Journal of Computer Applications
计算机应用,2014,34(1):69-72,112
ISSN 1001-9081
CODEN JYIIDU
2014-01-10
http://www.joca.cn

文章编号:1001-9081(2014)01-0069-04
doi:10.11772/j.issn.1001-9081.2014.01.0069

ARIRANG-256 的 Biclique 攻击

卫宏儒[1*],郑雅菲[1],王新宁[2]
(1.北京科技大学 数理学院,北京 100083;2.北京科技大学 基础学科教研室,北京 102100)
(*通信作者电子邮箱 zhengyafei111@sina.com)

摘　要:对 SHA-3 计划候选算法 ARIRANG 采用的分组密码 ARIRANG-256 进行了安全性分析。利用 ARIRANG-256 的密钥扩展与算法本身的加密结构,建立 9 轮 32 维的 Bicliques,并利用建立的 Bicliques 给出完整 40 轮 ARIRANG-256 的 Biclique 攻击结果,数据复杂度为 2^{32},计算复杂度为 $2^{510.8}$。攻击对数据量的要求非常小且计算复杂度优于穷举搜索攻击,是 Biclique 攻击在分组密码全轮安全性分析中的又一次成功应用。

关键词:分组密码;ARIRANG-256;Biclique 攻击;中间相遇;复杂度
中图分类号:TP309.7　　**文献标志码**:A

Biclique cryptanalysis of ARIRANG-256

WEI Hongru[1*], ZHENG Yafei[1], WANG Xinning[2]
(1. *School of Mathematics and Physics, University of Science and Technology Beijing, Beijing* 100083, *China*;
2. *Department of Basic Courses, University of Science and Technology Beijing, Beijing* 102100, *China*)

Abstract: The security of block cipher ARIRANG-256 used in the compression function of ARIRANG, which was one candidate of SHA-3, was analyzed. Based on the key schedule and the encryption structure of the algorithm, 9-round 32 dimensional Bicliques were constructed, and under these Bicliques, full 40-round ARIRANG-256 was attacked. The data complexity is 2^{32} and the time complexity is $2^{510.8}$. The attack has very small data requirement and its time complexity is better than exhaustive search.

Key words: block cipher; ARIRANG-256; Biclique attack; meet-in-the-middle; complexity

0　引言

散列函数 ARIRANG 是由学者 Chang 等提出的 SHA-3 计划的候选算法之一,为 MD 迭代结构,其压缩函数采用 40 轮非平衡 Feistel 结构,根据输出长度的不同,分为 ARIRANG-224、ARIRANG-256、ARIRANG-384、ARIRANG-512 四个版本[1]。

对分组密码的安全性分析能够从一定程度上反映散列函数的安全性。散列函数 ARIRANG 提出后,密码学界对其安全性进行了评估。Guo 等给出了 26 轮 ARIRANG-256 的碰撞攻击和完整轮数 ARIRANG-224、ARIRANG-384 的伪碰撞攻击[2];Hong 等给出了 35 轮 ARIRANG 的原像攻击[3];2011 年张鹏等首次对完整轮数的 ARIRANG 应用相关密钥矩形攻击,给出 ARIRANG 算法不抵抗相关密钥矩阵攻击的结论[4]。

Biclique 攻击是从散列函数分析中引入分组密码分析的一种新技术[5],适合对密钥生成简单且混淆速度慢的密码算法进行分析。Biclique 攻击已经在对 AES、SQUARE、HIGHT、ARIA-256、Twine、Piccolo、PRESENT、LED 等算法的全轮安全性分析上得出了较好的分析结果。如 Biclique 攻击对 AES-128/192/256 进行全轮分析,虽然并未对 AES 的安全性构成实质上的威胁,但是在全轮 AES 的安全性分析上做出了贡献[6];学者 Hamid Mala 给出了 SQUARE 算法的 Biclique 分析,通过采用独立相关密钥差分建立 3 轮 Biclique,对全轮 SQUARE 算法得到了时间复杂度为 2^{126},数据复杂度为 2^{48} 选择明文的攻击结果[7];Biclique 攻击对全轮的 HIGHT、ARIA-256、Twine、Piccolo-80 以及 PRESENT 和 LED 等算法也都取得了优于穷举攻击的计算复杂度,其详细的分析过程与结果可参见文献[8-12]。

ARIRANG 算法的密钥生成方式简单,每轮的轮子密钥可由初始密钥线性生成。在加密过程中选取输入差分在特定位置时,扩散层可达到较慢的混淆速度。基于 ARIRANG 算法的这两个特点,本文对全 40 轮 ARIRANG 算法应用 Biclique 攻击,攻击的数据复杂度为 2^{32},计算复杂度为 $2^{510.8}$,优于穷举搜索,尤其对数据量的要求较低,是 Biclique 攻击在分组密码算法全轮安全性分析中的又一次成功应用。

1　符号说明与 ARIRANG 算法

1.1　符号说明

表 1 对文章中使用的符号进行说明。

表 1　符号说明

符号	说明
A	比特串
X_i	第 i 轮输入
K^i	K 的第 $i+1$ 个分组($i=0,1,\cdots,31$)
$A \parallel B$	联接 A、B 两个比特串
$A^{<<<s}$	比特串 A 左循环移位 s 比特
v_j^i	第 j 轮输出的第 $i+1$ 个分组,$i=0,1,\cdots,7$

收稿日期:2013-07-02;**修回日期**:2013-09-25。
基金项目:国家自然科学基金资助项目(61272476);内蒙古自治区科技创新引导奖励基金资助项目(2012)。
作者简介:卫宏儒(1963-),男,陕西宝鸡人,副教授,主要研究方向:数学、信息安全、密码学、物联网;　郑雅菲(1988-),女,河北任丘人,硕士研究生,主要研究方向:密码学;　王新宁(1974-),女,北京人,讲师,主要研究方向:计算机网络、信息系统。

1.2 ARIRANG 算法

分组密码 ARIRANG-256 分组长度为 256 比特，密钥长度为 512 比特，为 40 轮迭代分组密码。算法轮函数采用如图 1 所示的非平衡 Feistel 结构，记第 i 轮的输入为：

$$X_i = A_i \| B_i \| C_i \| D_i \| E_i \| F_i \| G_i \| H_i$$

则第 $i(i = 0,1,\cdots,39)$ 轮的输出为：

$$X_{i+1} = A_{i+1} \| B_{i+1} \| C_{i+1} \| D_{i+1} \| E_{i+1} \| F_{i+1} \| G_{i+1} \| H_{i+1}$$

其中：

$$T_1 \leftarrow g^{(l)}(A_i \oplus k_{2i}), T_2 \leftarrow g^{(l)}(E_i \oplus k_{2i+1})$$

$$B_{i+1} \leftarrow A_i \oplus k_{2i}, F_{i+1} \leftarrow E_i \oplus k_{2i+1}$$

$$C_{i+1} \leftarrow B_i \oplus T_1, G_{i+1} \leftarrow F_i \oplus T_2$$

$$D_{i+1} \leftarrow C_i \oplus (T_1^{<<<s_1})$$

$$H_{i+1} \leftarrow G_i \oplus (T_2^{<<<s_3})$$

$$E_{i+1} \leftarrow D_i \oplus (T_1^{<<<s_2})$$

$$A_{i+1} \leftarrow H_i \oplus (T_2^{<<<s_4})$$

其中：$l = 256/512$，$k_{2i}k_{2i+1}$ 为第 i 轮的轮密钥，在 ARIRANG-256 中有 $(s_1, s_2, s_3, s_4) = (13,23,29,7)$，每个 $g^{(l)}$ 运算中均包含 4 个 8 × 8 的 S 盒操作。

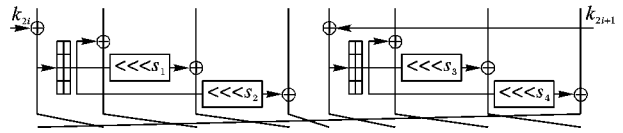

图 1 ARIRANG 算法的轮函数

ARIRANG 算法的密钥扩展由两部分组成。首先由初始密钥 $MK = (m_0, m_1, \cdots, m_{15})$ 扩展成：$w_i (i = 0,1,\cdots,31)$

$$w_i = m_i;\ i = 0,1,\cdots,15$$

$$w_{16} = (w_9 \oplus w_{11} \oplus w_{13} \oplus w_{15} \oplus s_0)^{<<<r_0}$$

$$w_{17} = (w_8 \oplus w_{10} \oplus w_{12} \oplus w_{14} \oplus s_1)^{<<<r_1}$$

$$w_{18} = (w_1 \oplus w_3 \oplus w_5 \oplus w_7 \oplus s_2)^{<<<r_2}$$

$$w_{19} = (w_0 \oplus w_2 \oplus w_4 \oplus w_6 \oplus s_3)^{<<<r_3}$$

$$w_{20} = (w_{14} \oplus w_4 \oplus w_{10} \oplus w_0 \oplus s_4)^{<<<r_0}$$

$$w_{21} = (w_{11} \oplus w_1 \oplus w_7 \oplus w_{13} \oplus s_5)^{<<<r_1}$$

$$w_{22} = (w_6 \oplus w_{12} \oplus w_2 \oplus w_8 \oplus s_6)^{<<<r_2}$$

$$w_{23} = (w_3 \oplus w_9 \oplus w_{15} \oplus w_5 \oplus s_7)^{<<<r_3}$$

$$w_{24} = (w_{13} \oplus w_{15} \oplus w_1 \oplus w_3 \oplus s_8)^{<<<r_0}$$

$$w_{25} = (w_4 \oplus w_6 \oplus w_8 \oplus w_{10} \oplus s_9)^{<<<r_1}$$

$$w_{26} = (w_5 \oplus w_7 \oplus w_9 \oplus w_{11} \oplus s_{10})^{<<<r_2}$$

$$w_{27} = (w_{12} \oplus w_{14} \oplus w_0 \oplus w_2 \oplus s_{11})^{<<<r_3}$$

$$w_{28} = (w_{10} \oplus w_0 \oplus w_6 \oplus w_{12} \oplus s_{12})^{<<<r_0}$$

$$w_{29} = (w_{15} \oplus w_5 \oplus w_{11} \oplus w_1 \oplus s_{13})^{<<<r_1}$$

$$w_{30} = (w_2 \oplus w_8 \oplus w_{14} \oplus w_4 \oplus s_{14})^{<<<r_2}$$

$$w_{31} = (w_7 \oplus w_{13} \oplus w_3 \oplus w_9 \oplus s_{15})^{<<<r_3}$$

用于每轮加密的轮密钥 $K = k_0, k_1, \cdots, k_{79}$ 通过 $k_i = w_{\sigma(i)} (i = 0,1,\cdots,79)$ 得到。本文攻击不涉及 S 盒的具体操作，故不再介绍，其详细设计与常数 s_i、r_i 以及 σ 变换的取值请参见文献[1]。

2 Biclique 攻击

将 Biclique 攻击应用于分组密码算法，首先假设密码算法 E 可以表示为 3 个子密码的连接：$E = f \circ g \circ h$，S 表示明文 P 在 f 作用下的结果，即 $f_K(P) = S$。假设 f 是在包含 2^{2d} 个子密钥的密钥组 $\{K[i,j]\}$ 作用下，关于 2^d 个中间变量 $\{S_j\}$ 与 2^d 个明文 $\{P_i\}$ 的函数，则若有 $S_j = f_{K[i,j]}(P_i), \forall i,j \in \{0,1,\cdots,2^d - 1\}$ 成立，那么三元组 $\{\{P_i\},\{S_j\},K[i,j]\}$ 称为一个 d 维 Biclique。

总结分组密码 Biclique 攻击的步骤如下：

1）密钥分割。将密钥空间分割成 2^{k-2d} 组，k 为原始密钥长度，则每组有 2^{2d} 个子密钥。对每一组密钥进行下一步操作。

2）建立 Biclique。建立 2^d 个中间变量 $\{S_j\}$ 与 2^d 个明文 $\{P_i\}$ 间满足如下方程的结构：

$$S_j = f_{K[i,j]}(P_i);\ \forall i,j \in \{0,1,\cdots,2^d - 1\}$$

3）数据收集。收集明密文对 (P_i, C_i)。

4）匹配检查。检查是否存在 i, j 满足：

$$g \circ h_{K[i,j]}(S_j) = C_i$$

文献[6]给出了建立 Biclique 的两种方法，本文选择利用两条独立相关密钥来建立 Biclique 结构。

设基础运算为：

$$P_0 \xrightarrow[f]{K[0,0]} S_0$$

首先根据 ARIRANG-256 的密钥生成方式选取两条独立相关密钥差分 Δ_i^k 与 ∇_j^k。

令 $\Delta S = 0$，密钥差分为 Δ_i^k 时，可得到：

$$\Delta_i = \Delta P = P_0 \oplus P_i$$

$$0 \xrightarrow[f^{-1}]{\Delta_i^k} \Delta_i$$

令 $\Delta P = 0$，密钥差分为 ∇_j^k 时，可得到

$$\nabla_j = \Delta S = S_0 \oplus S_j$$

$$\nabla_j \xrightarrow[f^{-1}]{\nabla_j^k} 0$$

两密钥差分集合不共享任意活跃 S 盒，所以有：

$$\nabla_j \xrightarrow[f^{-1}]{\nabla_j^k \oplus \Delta_i^k} \Delta_i;\ \forall i,j \in \{0,1,\cdots,2^d - 1\}$$

因为所有以上结果均是基于基础运算[$\{P_0\}$, $\{S_0\}$, $\{K[0,0]\}$]取得的，故有：

$$S_0 \oplus \nabla_j \xrightarrow[f^{-1}]{\nabla_j^k \oplus \Delta_i^k \oplus K[0,0]} P_0 \oplus \Delta_i$$

$$P_i = P_0 \oplus \Delta_i$$

$$S_j = S_0 \oplus \nabla_j$$

$$K[i,j] = K[0,0] \oplus \Delta_i^k \oplus \nabla_j^k$$

这样得到的三元组[$\{P_i\}$, $\{S_j\}$, $\{K[i,j]\}$]即为一个 d 维 Biclique。接下来即可对剩余轮数 $g \circ h$ 应用中间相遇匹配来得到最终的分析结果。首先计算 $C_i = E_K(P_i)$，然后选取 g 与 h 过程中的一个中间匹配位 v，最后通过中间相遇部分匹配来筛选正确密钥。

3 ARIRANG-256 的 Biclique 攻击

首先将密钥空间分割成 2^{448} 个密钥子空间，每个子空间包含 2^{32} 个密钥。对每一个密钥子空间建立 0 到第 8 轮的 Biclique，并基于建立的 Biclique 对剩余 31 轮加密应用中间相遇攻击，从而得到全轮的分析结果。

3.1 密钥分割

根据密钥扩展策略推测各轮子密钥。表 2 给出各轮子密钥涉及初始密钥分组 $MK = (m_0, m_1, \cdots, m_{15})$ 的情况。

表 2　轮子密钥涉及初始密钥分组的情况

R	m_i	R	m_i	R	m_i	R	m_i
0	m_9,m_{11},m_{13},m_{15}; m_8,m_{10},m_{12},m_{14}	10	m_{14},m_4,m_{10},m_0; m_{11},m_1,m_7,m_{13}	20	m_{13},m_{15},m_1,m_3; m_4,m_6,m_8,m_{10}	30	m_{10},m_0,m_6,m_{12}; m_{15},m_5,m_{11},m_1
1	$m_0;m_1$	11	$m_3;m_6$	21	$m_{12};m_5$	31	$m_7;m_2$
2	$m_2;m_3$	12	$m_9;m_{12}$	22	$m_{14};m_7$	32	$m_{13};m_8$
3	$m_4;m_5$	13	$m_{15};m_2$	23	$m_0;m_9$	33	$m_3;m_{14}$
4	$m_6;m_7$	14	$m_5;m_8$	24	$m_2;m_{11}$	34	$m_9;m_4$
5	m_1,m_3,m_5,m_7; m_2,m_4,m_6,m_8	15	m_6,m_{12},m_2,m_8; m_3,m_9,m_{15},m_5	25	m_5,m_7,m_9,m_{11}; m_{12},m_{14},m_0,m_2	35	m_2,m_8,m_{14},m_4; m_7,m_{13},m_3,m_9
6	$m_8;m_9$	16	$m_{11};m_{14}$	26	$m_4;m_{13}$	36	$m_{15};m_{10}$
7	$m_{10};m_{11}$	17	$m_1;m_4$	27	$m_6;m_{15}$	37	$m_5;m_0$
8	$m_{12};m_{13}$	18	$m_7;m_{10}$	28	$m_8;m_1$	38	$m_{11};m_6$
9	$m_{14};m_{15}$	19	$m_{13};m_0$	29	$m_{10};m_3$	39	$m_1;m_{12}$

观察初始密钥的 16 个分组在算法 0 到第 8 轮加密密钥中的使用情况,选取 $K_{0,0}=(****|****|****|**00)$ 为基础密钥,其中 $K_{0,0}^{14}K_{0,0}^{15}$ 两个分组值为 0,其他分组取任意值。一个包含 2^{64} 个密钥的子密钥空间可记为:

$$K_{i,j}=K_{0,0}\oplus(0000|0000|0000|00ij);\quad i,j\in\{0,1,\cdots,2^{32}-1\}$$

3.2　建立 9 轮 Biclique

随机选取明文 P_0 并计算 $S_0=f_{K_{0,0}}(P_0)$,其中 f 表示 0 到第 8 轮加密。以下通过两个包含 2^{32} 条基于 $P_0\xrightarrow{K_{0,0}}S_0$ 的相关密钥差分的集合来构建 Biclique。

f 上的 Δ_i 差分路径:在密钥差分 $\Delta_i^K=(0000|0000|0000|00i0)$ 下计算,当输出差分 $\Delta S=0$ 时,输入差分为 $\Delta_i=\Delta P=P_0\oplus P_i$。

f 上的 ∇_j 差分路径:在密钥差分 $\nabla_j^K=(0000|0000|0000|000j)$ 下计算,当输入差分 $\Delta P=0$ 时,输出差分为 $\nabla_j=\nabla S=S_0\oplus S_j$。即有:

$$0\xrightarrow[f^{-1}]{\Delta_i^K}\Delta_i$$

$$0\xrightarrow[f]{\nabla_j^K}\nabla_j$$

观察表 1 中数据可见,m_{14} 与 m_{15} 仅在第一轮 $R=0$ 时用到,且位于不同的位置,即不共享任何活跃 S 盒,∇_i^k 与 Δ_j^k 为两条 ARIRANG-256 的首 9 轮独立密钥差分。所以 $\forall i,j\in\{0,1,\cdots,2^{32}-1\}$ 有下式成立:

$$\Delta_i\xrightarrow[f]{\Delta_i^k\oplus\nabla_j^k}\nabla_j$$

$$P_i\oplus\Delta_i\xrightarrow[f]{\Delta_i^k\oplus\nabla_j^k\oplus K[0,0]}S_0\oplus\nabla_j$$

只需取:

$$P_i=P_0\oplus\Delta_i$$

$$S_j=S_0\oplus\nabla_j$$

$$K[i,j]=K[0,0]\oplus\Delta_i^k\oplus\nabla_j^k$$

得到的三元组$[\{P_i\},\{S_j\},\{K[i,j]\}]$即为一个 32 维 9 轮 Biclique。$\Delta_i$ 与 ∇_j 的推导过程如图 2 所示。

观察 $P_i=P_0\oplus\Delta_i$,明文中仅在第 5 个分组处存在差分,所以选择明文仅在第 5 个分组处取遍所有可能值,其他位置均为固定值,即攻击对数据量的要求不超过 2^{32}。

3.3　中间相遇过程

每个 Biclique 中有 2^{32} 个明文 P_i 与 2^{32} 个中间状态 S_j,且每个 P_i 与 S_j 之间由 $K[i,j]$ 唯一相连。攻击者对每个 P_i 相应

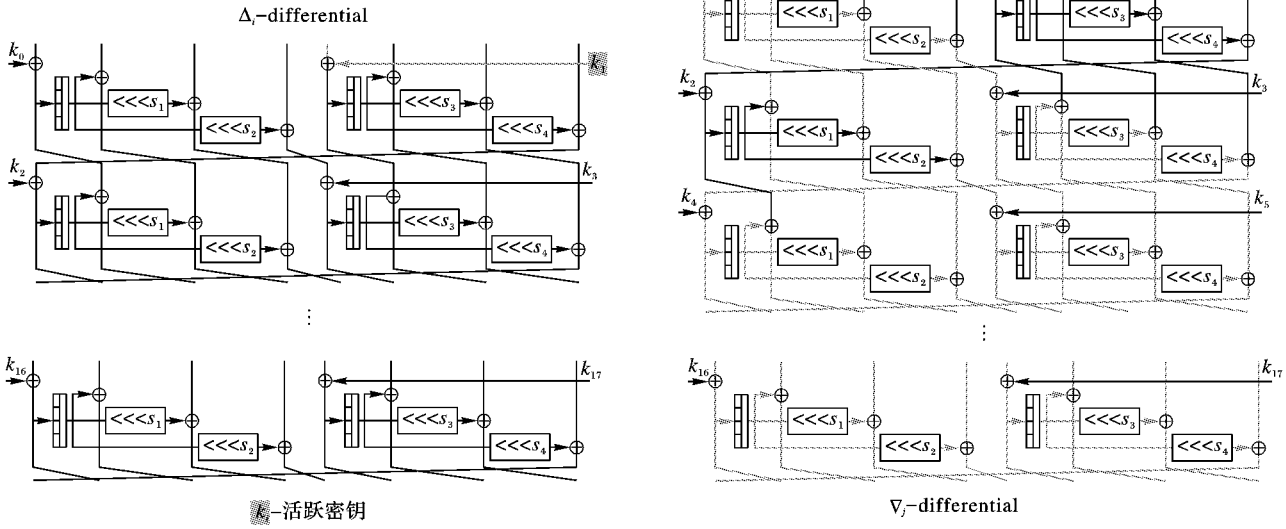

图 2　由 Δ_i^k 与 ∇_j^k 建立的 8 轮 Biclique

的 C_i 检查是否存在 j 使下式成立：

$$C_i \xrightarrow{K[i,j]} S_j$$

该步计算复杂度为 2^{2d}，这样整体的计算复杂度将为 $2^{k-2d} \times 2^{2d}$，接近穷举攻击的计算量。以下考虑利用预计算与中间相遇匹配方法来降低复杂度。

首先计算并存储如下 2^d 次部分加密与 2^d 次部分解密：

$$j = 0,1,\cdots,2^d - 1: S_j \xrightarrow{K[0,j]} v'$$

$$i = 0,1,\cdots,2^d - 1: v'' \xleftarrow{K[i,0]} C_i$$

其中：$v'v''$ 为 g、h 在某一轮达到匹配的中间状态，该步被称为基础计算。对每种密钥候选值，分别计算 v' 与 v''：若 $v' \neq v''$，则判定为错误密钥；若 $v' = v''$，则利用其他明密文对进行再次检验。重复该过程，直到得到唯一正确密钥。

表 3 Biclique 攻击参数

参数	值
总轮数	40
Biclique 维数	32
Biclique 长度	9(0～8)
匹配位	v_{19}^1
前向	9～19
后向	20～39

本文攻击考虑在第 19 轮的第 2 个分组 v_{19}^1 处进行匹配，每次匹配对密钥候选值的筛选概率为 2^{-32}。前向与后向计算的具体匹配过程如图 3 所示。

利用不同的密钥候选值，对选择明文进行加密计算 v_{19}^1 的值时，有些 S 盒不涉及(白色)，故不需计算；有些 S 盒不受密钥差分影响(灰色)，故仅需计算 1 次，称其为不活跃 S 盒；蓝色的活跃 S 盒受密钥差分影响，需要重复进行 2^{32} 次运算。对相应密文进行解密计算 v_{19}^1 同样如此。

图 3 中，前向与后向计算不涉及 S 盒 12 + 16 = 28 个，涉及活跃 S 盒 68 + 72 = 140 个，涉及不活跃 S 盒 8 + 72 = 80 个。在匹配过程中，非线性的 S 盒运算占据了主要计算量，因此，减少 S 盒的运算次数即可降低整个攻击的计算复杂度。本文中即利用 S 盒运算的减少量来衡量计算复杂度改善的程度。

3.4 攻击复杂度

攻击的计算复杂度由几部分构成。在 Biclique 构造阶段，对 2^{448} 个 Biclique 中的每一个都要进行 2^{32} 次 9 轮加密来得到 2^{32} 个中间状态 S_j；因为数据复杂度不超过 2^{32}，数据收集阶段不超过 2^{32} 次加密；中间相遇部分匹配阶段包括预计算和重新计算两个步骤，预计算为 2^{32} 次 8 轮加密，每个 Biclique 的重新计算可用 $2^d \times (72+68) = 2^{32} \times 140$ 个 S 盒计算来表示，又 40 轮加密所需 S 盒计算总数为 $8 \times 40 = 320$ 个，则重新计算的复杂度可用 $2^{2d} \times (140/320) \approx 2^{2d-1.2}$ 来表示。

综上，中间相遇匹配阶段的总的计算复杂度约为：

$$2^d \times (80/320) + 2^{2d} \times (140/320) \approx 2^{2d-1.2}$$

完整 Biclique 攻击的计算复杂度为：

$$TC = 2^{k-d} \times \frac{8}{40} + 2^{32} + 2^{k-d} \times \frac{32}{40} + 2^{k-2d} \times 2^{2d-1.2} \approx 2^{510.8}$$

由 3.2 节分析可知数据复杂度不超过 2^{32}。

存储复杂度由两部分组成，存储一个 Biclique 需存储 $2^{d+1} = 2^{33}$ 个明文与中间状态值与 $2^{2d} = 2^{64}$ 个密钥。预计算所需的存储为 $2^{d+1} = 2^{33}$。所以总的存储复杂度为：$2^{33} + 2^{33} + 2^{64} \approx 2^{64}$。

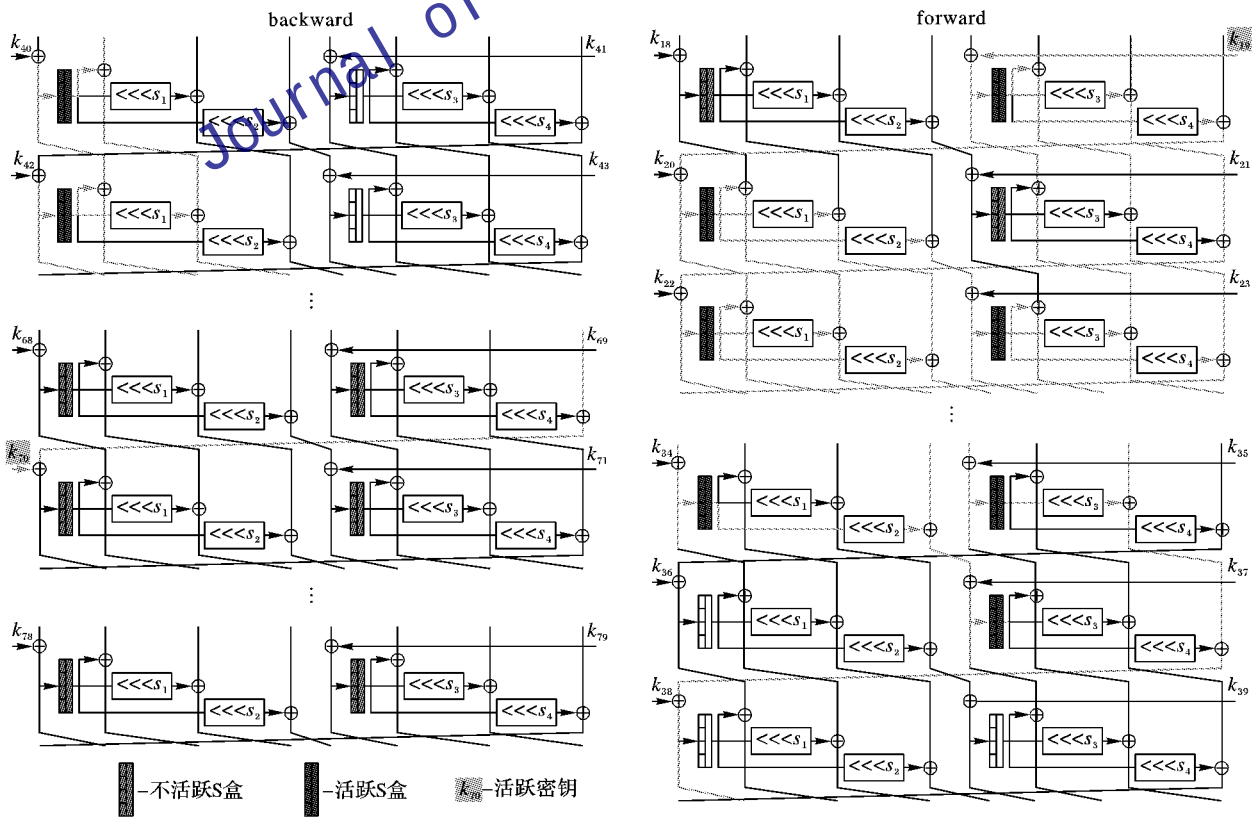

图 3 中间相遇匹配过程

(下转第 112 页)

3 结语

本文提出了一种基于攻击图与报警数据相似性分析的混合报警关联模型。模型首先在报警数据预处理中消除了 IDS 产生的周期性误报警和重复报警，然后将预处理后的报警数据根据攻击图或报警相似度进行关联，进而重构入侵攻击场景。模型能够对初始攻击图的定义缺陷利用报警数据相似分析进行完善与补充。实验验证了混合模型的有效性。

模型中报警相似度计算的属性权值和判断阈值是人工设定的，权值的设定与具体的攻击类型相关，因此限制模型的应用范围。进一步的工作将利用学习的方法调整报警相似性分析的判断阈值，使其能够适应网络环境和攻击的变化。

参考文献：

[1] MAINES J, KEWLEY D, TINNEL L, *et al*. Validation of sensor alert correlators [J]. IEEE Security & Privacy Magazine, 2003, 1(1): 46 – 56.

[2] NING P, YUN C, REEVES D S, *et al*. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security, 2004, 7(2): 274 – 318.

[3] DEBAR H, WESPI A. Aggregation and correlation of intrusion-detection alerts [C]// RAID 2001: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, LNCS 2212. Berlin: Springer-Verlag, 2001: 85 – 103.

[4] VALDES A, SKINNER K. Probabilistic alert correlation [C]// RAID 2001: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, LNCS 2212. Berlin: Springer-Verlag, 2001: 54 – 68.

[5] REN H, STAKHANOVA N. An online adaptive approach to alert correlation [C]// DIMVA 2010: Proceedings of the 7th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer-Verlag, 2010: 153 – 172.

[6] AHMADINEJAD S H. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer Networks, 2011, 55(9): 2221 – 2240.

[7] AHMADINEJAD S H, JALILI S. Alert correlation using correlation probability estimation and time windows [C]// ICCTD 2009: Proceedings of the 2009 International Conference on Computer Technology and Development. Piscataway, NJ: IEEE Press, 2009: 170 – 175.

[8] CURRY D, DEBAR H. Intrusion detection message exchange format data model and extensible markup language (XML) document type definition [EB/OL]. [2007-05-01]. http://tools.ietf.org/html/rfc4765.2003.

[9] LI D, LI Z, LEI J. Research on the method of reducing false positives with periodicity[J]. Journal of Chinese Computer Systems, 2009, 30(7): 2446 – 2449. (李东, 李之棠, 雷杰. 周期性误告警去除方法研究[J]. 小型微型计算机系统, 2009, 30(7): 1336 – 1340.)

[10] GUO F, YU M, YE J. Alert aggregation algorithm based on category and similarity[J]. Journal of Computer Applications, 2007, 27(10): 2446 – 2449. (郭帆, 余敏, 叶继华. 一种基于分类和相似度的报警聚合方法[J]. 计算机应用, 2007, 27(10): 2446 – 2449.)

[11] CHEN F, ZHANG Y, SU J, *et al*. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4): 838 – 848. (陈锋, 张怡, 苏金树. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4): 838 – 848.)

[12] MIT/LL. 2000 DARPA intrusion detection scenario specific datasets[EB/OL]. [2010-03-26]. http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html.

(上接第 72 页)

4 结语

综合 Biclique 攻击在分组密码安全性分析中的现有应用，可以发现 Biclique 攻击适合应用于密钥扩展策略简单、扩散层混淆速度较慢的算法，而与非线性 S 盒的具体设计无关。考虑这两种因素，本文选择建立 ARIRANG-256 的 0 到第 8 轮 32 维 Biclique，对完整 40 轮的 ARIRANG-256 应用 Biclique 攻击，得到了优于穷举攻击的计算复杂度。与 ARIRANG-256 已有的分析结果相比，本文分析结果的优势体现为全轮攻击且数据复杂度足够小，是 Biclique 攻击在分组密码全轮安全性分析中的又一次成功应用。考虑到 Biclique 攻击较大的计算复杂度，以后的研究方向为 Biclique 攻击在分组密码中应用的改进，进一步减少其计算复杂度。

参考文献：

[1] CHANG D, HONG S, KANG G. ARIRANG: SHA-3 proposal[EB/OL]. [2009-10-10]. http://csrc.nist.govgroups/ST/hash/sha-3/Round1/documents/ARIRANG.zip.

[2] GUO J, MATUSIEWICZ K, KNUDSEN L R. Practical pseudo-collisions for Hash functions ARIRANG-224/384[M]. Berlin: Springer-Verlag, 2009: 141 – 156.

[3] HONG D, KOO B, KIM W H. Preimage attacks on reduced steps of ARIRANG and PKC 98-hash[C]// Proceedings of ICISC 2009. Seoul: [s.n.], 2009: 315 – 331.

[4] ZHANG P, LI R L, LI C. Related-key rectangle attack on the full ARIRANG encryption mode[J]. Journal on Communications, 2011, 32(8): 15 – 22. (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.)

[5] KHOVRATOVICH D, RECHBERGER C, SAVELIEVA A. Bicliques for preimages: attacks on Skein-512 and the SHA-2 family [EB. OL]. [2012-10-10]. http://eprint.iacr.org/2011/286.

[6] BOGDANOV A, KHOVRATOVICH D, RECHBERGER C. Biclique cryptanalysis of the full AES[C]// Proceedings of ASIACRYPT 2011, LNCS 7073. Berlin: Springer-Verlag, 2011: 344 – 371.

[7] MALA H. Biclique cryptanalysis of the block cipher SQUARE[EB/OL]. [2012-10-10]. http://eprint.iacr.org/2011/500.

[8] HONG D, KOO B, KWON D. Biclique attack on the full HIGHT [C]// Proceedings of ICISC 2011, LNCS 7259. Berlin: Springer-Verlag, 2011: 365 – 374.

[9] CHEN S, XU T. Biclique attack of the full ARIA-256[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/011.pdf.

[10] COBAN M, KARAKOC F, BOZTAS O. Biclique cryptanalysis of TWINE[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/422.pdf.

[11] WANG Y, WU W, YU X. Biclique cryptanalysis of reduced-round piccolo block cipher[C]// Proceedings of ISPEC 2012, LNCS 7232. Berlin: Springer-Verlag, 2012: 337 – 352.

[12] ABED F, FORLER C, LIST E, *et al*. Biclique cryptanalysis of the PRESENT and LED lightweight ciphers[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/591.pdf.