献
7	$2^{238.2}$	2^{56}	$2^{124.2}$	差分枚举	本文方法
8	2^{238}	2^{56}	$2^{253.6}$	差分枚举	本文方法
8	2^{252}	2^{56}	$2^{251.6}$	中间相遇	文献[6]

6　总结

本文基于中间相遇攻击的理论，进一步深化给出了对 ARIA 算法差分枚举攻击的基本思想，接着描述 ARIA 算法并以差分枚举理论分析了 ARIA 算法的差分性质，然后在此基础上攻击了 7 轮和 8 轮 ARIA 算法，相比相同轮数 ARIA 算法的中间相遇攻击有一定的优势。

参 考 文 献

[1] Kwon D, Kim J, and Park S, *et al*.. New block cipher: ARIA[C]. ICISC 2003, LNCS 2971: 432–445.

[2] Biryukov A, Canniere D C, and Lano J, *et al*.. Security and performance analysis of ARIA. Version 1.2. Dept. Electrical Engineering-ESAT/SCD-COSIC Katholieke Universiteit Leuven Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium, Jan. 7, 2004.

[3] Wu Wen-ling, Zhang Wen-tao, and Feng Deng-guo. Impossible differential cryptanalysis of Reduced-Round ARIA and Camellia[J]. *Journal of Computer Science and*

Technology, 2007, 22(3): 449–456.

[4] Fleischmann E, Gorski M, and Lucks S. Attacking reduced rounds of the ARIA block cipher. Cryptology ePrint Archive: Report 2009/334, http://eprint.iacr.org/2009/334. 2009.

[5] Fleischmann E, Forler C, and Gorski M, *et al.*. New boomerang attacks on ARIA[C]. INDOCRYPT 2010, LNCS 6498: 163–175.

[6] Li Yan-jun, Wu Wen-ling, and Zhang Lei. Integral attacks on reduced-round ARIA block cipher[C]. ISPEC 2010, LNCS 6047: 19–29.

[7] Tang Xue-hai, Sun Bing, and Li Rui-lin, *et al.*. A meet-in-the-middle attack on ARIA. Cryptology ePrint Archive: Report 2010/168, http://eprint.iacr.org/2010/168. 2010.

[8] Demirci H, Selcuk A A, and Ture E. A new meet-in-the-middle attack on the IDEA Block Cipher[C]. SAC 2003, LNCS 3006: 117–129.

[9] Demirci H and Selcuk A A. A meet-in-the-middle attack on 8-round AES[C]. FSE 2008, LNCS 5086: 116–126.

[10] Dunkelman O, Keller N, and Shamir A. Improved single-key attacks on 8-round AES. Cryptology ePrint Archive: Report 2010/322, http://eprint.iacr.org/2010/322. 2010.

陈少真： 女，1967 年生，博士，教授，研究方向为信息安全.

鲁林真： 男，1985 年生，硕士生，研究方向为信息安全.