对完整轮数 ARIRANG 加密模式的新的相关密钥矩形攻击

刘 青[1] 卫宏儒[1,2]
(北京科技大学数理学院 北京 100083)[1] (信息安全国家重点实验室 北京 100191)[2]

摘 要 针对 ARIRANG 加密模式,利用相关密钥矩形攻击的方法对其安全性进行了重新评估。首先找到了一些新的 38 轮和 39 轮的高概率相关密钥矩形区分器,然后在此基础上将区分器进行改进,改进的主要思想是:利用模减差分和异或差分的混合表示方式代替原先的异或差分,同时在区分器的输出中选择一个差分集合代替原先单一的差分。基于以上各种新的高概率区分器,对全轮 ARIRANG 加密模式进行了攻击,其结果优于以往的攻击结果。其中最好的攻击结果为:攻击全轮的 ARIRANG-256 加密模式所需的数据复杂度和时间复杂度分别为 $2^{220.79}$ 和 $2^{155.60}$。

关键词 ARIRANG 加密模式,相关密钥矩形攻击,区分器,模减差分,差分集合
中图法分类号 TN918.1 **文献标识码** A

New Related-key Rectangle Attack on Full ARIRANG Encryption Mode

LIU Qing[1] WEI Hong-ru[1,2]
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)[1]
(State Key Laboratory of Information Security, Beijing 100191, China)[2]

Abstract The security of ARIRANG encryption mode was revaluated with the method of related-key rectangle attack. First, some new high-probability related-key rectangle distinguishers of 38 rounds and 39 rounds were found. Based on these distinguishers, some improvements in them were made. The main idea is the use of modular subtraction and XOR differential instead of the only XOR differential. Also, outputs of the distinguishers chose a differential set instead of the only XOR differential. All kinds of results based on these new high-probability distinguishers are presented, and they are better than the previous results. The best result is the attack on full ARIRANG-256 encryption mode with the data complexity and time complexity of $2^{220.79}$ and $2^{155.60}$, respectively.

Keywords ARIRANG encryption mode, Related-key rectangle attack, Distinguisher, Modular subtraction differential, Differential set

1 引言

相关密钥攻击是由 Biham 和 Knudsen 等在研究 LOKI 算法时分别独立提出的,该方法更多地考虑了密钥扩展算法的性质,通过研究不同密钥之间的关系对加密的影响来得到密钥信息,它也可以与差分攻击相结合,进行相关密钥差分攻击。后来,人们又在相关密钥攻击的基础上,通过寻找两个较短的差分特征,将其连接构成一个新的高概率区分器,这种方法被称为相关密钥矩形攻击。目前,利用此攻击方法分别对 SHACAL-1[1]、SHACAL-2[2,3]、HAS-160 加密模式[4]、AES-192 和 AES-256[5] 等算法进行了安全性分析,并得到了较为理想的攻击结果。

在 2008 年,Donghoon Chang 等提出了 SHA-3 计划候选算法中的一个算法——散列函数 ARIRANG[6],该散列函数中包含了一个分组密码组件。根据其输出长度的不同,ARIRANG 分为 4 种不同的类型:ARIRANG-224、ARIRANG256、ARIRANG-384和 ARIRANG-512,其分组密码组件都采用了 40 轮的非平衡 Feistel 结构。算法提出后,密码界对其安全性进行了评估,文献[7-9]主要针对不同轮数的 ARIRANG-256 加密模式进行了原像攻击。文献[10]中给出一个概率为 2^{-480} 的 38 轮相关密钥矩形区分器,利用此区分器对完整轮数的 ARIRANG-256 加密模式进行了攻击,得到了第一个对其完整轮数加密模式的分析结果。

针对 ARIRANG 加密模式,本文首先找到了一些新的 38 轮高概率相关密钥矩形区分器;其次对区分器的轮数进行延长,首次给出了 39 轮的相关密钥矩形区分器;然后在此基础上对区分器进行改进,得到概率更高的区分器。利用以上各种改进前后的区分器对全轮加密模式进行了攻击,并给出攻击结果。表 1 列出了对 ARIRANG-256 加密模式现有的攻击结果以及本文的结果。

到稿日期:2012-10-15 返修日期:2013-01-26 本文受信息安全国家重点实验室 2011 年开放课题(02-04-3),内蒙古自治区科技创新引导奖励资金(2012)资助。

刘 青(1989—),女,硕士生,主要研究方向为密码学,E-mail:44238392@qq.com;卫宏儒(1963—),男,硕士,副教授,主要研究方向为数学、信息安全与密码学以及物联网关键技术。

表 1　ARIRANG-256 加密模式的现有攻击结果

攻击方法	轮数	数据复杂度	时间复杂度	文献
原像攻击	33	—	2^{241}	[7]
	35	—	$2^{240.94}$	[8]
	40	—	2^{254}	[9]
相关密钥矩形攻击	40	2^{244}	2^{244}	[10]
	40	$2^{227.13}$	$2^{157.94}$	本文
	40	$2^{251.13}$	$2^{141.94}$	本文
	40	$2^{224.79}$	$2^{163.60}$	本文
	40	$2^{220.79}$	$2^{155.60}$	本文
	40	$2^{244.79}$	$2^{139.60}$	本文

2　算法简介

ARIRANG-256(ARIRANG-512)加密模式采用了 40 轮的非平衡 Feistel 结构，其明文分组长度为 256(512)bit，密钥长度为 512(1024)bit。然而 ARIRANG- 224 是 ARIRANG-256 输出的一个 32bit 的截断，ARIRANG-384 是 ARIRANG-512 输出的一个 128bit 的截断。这里以 ARIRANG-256 为例具体给出此加密模式的结构，如图 1 所示。

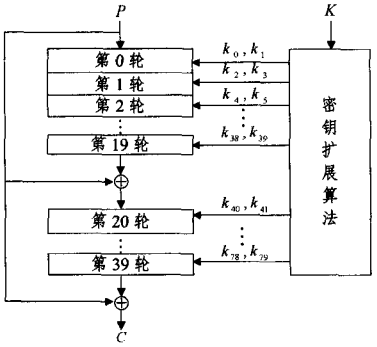

图 1　ARIRANG-256 的加密结构

ARIRANG-256 加密模式的明文输入 $P=(A_0,B_0,C_0,D_0,E_0,F_0,G_0,H_0)\in(F_2^{32})^8$，即为第 0 轮的输入。现假设第 i 轮的输入为 $(A_i,B_i,C_i,D_i,E_i,F_i,G_i,H_i)$，则第 i 轮的输出为 $(A_{i+1},B_{i+1},C_{i+1},D_{i+1},E_{i+1},F_{i+1},G_{i+1},H_{i+1})$，其中 $i=0,1,2,3,\cdots,39$，具体的轮函数结构如图 2 所示，也可以表示为：

$$L_1=g^{(256)}(A_i\oplus k_{2i}),L_2=g^{(256)}(E_i\oplus k_{2i+1}),$$

$$B_{i+1}=A_i\oplus k_{2i},C_{i+1}=B_i\oplus L_1,D_{i+1}=C_i\oplus(L_1^{<<<s_1}),$$

$$E_{i+1}=D_i\oplus(L_1^{<<<s_2}),F_{i+1}=E_i\oplus k_{2i+1},G_{i+1}=F_i\oplus L_2,$$

$$H_{i+1}=G_i\oplus(L_2^{<<<s_3}),A_{i+1}=H_i\oplus(L_2^{<<<s_4})$$

其中，k_{2i},k_{2i+1} 表示第 i 轮加密的轮密钥；$L^{<<<s_i}$ $(i=1,2,3,4)$ 表示将 L 循环左移 s_i 比特。在 ARIRANG-256 中，$(s_1,s_2,s_3,s_4)=(13,23,29,7)$，非线性函数 $g^{(256)}$ 是由 AES 的 S 盒和 $MDS_{4\times4}$ 矩阵构成的，这里不再详述。而此加密模式的密钥由初始密钥和扩展密钥两部分组成，具体见文献[6]。

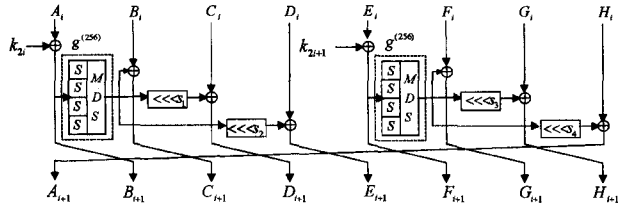

图 2　ARIRANG-256 的第 i 轮的轮函数

3　相关密钥矩形攻击的基本思想

相关密钥矩形攻击的实质是采用两个较短的差分特征代替单个差分特征来提高差分路线的概率，具体方法如下：

设 E 为一个分组密码算法，且 $E=E^1\circ E^0$，即明文 P 在密钥 K 作用下的加密可以表示为 $E_K(P)=E_K^1\circ E_K^0(P)$。假设算法 E^0 存在一个概率为 p 的相关密钥差分 $\alpha\to\beta$；算法 E^1 存在一个概率为 q 的相关密钥差分 $\gamma\to\delta$，即

$$\Pr[E_{K^a}^0\oplus E_{K^b}^0(P^b)=\beta\mid P^a\oplus P^b=\alpha]=p$$

$$\Pr[E_{K^c}^0\oplus E_{K^d}^0(P^d)=\beta\mid P^c\oplus P^d=\alpha]=p$$

$$\Pr[E_{K^a}^1\oplus E_{K^c}^1(X^c)=\delta\mid X^a\oplus X^c=\gamma]=q$$

$$\Pr[E_{K^b}^1\oplus E_{K^d}^1(X^d)=\delta\mid X^b\oplus X^d=\gamma]=q$$

其中，(K^a,K^b,K^c,K^d) 为相关密钥四元组，(X^a,X^b,X^c,X^d) 为明文四元组 (P^a,P^b,P^c,P^d) 在相关密钥四元组 (K^a,K^b,K^c,K^d) 下经算法 E^0 作用后的输出结果。而 ΔK 和 $\Delta K'$ 为密钥差分，且满足：

$$K^a\oplus K^b=K^c\oplus K^d=\Delta K$$

$$K^a\oplus K^c=K^b\oplus K^d=\Delta K'$$

相关密钥矩形区分器的具体构造：首先随机选取 $n\in\mathbf{N}$（$\mathbf{N}$ 为自然数集）个不同的明文对 $(P^a,P^b=P^a\oplus\alpha)$，分别计算其在密钥 K^a 和 K^b 作用下的加密结果 $C^a=E_{K^a}(P^a)$ 和 $C^b=E_{K^b}(P^b)$，将这些明密文对记为集合 I_0；再随机选取 n 个不同的明文对 $(P^c,P^d=P^c\oplus\alpha)$，分别计算其在密钥 K^c 和 K^d 作用下的加密结果 $C^c=E_{K^c}(P^c)$ 和 $C^d=E_{K^d}(P^d)$，将这些明密文对记为集合 I_1；然后分别选取集合 I_0 和 I_1 中明文对 $(P^a,P^b)\in I_0$ 和 $(P^c,P^d)\in I_1$，检验相应密文是否满足 $C^a\oplus C^c=C^b\oplus C^d=\delta$。该密文四元组 (C^a,C^b,C^c,C^d) 满足差分 δ 的概率约为：

$$\sum_{\beta,\gamma}p^2q^2=2^{-n}(\hat{p}\hat{q})^2$$

其中，

$$\hat{p}=\sqrt{\sum_\beta p^2}=\sqrt{\sum_\beta\Pr^2(\alpha\to\beta)}$$

$$\hat{q}=\sqrt{\sum_\gamma q^2}=\sqrt{\sum_\gamma\Pr^2(\gamma\to\delta)}$$

为计算 $\hat{p},\hat{q}$，需要计算对于算法 E^0 的输入差分为 α 的所有差分特征的概率，以及对于算法 E^1 的输出差分为 δ 的所有差分特征的概率。为使得计算具有可行性，通常令算法 E^0 的差分特征的前若干轮相同，算法 E^1 的差分特征的后若干轮相同，这样得到较为精确的 $\hat{p}$ 和 $\hat{q}$。

对于一个随机置换，满足 δ 测试的概率为 2^{-2n}。因此，如果满足 $(\hat{p}\hat{q})^2>2^{-n}$，则相关密钥矩形区分器便可将算法 E 和随机置换区分开。

4　对完整轮数 ARIRANG 加密模式的相关密钥矩形攻击

本文以 ARIRANG-256 为例，给出新的相关密钥矩形区分器及其攻击过程。

4.1　非线性函数 $g^{(256)}$ 的差分传播特性

ARIRANG-256 加密模式中的非线性函数 $g^{(256)}$ 采用了 AES 的 S 盒和 $MDS_{4\times4}$ 矩阵。为得到 $g^{(256)}$ 的一个高概率差分特征，通过 C 语言编程得到 AES 的 S 盒的 256×256 差分矩阵，发现矩阵的每一行、每一列（除第一行、第一列）均含有 1 个 4、126 个 2 和 129 个 0。那么对于一个 S 盒，必定存在概率为 2^{-6} 的差分特征，以下为其中之一，即当输入差分为全 1

差分时，输出差分为 $0x75$ 的概率为 2^{-6}：

$S(x)\oplus S(x\oplus 0xff)=0x75$

若 $MDS_{4\times4}$ 矩阵的输入为$(\lambda,\lambda,\lambda,\lambda)$，其输出仍为$(\lambda,\lambda,\lambda,\lambda)$。因此满足以下条件的 32bit 的字 x 有 2^8 个不同的取值（这里 $0x(75)_4$ 表示 $0x75757575$，下文记法类似）：

$g^{(256)}(x)\oplus g^{(256)}(x\oplus 0xffffffff)=0x(75)_4$

即全 1 差分经过 $g^{(256)}$ 函数后差分为 $0x(75)_4$ 的概率是 2^{-24}。

同样地，也可以得到 $g^{(256)}$ 的如下差分特征：差分 $0x(ba)_4$ 经过 $g^{(256)}$ 函数后差分为 $0x(97)_4$ 的概率也为 2^{-24}。

4.2 新的 38 轮的高概率相关密钥矩形区分器

为更好地对 ARIRANG 进行攻击，本文仍采用文献[8]在密钥扩展算法中引入的线性变换，同时利用文献[10]中的结果：由上述线性变换得到的等价初始密钥，以及由等价初始密钥扩展的轮密钥表。本文的攻击中所恢复的密钥均为等价密钥。

为利用 4.1 节得到的非线性函数 $g^{(256)}$ 两个概率为 2^{-24} 的差分特征，在区分器及密钥差分中采用全 1 差分 $e=0xffffffff$ 进行分析，且相关密钥四元组(K^a,K^b,K^c,K^d)满足如下关系（(K^a,K^b,K^c,K^d)均为等价初始密钥）：

$$\Delta K=K^a\oplus K^b=K^c\oplus K^d$$
$$=(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,e)$$
$$\Delta K'=K^a\oplus K^c=K^b\oplus K^d$$
$$=(0,0,0,0,0,0,0,0,0,0,0,0,0,0,e,0)$$

根据等价初始密钥扩展的轮密钥表以及密钥差分 ΔK，得到区分器的第一部分 E^0 为第 0 轮到第 18 轮，即概率为 $p=2^{-48}$ 的差分特征 $\alpha\to\beta$（见表 2）：

$$(0,0,0,0,0,e,0,e)\xrightarrow{19r}(0x(ae)_4,0x(ba)_4$$
$$0x(97)_4,0x(f2)_4,0x(cb)_4,0,e,0x(75)_4)$$

同样，根据等价初始密钥扩展的轮密钥表以及密钥差分 $\Delta K'$，得到区分器的第二部分 E^1 为第 19 轮到第 37 轮，即概率为 $q=2^{-48}$ 的差分特征 $\gamma\to\delta$（见表 3）：

$$(0,0,0,0,0,0x(75)_4,0x(51)_4,0x(ba)_4)\xrightarrow{19r}$$
$$(0x(ba)_4,0,0,0,0,e,0x(75)_4,0x(ae)_4)$$

表 2 E^0 的差分特征

轮数(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	$\Delta k_i(L,R)$	概率
−1	0	0	0	0	0	e	0	e	—	—
0	e	0	0	0	0	0	e	0	(0,0)	1
1	0	0	0	0	0	0	0	e	(e,0)	1
2	e	0	0	0	0	0	0	0	(0,0)	1
3	0	0	0	0	0	0	0	0	(e,0)	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
16	0	0	0	0	0	0	0	0	(0,0)	1
17	$0x(ba)_4$	0	0	0	0	e	$0x(75)_4$	$0x(ae)_4$	(0,e)	2^{-24}
18	$0x(ae)_4$	$0x(ba)_4$	$0x(97)_4$	$0x(f2)_4$	$0x(cb)_4$	0	e	$0x(75)_4$	(0,0)	2^{-24}

表 3 E^1 的差分特征

轮数(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	$\Delta k_i(L,R)$	概率
18	0	0	0	0	0	$0x(75)_4$	$0x(51)_4$	$0x(ba)_4$	—	—
19	0	0	0	0	0	e	0	e	(0,e)	2^{-24}
20	e	0	0	0	0	0	e	0	(0,0)	1
21	0	0	0	0	0	0	0	e	(e,0)	1
22	e	0	0	0	0	0	0	0	(0,0)	1
23	0	0	0	0	0	0	0	0	(e,0)	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
36	0	0	0	0	0	0	0	0	(0,0)	1
37	$0x(ba)_4$	0	0	0	0	e	$0x(75)_4$	$0x(ae)_4$	(0,e)	2^{-24}

注：表 2 中的第−1 轮所在行表示第 0 轮的输入差分，表 3 中的第 18 轮所在行表示第 19 轮的输入差分，第 i 轮所在行表示第 i 轮输出差分，$\Delta k_i(L,R)$表示第 i 轮左右两侧的轮密钥差分。

现计算 $\hat{p}$，取 E^0 差分特征的第 0 至 17 轮相同，只需计算第 18 轮所有可能的差分传播路径的概率。根据 256×256 差分矩阵的第 187 行，可得输入差分 $0x(ba)_4$ 经过非线性 $g^{(256)}$ 函数后的所有可能输出差分的概率，那么

$$\hat{p}=(\sum_{\beta}p^2)^{1/2}=(2^{-48\cdot2}+126\cdot2^{-52\cdot2})^{1/2}\approx2^{-47.71}$$

此外，通过观察表 2，发现 E^0 的第 0 至 16 轮都是以概率 1 成立的。若计算出第 17、18 轮的所有可能差分传播路径的概率，可得更准确的 $\hat{p}$：

$$\hat{p}=(\sum_{\beta}p^2)^{1/2}=(2^{-48\cdot2}+126\cdot2^{-52\cdot2}+126\cdot(2^{-52\cdot2}+126\cdot2^{-56\cdot2}))^{1/2}$$
$$\approx2^{-47.42}$$

同样地，为计算 $\hat{q}$，取 E^1 的第 20 至 37 轮相同，只需考虑第 19 轮的所有可能输入差分，类似可得到

$$\hat{q}=(\sum_{\gamma}q^2)^{1/2}=(2^{-48\cdot2}+126\cdot2^{-52\cdot2})^{1/2}\approx2^{-47.71}$$

综上，该相关密钥矩形区分器的概率约为 $2^{-n}\cdot(\hat{p}\hat{q})^2\approx2^{-446.26}$，此时有$(\hat{p}\hat{q})^2>2^{-n}$，即以上区分器就能将算法 E 和随机置换区分开。

4.3 39 轮的相关密钥矩形区分器

基于 4.2 节中的 38 轮区分器，考虑将其轮数延长，通过类似的分析得到一个 39 轮的相关密钥矩形区分器：区分器的第一部分 E^0 仍为第 0 轮到第 18 轮，与 4.2 节中的相同；而区分器的第二部分 E^1 为第 19 轮到第 38 轮，即概率为 $q=2^{-72}$ 的差分特征 $\gamma\to\delta'$：$(0,0,0,0,0,0x(75)_4,0x(51)_4,0x(ba)_4)\xrightarrow{20r}(0x(ae)_4,0x(ba)_4,0x(97)_4,0x(f2)_4,0x(cb)_4,0,e,0x(75)_4)$。

利用 4.2 节中的方法计算出以上 39 轮区分器的概率约

为 $2^{-494.26}$，具体过程不再赘述。

4.4 对完整轮数 ARIRANG-256 加密模式的相关密钥矩形攻击

利用 4.2 节及 4.3 节的区分器，对完整轮数 ARIRANG-256 加密模式进行攻击，以下为恢复第 38 和 39 轮部分轮密钥的具体过程。

1)随机选取 $2^{225.13}$ 个明文结构，即 $P_j^a=(A_{0,j}^a, B_{0,j}^a, C_{0,j}^a, D_{0,j}^a, E_{0,j}^a, F_{0,j}^a, G_{0,j}^a, H_{0,j}^a)$，$j=0,1,\cdots,2^{225.13}-1$。取 $P_j^b=P_j^a\oplus\alpha$，分别计算其在相关密钥 $K^a, K^b(K^b=K^a\oplus\Delta K)$ 作用下的加密结果，记为 C_j^a, C_j^b，将其明密文对构成的集合记为 I_0。

2)随机选取 $2^{225.13}$ 个明文结构，此时令 $P_j^c=P_j^a, P_j^d=P_j^b$(由于 ARIRANG-256 加密模式的第 19 轮后异或运算的作用)，分别计算其在相关密钥 $K^c, K^d(K^d=K^c\oplus\Delta K)$ 作用下的加密结果，记为 C_j^c, C_j^d，将其明密文对构成的集合记为 I_1。以上 $C_j^\Lambda=(A_{40,j}^\Lambda, B_{40,j}^\Lambda, C_{40,j}^\Lambda, D_{40,j}^\Lambda, E_{40,j}^\Lambda, F_{40,j}^\Lambda, G_{40,j}^\Lambda, H_{40,j}^\Lambda)$ $(\Lambda\in\{a,b,c,d\}; j=0,1,\cdots,2^{225.13}-1)$。

综上，攻击需要 $2^{225.13}$ 个明文对 (P_j^a, P_j^b) 和 $2^{225.13}$ 个明文对 (P_j^c, P_j^d)，即共有四元组 $(2^{225.13})^2=2^{450.26}$ 个，并将以上四元组集合记为 I。因此该攻击的数据复杂度为 $2^{225.13}\cdot 2^2=2^{227.13}$。

3)根据 4.2 节区分器的输出差分以及第 38 轮和 39 轮的差分传播路径(见图 3)，可知密文四元组 $(C_\tau^a, C_\tau^b, C_\tau^c, C_\tau^d)$，$\tau\in\{0,1,2,\cdots,2^{450.26}-1\}$，$\{C_\tau^a, C_\tau^b\}\in I_0$，$\{C_\tau^c, C_\tau^d\}\in I_1$ 需要满足如下等式，对集合 I 中的所有密文四元组进行检验：

$$\Delta B_{40,j}^{a,c}=\Delta B_{40,j}^{b,d}=0x(ae)_4$$

$$\Delta A_{40,j}^{a,c}\oplus(\Delta G_{40,j}^{a,c})^{<<<7}=\Delta A_{40,j}^{b,d}\oplus(\Delta G_{40,j}^{b,d})^{<<<7}=0x(75)_4$$

$$\Delta H_{40,j}^{a,c}\oplus(\Delta G_{40,j}^{a,c})^{<<<29}=\Delta H_{40,j}^{b,d}\oplus(\Delta G_{40,j}^{b,d})^{<<<29}=e$$

$$(\Delta F_{40,j}^{a,c}\oplus e)^{>>>23}\oplus(\Delta C_{40,j}^{a,c}\oplus 0x(ba)_4)^{<<<13}=\Delta D_{40,j}^{a,c}$$

$$(\Delta F_{40,j}^{b,d}\oplus e)^{>>>23}\oplus(\Delta C_{40,j}^{b,d}\oplus 0x(ba)_4)^{<<<13}=\Delta D_{40,j}^{b,d}$$

$$(\Delta F_{40,j}^{a,c}\oplus e)^{>>>10}\oplus(\Delta C_{40,j}^{a,c}\oplus 0x(ba)_4)^{<<<23}=\Delta E_{40,j}^{a,c}$$

$$(\Delta F_{40,j}^{b,d}\oplus e)^{>>>10}\oplus(\Delta C_{40,j}^{b,d}\oplus 0x(ba)_4)^{<<<23}=\Delta E_{40,j}^{b,d}$$

其中，$\Delta Y_{40,j}^{x_1,x_2}=Y_{40,j}^{x_1}\oplus Y_{40,j}^{x_2}$，$Y\in\{A,B,C,D,E,F,G,H\}$，$x_1, x_2\in\{a,b,c,d\}$。然而对于任意的一个四元组，满足其中一个等式的概率为 2^{-32}，则满足条件的密文四元组个数为 $2^{450.26}\cdot(2^{-32\cdot 5})^2=2^{130.26}$，将满足条件的密文四元组记为集合 I_2。

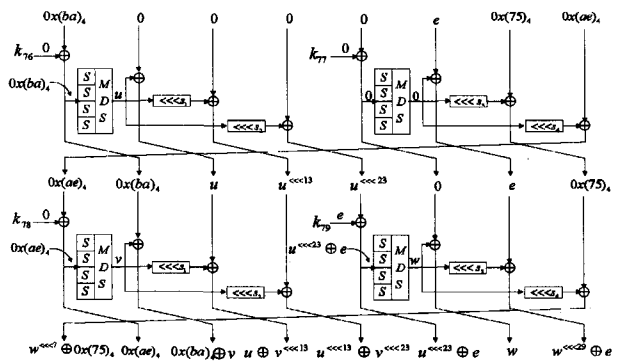

图 3 第 38 轮和 39 轮的差分传播路径

4)猜测第 39 轮的密钥 $k_t^\kappa(t=78,79)$，根据相关密钥组之间的差分关系计算出 $k_{78}^\kappa, k_{79}^\kappa(\kappa\in\{b,c,d\})$，相关密钥组之间的差分关系如下：

$$k_{78}^a\oplus k_{78}^\kappa=k_{78}^b\oplus k_{78}^d=0, k_{79}^a\oplus k_{79}^\kappa=k_{79}^b\oplus k_{79}^d=e$$

$$k_{78}^a\oplus k_{78}^b=k_{78}^c\oplus k_{78}^d=0, k_{79}^a\oplus k_{79}^b=k_{79}^c\oplus k_{79}^d=0$$

首先利用以上猜测密钥 $k_{78}^\Lambda(\Lambda\in\{a,b,c,d\})$ 对集合 I_2 中密文组进行部分解密，恢复出第 39 轮输入四元组中的一部分 $(A_{39,j}^\Lambda, B_{39,j}^\Lambda, C_{39,j}^\Lambda, D_{39,j}^\Lambda)$，$\Lambda\in\{a,b,c,d\}$，再对以上恢复出的所有四元组检验如下等式是否成立：

$$g^{(256)}(A_{39,j}^a\oplus k_{78}^a)\oplus g^{(256)}(A_{39,j}^c\oplus k_{78}^c)=\Delta B_{40,j}^{a,c}\oplus\Delta C_{40,j}^{a,c}\oplus 0x(14)_4$$

$$g^{(256)}(A_{39,j}^b\oplus k_{78}^b)\oplus g^{(256)}(A_{39,j}^d\oplus k_{78}^d)=\Delta B_{40,j}^{b,d}\oplus\Delta C_{40,j}^{b,d}\oplus 0x(14)_4$$

若成立，则对应的四元组和密钥为正确的候选值；否则进行淘汰，这样将满足条件的四元组记为集合 I_3。淘汰后剩余四元组的个数为 $2^{130.26}\cdot 2^{-32\cdot 2}=2^{66.26}$，此时对集合 I_2 中的密文组进行部分解密需要的时间复杂度为 $2^{130.26}\cdot 2^{32}\cdot 4/(2\cdot 40)\approx 2^{157.94}$。

其次利用猜测密钥 $k_{79}^\Lambda(\Lambda\in\{a,b,c,d\})$ 对集合 I_3 中的密文组进行部分解密，恢复出第 39 轮输入四元组的另一部分 $(E_{39,j}^\Lambda, F_{39,j}^\Lambda, G_{39,j}^\Lambda, H_{39,j}^\Lambda)$，$\Lambda\in\{a,b,c,d\}$，同样对以上恢复出的所有四元组检验如下等式是否成立：

$$g^{(256)}(E_{39,j}^a\oplus k_{79}^a)\oplus g^{(256)}(E_{39,j}^c\oplus k_{79}^c)=\Delta G_{40,j}^{a,c}$$

$$g^{(256)}(E_{39,j}^b\oplus k_{79}^b)\oplus g^{(256)}(E_{39,j}^d\oplus k_{79}^d)=\Delta G_{40,j}^{b,d}$$

同理，若成立，则对应的四元组和密钥为正确的候选值；否则进行淘汰，此时将满足条件的四元组记为集合 I_4。淘汰后剩余四元组的个数为 $2^{66.26}\cdot 2^{-32\cdot 2}=2^{2.26}$，此时对集合 I_3 中的密文组进行部分解密需要的时间复杂度为 $2^{32}\cdot 2^{66.26}\cdot 2^{32}\cdot 4/(2\cdot 40)\approx 2^{125.94}$。

5)再猜测第 38 轮左面的密钥 k_{76}^κ，根据相关密钥组之间的差分关系，计算出密钥组 $k_{76}^\kappa(\kappa\in\{b,c,d\})$：

$$k_{76}^a\oplus k_{76}^\kappa=k_{76}^b\oplus k_{76}^d=0$$

$$k_{76}^a\oplus k_{76}^b=k_{76}^c\oplus k_{76}^d=0$$

利用以上密钥组对集合 I_4 中的密文组进行解密，恢复出第 38 轮的输入四元组 $(A_{38,j}^\Lambda, B_{38,j}^\Lambda, C_{38,j}^\Lambda, D_{38,j}^\Lambda, E_{38,j}^\Lambda, F_{38,j}^\Lambda, G_{38,j}^\Lambda, H_{38,j}^\Lambda)$，$\Lambda\in\{a,b,c,d\}$，再对以上恢复出的所有四元组检验如下等式是否成立：

$$g^{(256)}(A_{38,j}^a\oplus k_{76}^a)\oplus g^{(256)}(A_{38,j}^c\oplus k_{76}^c)=(\Delta F_{40,j}^{a,c}\oplus e)^{>>>23}$$

$$g^{(256)}(A_{38,j}^b\oplus k_{76}^b)\oplus g^{(256)}(A_{38,j}^d\oplus k_{76}^d)=(\Delta F_{40,j}^{b,d}\oplus e)^{>>>23}$$

若成立，则对应四元组和密钥为正确的候选值。由于 $2^{450.26}\cdot 2^{-446.26}=2^4$，若 4)中所猜密钥是正确密钥，则剩余四元组理论上有 2^4 个，因此以上利用密钥四元组对集合 I_4 中的密文组解密需要的时间复杂度至多为 $(2^{32})^2\cdot 2^4\cdot 2^{32}\cdot 4/(2\cdot 40)\approx 2^{95.68}$。

6)重复步骤 4)和 5)，直到正确密钥唯一确定。

综上，整个攻击过程所需的数据复杂度为 $2^{225.13}\cdot 2^2=2^{227.13}$，而时间复杂度主要由第 4)步决定，约为 $2^{157.94}+2^{125.94}\approx 2^{157.94}$ 次 40 轮 ARIRANG-256 加密运算。

根据相关密钥矩形攻击中的概率统计模型，假设正确密钥被统计的次数用 W_i 来表示，则 $W_i\sim Poisson(\lambda=2^{450.26}\cdot 2^{-446.26}=2^4)$，那么正确密钥被统计超过 5 次的概率为 $\Pr(W_i\geqslant 5)\approx 0.9996$，即攻击成功的概率约为 99.96%。

类似地，利用 4.3 节的 39 轮区分器对完整轮数 ARIRANG-256 加密模式进行攻击，与上述 38 轮区分器的攻

击过程不同的是，只猜测最后一轮的密钥，根据第 39 轮的差分传播路径(见图 4)，可知密文四元组(C^a,C^b,C^c,C^d)需要满足的等式有所增多：

$\Delta B_{40,j}^{a,c}=\Delta B_{40,j}^{b,d}=0x(ae)_4$；$\Delta F_{40,j}^{a,c}=\Delta F_{40,j}^{b,d}=0x(34)_4$

$\Delta A_{40,j}^{a,c}\oplus(\Delta G_{40,j}^{a,c})^{<<<7}=\Delta A_{40,j}^{b,d}\oplus(\Delta G_{40,j}^{b,d})^{<<<7}=0x(75)_4$

$\Delta H_{40,j}^{a,c}\oplus(\Delta G_{40,j}^{a,c})^{<<<29}=\Delta H_{40,j}^{b,d}\oplus(\Delta G_{40,j}^{b,d})^{<<<29}=e$

$(\Delta D_{40,j}^{a,c}\oplus 0x(97)_4)^{<<<10}=\Delta E_{40,j}^{a,c}\oplus 0x(f2)_4$

$(\Delta D_{40,j}^{b,d}\oplus 0x(97)_4)^{<<<10}=\Delta E_{40,j}^{b,d}\oplus 0x(f2)_4$

$(\Delta C_{40,j}^{a,c}\oplus 0x(ba)_4)^{<<<13}=\Delta D_{40,j}^{a,c}\oplus 0x(97)_4$

$(\Delta C_{40,j}^{b,d}\oplus 0x(ba)_4)^{<<<13}=\Delta D_{40,j}^{b,d}\oplus 0x(97)_4$

通过计算，攻击全轮 ARIRANG-256 所需的数据复杂度和时间复杂度分别为 $2^{251.13}$ 和 $2^{141.94}$。

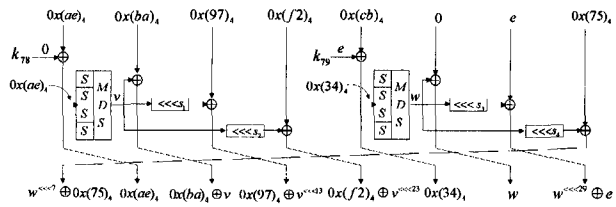

图 4　第 39 轮的差分传播路径

5　更多高概率相关密钥矩形区分器的构造

若区分器第一部分 E^0 的差分特征的输入差分中仅有差分 σ，同时满足：非零差分 σ 经过 $g^{(256)}$ 函数作用后的输出差分为 ω 的概率是 2^{-24}，以及非零差分 $\omega^{<<<s_4}$ 经过 $g^{(256)}$ 函数作用后的输出差分为 ϵ 的概率也是 2^{-24}，其中 $\sigma,\omega,\epsilon\in F_2^{32}$，且相关密钥四元组($K^a$,$K^b$,$K^c$,$K^d$)满足如下关系：

$\Delta K=K^a\oplus K^b=K^c\oplus K^d=(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\sigma)$

$\Delta K'=K^a\oplus K^c=K^b\oplus K^d=(0,0,0,0,0,0,0,0,0,0,0,0,0,0,\sigma,0)$

则由等价初始密钥扩展的轮密钥表以及密钥差分 ΔK，得到区分器的第一部分 E^0 为第 0 轮到第 18 轮，即概率为 $p=2^{-48}$ 的差分特征 $\alpha\to\beta$(见表 4)：

$$(0,0,0,0,0,\sigma,0,\sigma)\xrightarrow{19r}(\omega^{<<<s_3},\omega^{<<<s_4},\epsilon,\epsilon^{<<<s_1},\epsilon^{<<<s_2},0,\sigma,\omega)$$

同样，由等价初始密钥扩展的轮密钥表以及密钥差分 $\Delta K'$，得到区分器的第二部分 E^1 为第 19 轮到第 38 轮，即概率为 $q=2^{-72}$ 的差分特征 $\gamma\to\delta'$(见表 5)：

$$(0,0,0,0,0,\omega,\sigma\oplus(\omega^{<<<s_3}),\omega^{<<<s_4})\xrightarrow{20r}(\omega^{<<<s_3},\omega^{<<<s_4},\epsilon,\epsilon^{<<<s_1},\epsilon^{<<<s_2},0,\sigma,\omega)$$

通过计算可知，上述 39 轮区分器的概率均为 $2^{-494.26}$。

若将区分器的第二部分 E^1 末尾减少一轮，即从第 19 轮到第 37 轮，那么得到概率为 $q=2^{-48}$ 的差分特征 $\gamma\to\delta$：

$$(0,0,0,0,0,\omega,\sigma\oplus(\omega^{<<<s_3}),\omega^{<<<s_4})\xrightarrow{19r}(\omega^{<<<s_4},0,0,0,0,\sigma,\omega,\omega^{<<<s_3})$$

然而，以上 38 轮区分器的概率均为 $2^{-446.26}$。

利用上述 38 轮和 39 轮相关密钥矩形区分器对全轮 ARIRANG-256 进行攻击，方法与第 4 节类似，得到的攻击结果与第 4 节也相同。

表 4　E^0 的差分特征

轮数(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	$\Delta k_i(L,R)$	概率
−1	0	0	0	0	0	σ	0	σ	—	—
0	σ	0	0	0	0	0	σ	0	(0,0)	1
1	0	0	0	0	0	0	0	σ	(σ,0)	1
2	σ	0	0	0	0	0	0	0	(0,0)	1
3	0	0	0	0	0	0	0	0	(σ,0)	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
16	0	0	0	0	0	0	0	0	(0,0)	1
17	$\omega^{<<<s_4}$	0	0	0	0	σ	ω	$\omega^{<<<s_3}$	(0,σ)	2^{-24}
18	$\omega^{<<<s_3}$	$\omega^{<<<s_4}$	ϵ	$\epsilon^{<<<s_1}$	$\epsilon^{<<<s_2}$	0	σ	ω	(0,0)	2^{-24}

表 5　E^1 的差分特征

轮数(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	$\Delta k_i(L,R)$	概率
18	0	0	0	0	0	ω	$\sigma\oplus(\omega^{<<<s_3})$	$\omega^{<<<s_4}$	—	—
19	0	0	0	0	0	σ	0	σ	(0,σ)	2^{-24}
20	σ	0	0	0	0	0	σ	0	(0,0)	1
21	0	0	0	0	0	0	0	σ	(σ,0)	1
22	σ	0	0	0	0	0	0	0	(0,0)	1
23	0	0	0	0	0	0	0	0	(σ,0)	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
36	0	0	0	0	0	0	0	0	(0,0)	1
37	$\omega^{<<<s_4}$	0	0	0	0	σ	ω	$\omega^{<<<s_3}$	(0,σ)	2^{-24}
38	$\omega^{<<<s_3}$	$\omega^{<<<s_4}$	ϵ	$\epsilon^{<<<s_1}$	$\epsilon^{<<<s_2}$	0	σ	ω	(0,0)	2^{-24}

6　改进的高概率相关密钥矩形区分器及其攻击结果

在前两节得到的区分器基础上，利用模减差分和异或差分的混合表示方式代替原先单一的异或差分，在区分器的输出中选择一个差分集合代替原先的差分。利用这两种改进方案，得到概率更高的区分器，具体的改进过程如下。

在第 5 节得到的 38 轮区分器的第 19 轮输入差分中取 $\sigma=0x(03)_4$，$\omega=0x(18)_4$ 和 $\epsilon=0x(9d)_4$。若将此区分器的第二部分 E^1 的输出差分变为模减差分和异或差分的混合，但其输入差分仍然采用异或差分，那么第 19 轮到第 37 轮的差分特征 $\gamma\to\delta$ 变为：

$$(0,0,0,0,0,0x(18)_4,0,0x(0c)_4)\xrightarrow{19r}(Z^{<<<s_4},0,0,0,$$

$0,0x(03)_4,Z,Z^{<<<s_3})$

这里 Z 表示第 37 轮右面的非线性函数 $g^{(256)}$ 作用后的输出异或差分，但是 $g^{(256)}$ 中的每个 S 盒必须满足如下条件：

$$S(x)-S(x\oplus 0x03)=\Omega$$

其中，Ω 表示每个 S 盒的输出模减差分，且 $\Omega=50$（或 -50）（通过 C 编程得出，满足上式的 x 有 6 个不同的值），那么满足 $S'(y)-S'(y\oplus 0x(03)_4)=\Omega\cdot(1+2^8+2^{16}+2^{24})$ 的 32bit 的 y 有 6^4 个不同的值（S' 表示非线性函数 $g^{(256)}$ 中 4 个并置的 S 盒运算，下同），于是第 37 轮差分特征的概率为 $2^{-32}\cdot 6^4\approx 2^{-21.66}$。进而得到改进后区分器第二部分 E^1 差分特征的概率为 $\hat{q}=(\sum_{\gamma}q^2)^{1/2}=(2^{-45.66\cdot 2}+126\cdot 2^{-49.66\cdot 2})^{1/2}\approx 2^{-45.37}$，计算得到新区分器的概率约为 $2^{-441.58}$。

然而，满足以上条件的输出差分 Z 至多有 6^4 个不同的值，那么在进行密文四元组淘汰时，需要检验的等式有所增多，即至多有 6^4 组类似于第 4.4 节 3）中的等式组。通过计算，攻击所需 $2^{222.79}$ 个明文结构，那么数据复杂度为 $2^{222.79}\cdot 2^2=2^{224.79}$。经过对密文四元组的淘汰，剩余满足条件的四元组至多为 $(2^{222.79})^2\cdot(2^{-32\cdot 5})^2\cdot 6^4\approx 2^{135.92}$。

同样，猜测第 39 轮的密钥 k_t^a（$t=78,79$），对以上满足条件的四元组进行解密，恢复出第 39 轮的输入四元组，再进行类似第 4.4 节 4）中的条件检验，这时也至多有 6^4 组这样的等式组。此时剩余的四元组至多有 $2^{135.92}\cdot 2^{-32\cdot 4}\cdot 6^4\approx 2^{18.26}$，上述解密所需时间复杂度至多为 $(2^{135.92}\cdot 2^{32}+2^{32}\cdot 2^{135.92}\cdot 2^{-32\cdot 2}\cdot 6^4\cdot 2^{32})\cdot 4/(2\cdot 40)\approx 2^{163.60}$。再猜测第 38 轮的密钥 $k_{38}^{a_6}$，对满足条件的四元组进行部分解密，从而判断是否满足类似第 4.4 节 5）的条件，此过程所需时间复杂度约为 $(2^{32})^2\cdot 2^{18.26}\cdot 2^{32}\cdot 4/(2\cdot 40)\approx 2^{109.94}$。

重复以上步骤，直到正确密钥唯一确定。为验证得到的可能正确密钥，这里还可以判断以下条件是否成立：

$$S'(F_{38,j}^a)-S'(F_{38,j}^c)=\Omega\cdot(1+2^8+2^{16}+2^{24})$$

$$S'(F_{38,j}^b)-S'(F_{38,j}^d)=\Omega\cdot(1+2^8+2^{16}+2^{24})$$

综上，整个攻击过程所需数据复杂度为 $2^{224.79}$，时间复杂度至多为 $2^{163.60}$，同时攻击成功的概率仍为 99.96%。

若将上述 S' 满足的条件换为：$S'(y)-S'(y\oplus 0x(03)_4)=\Omega\cdot(\pm 1\pm 2^8\pm 2^{16}\pm 2^{24})$，那么满足条件的 y 值有 12^4 个，于是第 37 轮差分特征的概率为 $2^{-32}\cdot 12^4=2^{-17.66}$。进而得到改进后区分器第二部分 E^1 差分特征的概率为：

$$\hat{q}=(\sum_{\gamma}q^2)^{1/2}=(2^{-41.66\cdot 2}+126\cdot 2^{-45.66\cdot 2})^{1/2}\approx 2^{-41.37}$$

这样得到区分器的概率约为 $2^{-433.58}$。然而满足此条件的输出差分 Z 也至多有 6^4 个不同的值，通过进行类似的分析，得到攻击所需的数据复杂度为 $2^{220.79}$，时间复杂度至多为 $2^{155.60}$。

同样，在第 5 节得到的 39 轮区分器的第 19 轮输入差分中取 $\sigma=0x(bc)_4$，$\omega=0x(06)_4$ 和 $\varepsilon=0x(18)_4$，对其第二部分 E^1 也可以进行类似的改进，那么第 19 轮到第 38 轮的差分特征 $\gamma\to\delta'$ 变为：

$$(0,0,0,0,0,0x(06)_4,0x(7c)_4,0x(03)_4)\xrightarrow{20r}(0x(c0)_4,0x(03)_4,Z,Z^{<<<s_1},Z^{<<<s_2},0,0x(bc)_4,0x(06)_4)$$

其中 Z 的含义如上，S' 满足的条件为 $S'(y)-S'(y\oplus 0x(03)_4)=50\cdot(\pm 1\pm 2^8\pm 2^{16}\pm 2^{24})$，通过计算，即可得到此区分器的概率约为 $2^{-481.58}$，对全轮算法攻击的数据复杂度为 $2^{244.79}$，时间复杂度至多为 $2^{139.60}$。

结束语 本文对全轮 ARIRANG-256 加密模式抵抗相关密钥矩形攻击的能力进行了重新评估，通过寻找新的区分器以及对区分器进行改进，得到了概率更高的相关密钥区分器，利用其对全轮加密模式进行了攻击。攻击结果表明：与已有的结果相比较，新攻击在数据复杂度和时间复杂度上均有优势，尤其是攻击所需时间复杂度大幅降低。类似地，考虑利用本文对相关密钥矩形攻击区分器的改进方案，对其它分组密码算法抗相关密钥矩形攻击的能力进行重新评估.

参 考 文 献

[1] Kim J, Kim G, Hong S, et al. The related-key rectangle attack-application to SHACAL-1[C]//Wang H. Proceedings of ACISP 2004, LNCS 3108. Berlin Heidelberg: Springer- Verlag, 2004: 33-42

[2] Wang G. Related-key rectangle attack on 43-round SHACAL-2 [C]//Dawson E, Wong D S. Proceedings of ISPEC 2007, LNCS 4464. Berlin Heidelberg: Springer-Verlag, 2007: 33-42

[3] 韦永壮，胡予濮. 42 轮 SHACAL-2 新的相关密钥矩形攻击[J]. 通信学报，2009，30(1)：7-11

[4] Dunkelman O, Fleischmann E, Gorski M, et al. Related-key rectangle attack of the full HAS-160 encryption mode [C]//Roy B, Sendrier N. Proceedings of INDOCRYPT 2009, LNCS 5922. Berlin Heidelberg: Springer-Verlag, 2009: 157-168

[5] 韦永壮，胡予濮. 简化 AES-192 和 AES-256 的相关密钥矩形新攻击[J]. 中国科学 F 辑：信息科学，2009，39(2)：246-253

[6] Chang D, Hong S, Kang C, et al. ARIRANG: SHA-3 proposal [EB/OL]. http://csrc. nist. gov/groups/ST/hash/sha-3/Ro-und1/documents/ARIRANG. zip, 2009

[7] Hong D, Kim W H, Koo B. Preimage Attack on ARIRANG [EB/OL]. http://eprint. iacr. org/2009/147, 2009

[8] Hong D, Koo B, Kim W H, et al. Preimage attacks on reduced steps of ARIRANG and PKC98-hash[C]//Lee D and Hong S. Proceedings of ICISC 2009, LNCS 5984. Berlin Heidelberg: Springer-Verlag, 2010: 315-331

[9] Ohtahara C, Okada K, Sasaki Y, et al. Preimage Attacks on Full-ARIRANG[C]//Parampalli U and Hawkes P. Proceedings of ACISP 2011, LNCS 6812. Berlin Heidelberg: Springer-Verlag, 2011: 417-422

[10] 张鹏，李瑞林，李超. 对完整轮数 ARIRANG 加密模式的相关密钥矩形攻击[J]. 通信学报，2011，32(8)：15-22