计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2014.20130639
51(10):2329-2335,2014

分组密码 SHACAL2 的 Biclique 攻击

郑雅菲　　卫宏儒
(北京科技大学数理学院　北京　100083)
(zhengyafei111@sina.com)

Biclique Cryptanalysis of Block Cipher SHACAL2

Zheng Yafei and Wei Hongru
(*School of Mathematics and Physics*, *University of Science and Technology Beijing*, *Beijing* 100083)

Abstract　SHACAL2 is a block cipher designed by Handschuh H. et al based on the standard Hash function SHA2 in 2002. It one of the European standard block ciphers, and has relatively high security because of its long block length and key length, which are 256b and 512b respectively. There have been a few security analysis results about SHACAL2, such as impossible differential cryptanalysis and related-key rectangle attack on reduced rounds of SHACAL2. Taking advantage of the characteristics of the key schedule and the permutation layer of block cipher SHACAL2, 18-round 32-dimensional Biclique of the first eight rounds of SHACAL2 is constructed. Based on the Biclique constructed, Biclique attack is applied to the whole 64-round SHACAL2. And the results show that, using Biclique attack to recover the whole 512b key information of 64-round SHACAL2, the data complexity is no more than 2^{224} chosen plaintexts, and the time complexity is $2^{511.18}$ 64-round encryptions. Compared with the known analysis results, the data complexity of Biclique attack decreased obviously, and the time complexity is better than exhaustive search. For whole round SHACAL2, Biclique attack is a relatively effective method. This is the first single-key attack for whole round SHACAL2.

Key words　block cipher; SHACAL2; Biclique attack; meet-in-the-middle (MITM) attack; complexity

摘　要　分组密码算法 SHACAL2 是由 Handschuh 等人于 2002 年基于标准散列函数 SHA2 设计的,具有较高的安全性.利用 SHACAL2 算法密钥生成策略与扩散层的特点,构造了 SHACAL2 的首 18 轮 32 维 Biclique.基于构造的 Biclique 对完整 64 轮 SHACAL2 算法应用 Biclique 攻击.分析结果表明,Biclique 攻击恢复 64 轮 SHACAL2 密钥的数据复杂度不超过 2^{224} 已知明文,时间复杂度约为 $2^{511.18}$ 次全轮加密.与已知分析结果相比,Biclique 攻击所需的数据复杂度明显降低,且计算复杂度优于穷举攻击.对全轮的 SHACAL2 算法,Biclique 攻击是一种相对有效的攻击方法.这是首次对 SHACAL2 算法的单密钥全轮攻击.

关键词　分组密码;SHACAL2;Biclique 攻击;中间相遇攻击;复杂度

中图法分类号　TP309

收稿日期:2013-05-02;**修回日期**:2013-12-03

基金项目:内蒙古自治区科技创新引导奖励基金资助项目(2012);国家自然科学基金面上项目(61272476)

2003年,欧洲NESSIE(new european schemes for signatures,integrity,and encryption)计划公布了新的分组密码标准算法:Rijindael[1],MISTY1[2],Camellia[3],SHACAL2[4].其中SHACAL2是基于标准散列函数SHA2设计的,分组长度为256 b,密钥长度为512 b,迭代轮数为64轮,是欧洲分组密码标准算法中分组长度和密钥长度最长的、安全性较高.表1示出SHACAL2算法现有的安全性分析结果:

Table 1 Summary of Cryptanalysis of SHACAL2

表1 SHACAL2算法安全性分析总结

R	Attack	Time Complexity	Data Complexity	Reference
28	Integral Attack	$2^{494.1}$	463×2^{32}	Ref[5]
30	Impossible Differential Cryptanalysis	$2^{495.1}$	744	Ref[6]
35	Related-key Rectangle Attack	$2^{452.1}$	$2^{42.4}$	Ref[7]
42	Related-key Rectangle Attack	$2^{488.37}$	$2^{243.38}$	Ref[8]
42	Related-key Rectangle Attack	$2^{472.6}$	2^{235}	Ref[9]
44	Related-key Rectangle Attack	$2^{497.2}$	2^{233}	Ref[10]
64	Biclique Attack	$2^{511.18}$	2^{224}	This Paper

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[11],适合对密钥生成简单且混淆速度慢的密码算法进行分析,目前在对AES,SQUARE,HIGHT,ARIA-256,TWINE,Piccolo等算法的安全性分析上已经取得了较好的结果.如Biclique攻击对AES-128/192/256进行全轮分析,虽然未对AES的安全性构成实质上的威胁,但是在全轮AES的安全性分析上作出了贡献[12];学者Mala给出了SQUARE算法的Biclique攻击,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[13];Biclique攻击对全轮的HIGHT,ARIA-256,TWINE以及Piccolo-80等分组密码算法也都取得了优于穷举攻击的分析结果[14-17].

SHACAL2算法的密钥生成方式比较简单,每轮的轮子密钥可由初始密钥线性表示.基于该特点,本文对完整64轮SHACAL2算法应用Biclique攻击,攻击的数据复杂度不超过2^{224},计算复杂度为$2^{511.18}$,优于穷举搜索.对全轮SHACAL2算法而言,Biclique攻击是比较有效的一种攻击方法.

1 算法SHACAL2

1.1 符号说明

表2对本文采用的符号进行说明:

Table 2 Symbol Description

表2 符号说明

Symbol	Description
R	Round
$a\parallel b$	Connect a and b
k_i	i-th 32 b Group of k, i Starts from 0
$a_{(b)}$	The Length of a is b
X_t	t-th 32 b Group of X
$S^r_{(64)}$	64 b Output of r-th Round
S^r_t	t-th 32 b Group of the Output of r-th Round

1.2 SHACAL2算法介绍

SHACAL2算法分组长度为256 b,密钥长度为512 b,迭代轮数为64.加密时明文P首先被拆分为8个32 b的子块,即

$$P_{(256)}=A_0\parallel B_0\parallel C_0\parallel D_0\parallel E_0\parallel F_0\parallel G_0\parallel H_0,$$

$$T_1=H_i+f_1(E_i)+g_0(E_i,F_i,G_i)+K_i+W_i,$$

$$T_2=f_0(A_i)+g_1(A_i,B_i,C_i),$$

$$H_{i+1}=G_i,G_{i+1}=F_i,F_{i+1}=E_i,E_{i+1}=D_i+T_1,$$

$$D_{i+1}=C_i,C_{i+1}=B_i,B_{i+1}=A_i,A_{i+1}=T_1+T_2,$$

$$f_0(X)=(X>>>2)\oplus(X>>>13)\oplus(X>>>22),$$

$$f_1(X)=(X>>>6)\oplus(X>>>11)\oplus(X>>>25),$$

$$g_0(X,Y,Z)=(X\cap Y)\oplus(\bar{X}\cap Z),$$

$$g_1(X,Y,Z)=(X\cap Y)\oplus(X\cap Z)\oplus(Y\cap Z).$$

其中,$i=0,1,\cdots,63$.输出256 b密文:

$$C_{(256)}=A_{64}\parallel B_{64}\parallel C_{64}\parallel D_{64}\parallel E_{64}\parallel F_{64}\parallel G_{64}\parallel H_{64}.$$

$W_i(i=0,1,\cdots,63)$为常数,其具体数值参见文献[3].

在生成轮子密钥时,512 b初始密钥首先被分为16个32 b的分组,即$K_{(512)}=k_0\parallel k_1\parallel\cdots\parallel k_{15}$.对$16\leqslant i<64$:

$$k_i=\sigma_1(k_{i-2})+k_{i-7}+\sigma_0(k_{i-15})+k_{i-16},$$

$$\sigma_0(X)=(X>>>7)\oplus(X>>>18)\oplus(X>>3),$$

$$\sigma_1(X)=(X>>>17)\oplus(X>>>19)\oplus(X>>10),$$

即可得到SHACAL2算法64个32 b的轮子密钥.

2 Biclique 攻击

将 Biclique 攻击应用于分组密码,首先假设密码算法 E 可以表示为 3 个子密码的连接:$E=f\circ g\circ h$,且 $S=f_k(P)$. 假设 f 是在 2^{2d} 个密钥集合$\{K[i,j]\}$作用下的关于 2^d 个中间变量$\{S_j\}$与 2^d 个明文$\{P_i\}$的函数,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$\langle\{P_i\},\{S_j\},K[i,j]\rangle$称为一个 d 维 Biclique. 文献[12]给出了利用相关密钥差分路径建立轮数较长 Biclique 的方法. Biclique 攻击适合应用于密钥生成策略较为简单且扩散层混淆速度较慢的分组密码算法.

分组密码 Biclique 攻击的步骤如下:

1) 密钥分割. 对整个密钥空间分组,且各个分组间无交集.

2) 建立 Biclique. 对每个密钥分组建立维数适合的 Biclique.

3) 过滤密钥. 筛除不满足每个 Biclique 要求的错误密钥:

① 确定中间匹配位 v 的位置;

② 对满足 Biclique 形式的明文 P_i 加密得到相应的密文 C_i;

③ 记 $S_j\rightarrow\vec{v}$ 为前向计算,$\overleftarrow{v}\leftarrow C_i$ 为后向计算. 若检验密钥 $K[i,j]$为正确密钥,则有 $S_j\rightarrow\vec{v}$, $\overleftarrow{v}\leftarrow C_i$,且 $\vec{v}=\overleftarrow{v}$ 成立,如此即可排除不满足匹配的错误密钥. 在该过程中利用部分匹配技巧可有效降低匹配过程的计算复杂度,从而降低整个攻击的复杂度.

4) 确定正确密钥. 对剩余的所有候选密钥进行匹配检验,直至得到正确密钥.

Biclique 攻击的结构框架如图 1 所示:

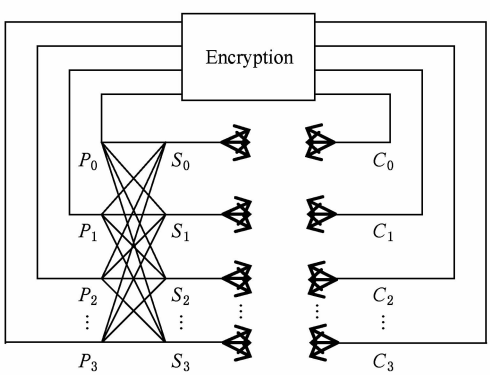

Fig. 1 Framework of Biclique attack.

图 1 Biclique 攻击结构框架

3 SHACAL2 的 Biclique 攻击

要构造 SHACAL2 算法基于密钥差分的 Biclique,首先要得到各轮轮密钥与初始密钥的关系. 根据 SHACAL2 密钥策略推测各轮轮密钥受初始密钥 16 个分组的影响情况如表 3 所示:

Table 3 Derivation of Round Keys

表 3 轮密钥推导

R	Subkey Involved
0～15	$k_i(i=0,1,\cdots,15)$
16	k_0,k_1,k_9,k_{14}
17	k_1,k_2,k_{10},k_{15}
18	$k_2,k_3,k_{11},k_0,k_1,k_9,k_{14}$
19	$k_3,k_4,k_{12},k_1,k_2,k_{10},k_{15}$
20	$k_4,k_5,k_{13},k_2,k_3,k_{11},k_0,k_1,k_9,k_{14}$
21	$k_5,k_6,k_{14},k_3,k_4,k_{12},k_1,k_2,k_{10},k_{15}$
22	$k_6,k_7,k_{15},k_4,k_5,k_{13},k_2,k_3,k_{11},k_0,k_1,k_9,k_{14}$
23	$k_7,k_8,k_0,k_1,k_9,k_{14},k_5,k_6,k_3,k_4,k_{12},k_2,k_{10},k_{15}$
24	$k_8,k_9,k_1,k_2,k_{10},k_{15},k_6,k_7,k_4,k_5,k_{13},k_3,k_{11},k_0,k_{14}$
25～63	$k_8,k_9,k_1,k_2,k_{10},k_{15},k_6,k_7,k_4,k_5,k_{13},k_3,k_{11},k_0,k_{14},k_{11}$

通过观察可发现,在 0～17 轮这 18 轮加密过程中 k_3 只被使用了一次. 在 0～22 轮这 23 轮加密过程中 k_8 只被使用了一次,但基于 k_8 建立 23 轮 32 维 Biclique 结构会使得攻击的数据复杂度为全明文本,即 2^{256} 选择明文,而计算复杂度仅有微小可忽略的变化. 而除 k_8 之外,基于 k_3 建立的 Biclique 结构轮数最长,所以下文选择利用 k_3 建立 SHACAL2 算法的 18 轮 32 维 Biclique 结构,基于建立的 Biclique 结构在接下来的 46 轮加密中应用中间相遇部分匹配,即可实现完整 64 轮 SHACAL2 算法的 Biclique 攻击.

3.1 密钥空间分割

首先定义基础密钥 $K[0,0]$,k_3 固定为 0,除 k_3 外的位置取遍所有的 2^{480} 种可能值. 基于 $K[0,0]$的子密钥空间 $K[i,j](i,j\in\{0,1\}^{32})$可定义为

$$K_0[0,0]=00;$$

$$K_0[i,0]=i0,K_0[0,j]=0j;$$

$$K_0[i,j]=ij.$$

将 512 b 密钥空间分割成 2^{448} 个子密钥空间,每个子密钥空间包含 2^{64} 个密钥值.

3.2 建立 Biclique 结构

定义 f 为 0～17 轮加密,对每一个密钥子空间

建立 18 轮 32 维 Biclique. 对密钥空间完成分割后，可以按照图 2 的方式来计算满足 Biclique 要求的明文与中间状态值.

首先令 $P_0=0_{(256)}$，计算 $S_0=f_{K[0,0]}(P_0)$，此步操作称为基础运算，如图 2(a)所示；然后在密钥 $K[0,j](0<j<2^{32})$下对 S_0 进行解密操作得到相应的明文 P_j，$K[0,j]$与 $K[0,0]$的密钥差分会引起部分明文的差分，在图 2(b)中，用填充黑色表示明文差分；最后在密钥 $K[i,0](0<i<2^{32})$下对 P_0 进行加密得到相应的中间状态值 S_i. $K[i,0]$与 $K[0,0]$间的密钥差分会引起部分中间状态值的差分，如图 2(c)所示，用黑色填充表示受密钥差分影响. 图 2 中填充为灰色的密钥表示受 k_3 影响的轮密钥，称为活跃密钥.

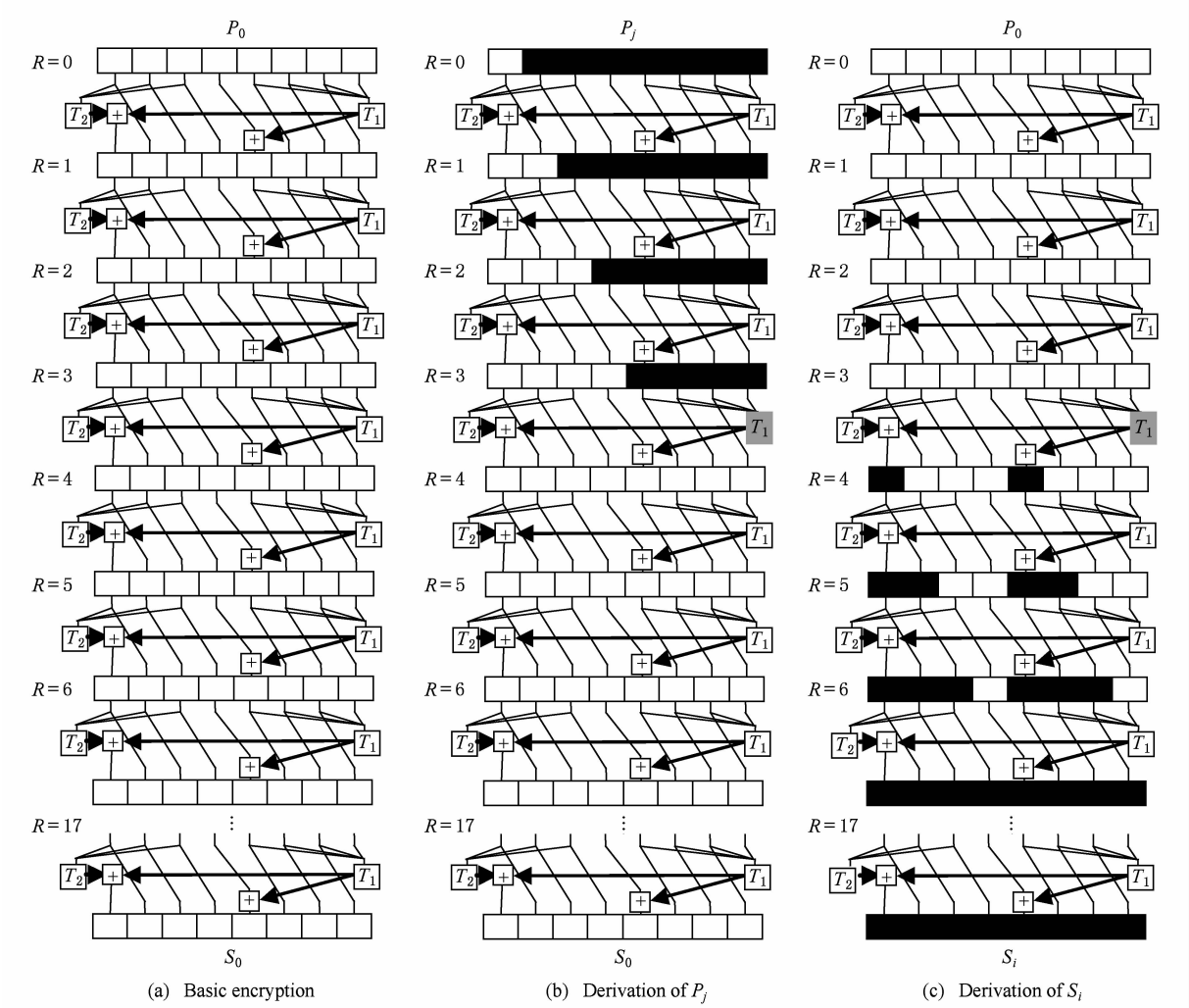

Fig. 2 Construction of Biclique.

图 2 Biclique 构造

根据 SHACAL2 的密钥生成策略可发现 2 条密钥差分不共享任何的活跃部分，即有 $P_j \xrightarrow{K[i,j]} S_i(i,j\in\{0,1\}^{32})$成立.

至此，完成对密钥分组，得到相应的 18 轮 32 维 Biclique.

3.3 中间相遇匹配

本文选择 $v=S_3^{26}$ 即 26 轮输出的第 4 个 32 b 分组作为中间匹配位置. 匹配位置选择的原则是计算复杂度优于穷举攻击，且使得需要计算的活跃部分最少. 接下来即可从 2 个方向计算匹配变量的值，同时删除不满足匹配的错误密钥.

固定 S_i，用密钥 $K[i,j](0<j<2^{32})$部分加密 S_i，得到 $v=S_3^{26}$. 如图 3(a)所示. 在计算匹配位 v 时，灰色部分表示不存在差分，仅需计算 1 次；白色部分表示不受影响可不计算；黑色部分表示受 $K[i,j]$与 $K[i,0]$之间的密钥差分影响，需要重新计算.

为了衡量计算量，选择需要计算的中间状态分组的数目为标准. 即在前向计算中对单个 S_i 可通过计算 20 个状态分组(灰色)、31 个状态分组(黑色)得到匹配变量的值. 同理，在后向计算过程中首先对

$P_j(0<j<2^{32})$加密得到相应的 2^{32} 个密文 C_j. 用密钥 $K[i,j](0<i<2^{32})$对 C_j 部分解密得到 $v=S_3^{26}$, 如图 3(b)所示,在后向计算中,对单个 C_j,可通过计算 18 个状态分组(灰色),$38\times8-18-23=263$ 个状态分组(黑色)得到匹配变量的值.

检验是否有 $\tilde{v}=\dot{v}$,若满足,继续检验,否则删除错误密钥. 穷举检验剩余的密钥候选值直到得到唯一的正确密钥值.

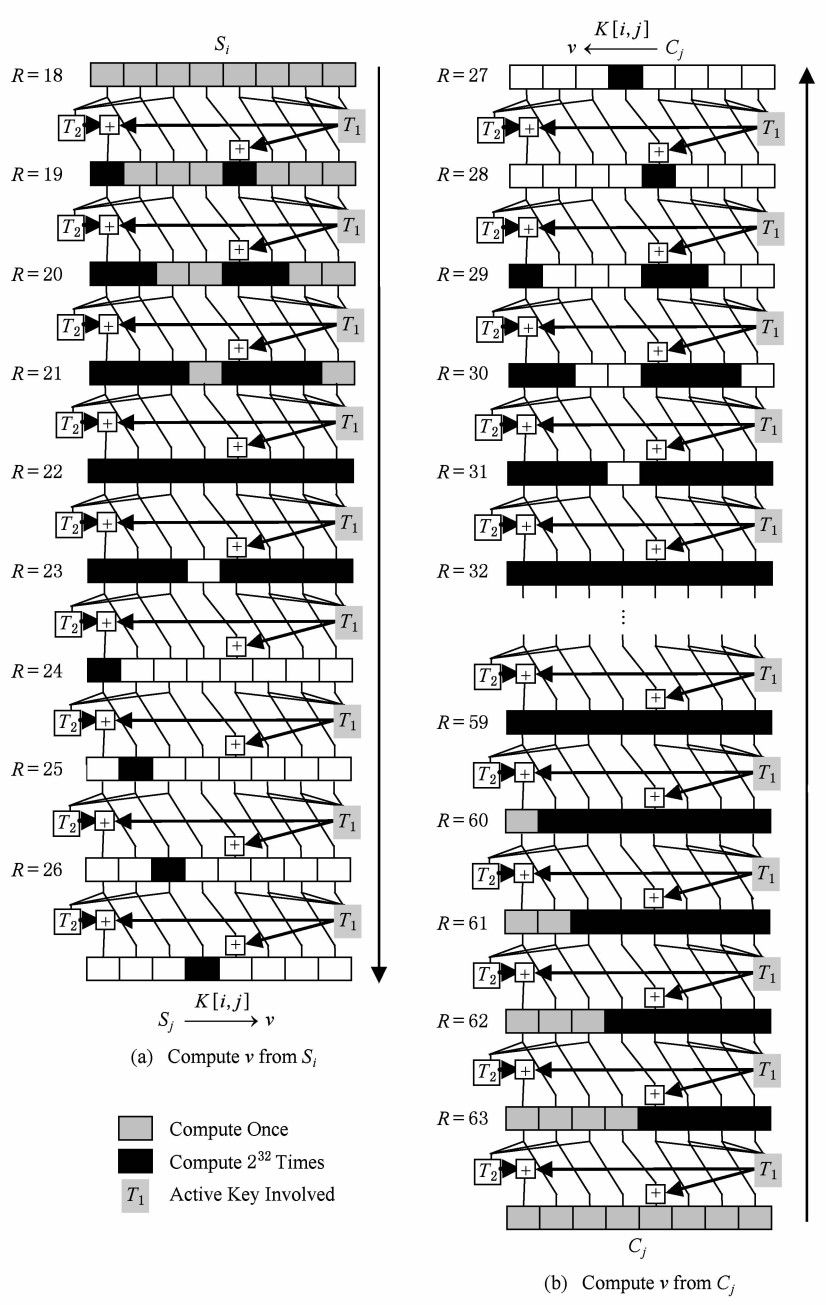

Fig. 3 Partial matches in the middle.

图 3 中间相遇部分匹配

3.4 复杂度分析

数据复杂度由需要进行加密的明文量决定,如图 2 所示,对每个 Biclique 令 $P=0_{(156)}$,则所有的明文在第 1 个 32 b 分组 P_0 处值相同,其他分组处取遍所有值,故数据复杂度不超过 2^{224}.

计算复杂度包括建立 Biclique 与中间相遇匹配 2 部分. 首先基础运算需要计算的 32 b 分组数量为 144 个,为了得到 $P_j(0<j<2^{32})$,需要计算 22 个 32 b 分组 2^{32} 次,为了得到 $S_i(0<i<2^{32})$,需要计算 108 个 32 b 分组 2^{32} 次. 所以建立 Biclique 的计算复

杂度为

$$(144+2^{32}\times(22+108))\div(37\times8)\approx2^{30.81}.$$

在中间相遇部分匹配阶段,对每个 Biclique 从 2 个方向计算中间匹配变量的值.其中,前向计算需要计算 $2^{32}(31\times2^{32}+20)$ 个 32 b 分组,后向计算需要计算 $2^{32}(263\times2^{32}+18)$ 个 32 b 分组.即共需要计算 $2^{32}(294\times2^{32}+38)$ 个 32 b 分组,这相当于 $(2^{32}(294\times2^{32}+38))\div(65\times8)\approx2^{63.17}$ 次 64 轮 SHACAL2 加密.已知共有 2^{448} 个 Biclique,所以总的计算复杂度为

$$TC=2^{448}(2^{30.81}+2^{63.17})\approx2^{511.18}.$$

与差分密码分析、线性密码分析等传统攻击方法相比较,Biclique 攻击最大的优点是可获得全轮算法的安全性分析结果,这是多数传统攻击方法无法做到的.

4 结 论

目前对算法 SHACAL2 安全性分析的最好结果是对 44 轮 SHACAL2 的相关密钥攻击,其数据复杂度为 2^{233},计算复杂度为 $2^{497.2}$.本文针对 SHACAL2 算法的密钥扩展与其加密结构的特点,对全 64 轮的 SHACAL2 算法应用 Biclique 攻击.攻击的数据复杂度不超过 2^{224},计算复杂度约为 $2^{511.18}$.这是 Biclique 攻击在分组密码全轮安全性分析中的又一次应用,据本文作者所知,这是首次对 SHACAL2 算法的单密钥全轮攻击.

综合 Biclique 攻击在分组密码安全性分析中的应用可以发现,Biclique 攻击对分组密码算法的密钥扩展策略与扩散层的要求比较严格,但是只要能够基于密钥特点建立轮数较长的 Biclique 结构,即可按照第 2 节中介绍的 Biclique 攻击步骤得到全轮密码算法的安全性分析结果,这使得 Biclique 攻击在分组密码安全性中的应用具有一定的可推广性.此外,观察 Biclique 攻击过程可以发现,计算复杂度的少量增加能够换取数据复杂度的较大改善,所以,接下来的研究内容将对分组密码安全性分析中 Biclique 攻击应用进行改进,改进方向为扩宽其应用范围与减小其接近穷举攻击的计算复杂度.

参 考 文 献

[1] Matsui M. New block encryption algorithm MISTY [G] //LNCS 1267: Proc of the 4th Int Workshop on Fast Software Encryption 1997. Berlin: Springer, 1997: 54-68

[2] Aoki K, Ichikawa T, Kanda M, et al. Camellia: A 128-bit block cipher suitable for multiple platforms—design and analysis [G] //LNCS 2012: Proc of the 3rd Int Symp on Theoretical Aspects of Computer Software. Berlin: Springer, 2001: 39-56

[3] Handschuh H, Naccache D. SHACAL: A family of block ciphers [EB/OL]. 2001[2013-11-25]. http://www.crypto

[4] nessie. orgBurrows J H. Secure hash standard [R/OL]. Washington D C: Department of Commerce, 1995[2013-11-25]. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA406543

[5] Shin Y, Kim J, Kim G, et al. Differential-linear type attacks on reduced rounds of SHACAL-2 [G] //LNCS 3108: Proc of Information Security and Privacy 2004. Berlin: Springer, 2004: 110-122

[6] Hong S, Kim J, Kim G, et al. Impossible differential attack on 30-round SHACAL-2 [G] //LNCS 2904: Proc of Progress in Cryptology (INDOCRYPT 2003). Berlin: Springer, 2003: 97-106

[7] Kim J, Kim G, Lee S, et al. Related-key attacks on reduced rounds of SHACAL-2 [G] //LNCS 3348: Proc of Progress in Cryptology (INDOCRYPT 2005). Berlin: Springer, 2005: 175-190

[8] Lu J, Kim J, Keller N, et al. Related-key rectangle attack on 42-round SHACAL-2 [G] //LNCS 4176: Proc of Information Security 2006. Berlin: Springer, 2006: 85-100

[9] Wei Yongzhuang, Hu Yupu. New related-key rectangle attack on 42-round SHACAL-2 [J]. Journal on Communications, 2009, 30(1): 7-11 (in Chinese)
(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)

[10] Jiqiang L, Jongsung K. Attacking 44 rounds of the SHACAL-2 block cipher using related-key rectangle cryptanalysis [J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 2008, 91(9): 2588-2596

[11] Khovratovich D, Rechberger C, Savelieva A. Biclique for preimages: Attacks on Skein-512 and the SHA-2 family [G] //LNCS 7549: Proc of Fast Software Encryption 2012. Berlin: Springer, 2012: 244-263

[12] Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES [G] //LNCS 7073: Proc of Advances in Cryptology (ASIACRYPT 2011). Berlin: Springer, 2011: 344-371

[13] Mala H. Biclique cryptanalysis of the block cipher SQUARE [EB/OL]. 2011[2013-11-25]. https://eprint.iacr.org/2011/500.pdf

[14] Hong D, Koo B, Kwon D. Biclique attack on the full HIGHT [G] //LNCS 7529: Proc of Information Security and Cryptology (ICISC 2012). Berlin: Springer, 2012: 365-374

[15] Chen S, Xu T. Biclique attack of the full ARIA-256 [EB/OL]. 2012[2013-11-25]. https://eprint.iacr.org/2012/011.pdf

[16] Çoban M, Karakoç F, Boztaş Ö. Biclique cryptanalysis of TWINE[G]//LNCS 7712: Proc of Cryptology and Network Security 2012. Berlin: Springe, 2012: 43-55

[17] Wang Yanfeng, Wu Wenling, Yu Xiaoli. Biclique cryptanalysis of reduced-round Piccolo block cipher [G] // LNCS 7232: Proc of SPEC 2012. Berlin: Springer, 2012: 337-352

Zheng Yafei, born in 1988. Master candidate. Her main research interests include cryptanalysis of block ciphers.

Wei Hongru, born in 1963. Associate professor. His main research interests include mathematics, information security and cryptography and key technologies of Internet of things.

2015 年起《计算机研究与发展》双月将固定领域专题

致广大读者和作者:

本刊从 2015 年起将双数期 1/2 版面固定为某个领域,每年将策划该领域的一个热点主题进行集中报道.具体的征文通知将在专题发表前 6 个月发布,请关注期刊网站!

具体领域分布及执行领域编委如下:

刊期	领域	领域编委	投稿方式	截稿日期
2 期	软件技术(含数据库)	孟小峰 xfmeng@ruc.edu.cn 中国人民大学	期刊网站投稿, 备注填写“年+专题名称”	上一年 10 月 1 日左右 (以具体征文通知为准)
4 期	网络技术	林闯 chlin@tsinghua.edu.cn 清华大学	期刊网站投稿, 备注填写“年+专题名称”	上一年 12 月 1 日左右 (以具体征文通知为准)
6 期	体系结构	刘志勇 zyliu@ict.ac.cn 中国科学院计算技术研究所	期刊网站投稿, 备注填写“年+专题名称”	当年 2 月 1 日左右 (以具体征文通知为准)
8 期	人工智能	周志华 zhouzh@nju.edu.cn 南京大学	期刊网站投稿, 备注填写“年+专题名称”	当年 4 月 1 日左右 (以具体征文通知为准)
10 期	信息安全	曹珍富 zfcao@sjtu.edu.cn 上海交通大学	期刊网站投稿, 备注填写“年+专题名称”	当年 6 月 1 日左右 (以具体征文通知为准)
12 期	应用技术	郑庆华 qhzheng@mail.xjtu.edu.cn 西安交通大学	期刊网站投稿, 备注填写“年+专题名称”	当年 8 月 1 日左右 (以具体征文通知为准)

此外,本刊依然欢迎自由来稿.谢谢!