Cobra-H64/128 算法的相关密钥-差分攻击

罗 伟,郭建胜
(解放军信息工程大学,河南郑州 450004)

摘 要: 本文研究了 Cobra-H64/128 分组密码算法在相关密钥-差分攻击下的安全性.针对 Cobra-H64 算法,利用新构造的相关密钥-差分路径和 CP 逆变换存在的信息泄露规律给出攻击算法 1,恢复出了全部 128bit 密钥,相应的计算复杂度为 2^40.5 次 Cobra-H64 算法加密,数据复杂度为 2^40.5 个选择明文,存储复杂度为 2^22bit,成功率约为 1;针对 Cobra-H128 算法,利用新构造的相关密钥-差分路径给出攻击算法 2,恢复出了全部 256bit 密钥,相应的计算复杂度为 2^76 次 Cobra-H128 算法加密,数据复杂度为 2^76 个选择明文,存储复杂度为 2^16.2bit.分析结果表明,Cobra-H64/128 算法在相关密钥-差分攻击条件下是不安全的.

关键词: 密码分析; Cobra-H64/128 算法; 相关密钥-差分攻击; 差分传递特性; 比特传递特性
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2013) 08-1569-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.08.018

Related-Key Differential Attacks on Cobra-H64/128

LUO Wei, GUO Jian-sheng
(*The PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: The security of Cobra-H64/128 block cipher under related-key differential cryptanalysis was studied. For Cobra-H64, we use related-key differential attack to get the whole 128 bits key with probability 1 based on the new constructed related-key differential and loopholes in CP box, and the corresponding computational complexity is 2^40.5 Cobra-H64 encryptions, the data complexity is 2^40.5 chosen-plaintexts, the memory complexity is 2^22 bits. To recover the whole 256 bits key of Cobra-H128, we need a computational complexity of 2^76 Cobra-H128 encryptions, a data complexity of 2^76 chosen-plaintexts, a memory complexity of 2^16.2 bits. The analysis results show that Cobra-H64/128 are unsafe under related-key differential attacks.

Key words: cryptanalysis; Cobra-H64/128 block cipher; related-key differential attack; differential transmission characteristic; bit transmission property

1 引言

物联网[1]相关技术的不断发展对密码算法的实现功耗和运行效率提出了新的要求,低功耗、高效率的密码算法设计与分析逐步成为研究热点.N A Moldovyan 等人[2]于 2005 年提出了 Cobra-H64/128 分组密码算法,算法利用 CP 盒[3]实现了数据的并行运算,选用简单的子密钥生成算法确保算法能够快速低耗运行,设计者声称该算法能够抵抗所有已知攻击.

相关密钥类型的复合攻击对选用简单子密钥生成算法的密码算法更具威胁[4,5].作为一种典型的相关密钥类型的复合攻击,相关密钥-差分攻击通过构造有效的相关密钥-差分实现对算法的攻击.近年来,各国学者利用相关密钥-差分攻击相继对 AES[6], LBlock[7] 以及 MD-64[8]等算法的安全性进行分析,得到了有效的攻击结果.

针对 Cobra-H64/128 算法,C Lee 等人[9]利用高概率相关密钥-差分路径对算法的安全性进行分析,分别恢复出了 Cobra-H64/128 算法的 23 和 63 比特密钥,这也是之前针对该算法最好的攻击结果.

本文分析研究了 Cobra-H64/128 算法的相关密钥-差分性质,利用新构造的相关密钥-差分路径和轮函数的比特传递特性分别给出攻击算法,恢复出了 Cobra-H64/128 算法的全部密钥.分析结果表明,Cobra-H64/128 算法在相关密钥-差分攻击条件下是不安全的.

2 算法介绍

Cobra-H64/128 算法分组长度分别为 64 和 128 比特,密钥长度分别为 128 和 256 比特,迭代轮数分别为 10 和 12 轮.算法采用类 Feistel 结构,其整体结构如图 1

收稿日期:2012-11-02;修回日期:2013-03-18;责任编辑:马兰英

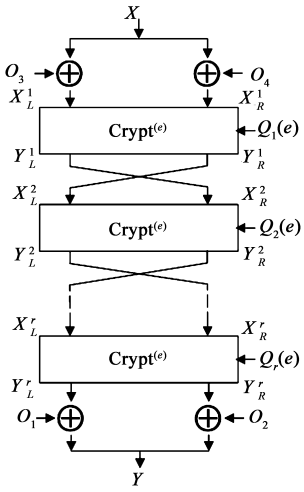


图1 Cobra-H64/128算法结构

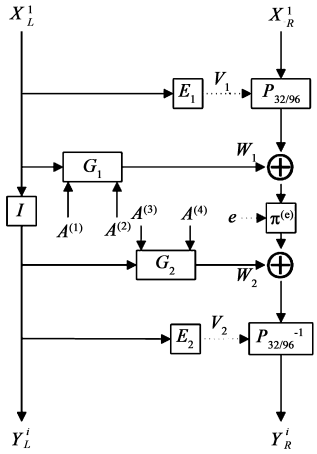


图2 Cobra-H64轮函数结构

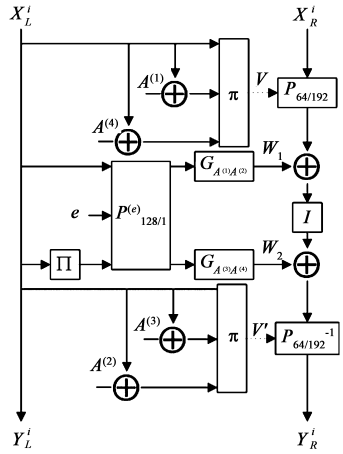


图3 Cobra-H128轮函数结构

所示，$e=0$ 时为加密算法，$e=1$ 时为解密算法.图 2 和图 3 分别给出了 Cobra-H64/128 算法的轮函数结构.

如图 1，Cobra-H64/128 算法利用密钥块 O_3，O_4 和 O_1，O_2 分别对数据进行入口白化和出口白化，前 $r-1$ 轮 Crypt$^{(e)}$变换后将输出数据块进行左右互换作为下一轮输入，最后一轮变换后不进行左右互换.

关于算法轮函数 Crypt$^{(e)}$各变换环节的详细信息以及子密钥生成算法详见参考文献[2].

本文符号约定如下：

$e_i/e_{i_1,i_2}/e_{i_1,i_2,i_3}$：表示二元序列在角标位置存在差分.

$P_{n/m}$：输入输出为 n 比特，控制序列为 m 比特的 CP 变换，$P_{n/m}^{-1}$为其逆变换.

$X/Y/X^i/Y^i$：分别表示明文，密文，算法第 i 轮输入，算法第 i 轮输出，加角标 $L(R)$时表示数据块左(右)半部分.

p_i，q_i：表示概率值.

$O_j^i/G^i/V^i/X(i)$：分别表示 O_j，G，V，X 的第 i 比特.

本文将差分路径通过的 $P_{2/1}$对应的控制比特称为差分传递线路.

3 轮函数相关密钥-差分特性分析

文献[9]在算法最后一轮构造 1 比特输出差分，利用差分在 CP 逆变换中的传递线路得到控制比特，结合密文恢复出相应的密钥比特.针对 Cobra-H64/128 算法，本文将 1 比特输出差分分别提升至第 9 和第 11 轮，构造更为有效的相关密钥-差分路径.

以下分析 Cobra-H64 算法中 $\Delta Y^9=(0,e_j)$时，第 10 轮各变换环节的相关密钥-差分特性.

引理 1 $\Delta X^{10}=(e_j,0)$时，G_1 输出差分 $\Delta W_1=e_j$ 的概率为

$$p_1=\begin{cases}2^{-3},1\leqslant j\leqslant 29\\ 2^{j-32},\text{others}\end{cases}$$

证明 输入差分为 e_j 时，G_1 输出差分如下

$$\begin{cases}\Delta W_1(j)=1\\ \Delta W_1(j+1)=l_{j-1}\oplus l_{j-2}\oplus l_{j-1}a_{j+1}''\\ \Delta W_1(j+2)=l_{j+1}\oplus l_{j-1}\oplus a_{j+1}''\oplus l_{j+1}a_{j+2}''\\ \Delta W_1(j+3)=l_{j+2}\oplus a_{j+2}'\end{cases}$$

其中 a_i'，a_i''分别表示 G_1 密钥输入 $A^{(1)}$，$A^{(2)}$的第 i 比特，l_i 表示 G_1 数据输入的第 i 比特.$\Delta W_1(i)=1$ 的概率为 $2^{-1}(i=j+1,j+2,j+3)$，从而 $\Delta W_1=e_j$ 的概率为

$$p_1=\begin{cases}2^{-3},1\leqslant j\leqslant 29\\ 2^{j-32},\text{others}\end{cases}$$

根据引理 1，G_2 输出差分 $\Delta W_2=e_{I(j)}$的概率为

$$p_2=\begin{cases}2^{-3},1\leqslant I(j)\leqslant 29\\ 2^{I(j)-32},\text{others}\end{cases}$$

定理 1 当 $j\leqslant 29$，$I(j)\leqslant 29$ 时，$(e_j,0)\rightarrow(e_{I(j)},e_{s,t})$的差分传播概率为 $2^{-21.6}$.

证明 $\Delta X^{10}=(e_j,0)$时，E_1，E_2 分别输出三比特差分.输入相等时，$P_{2/1}$输出不受控制比特影响，因此 $P_{32/96}$，$P_{32/96}^{-1}$输出差分与 E_1，E_2 输出差分无关的概率均为 $p_3=2^{-3}$.又密钥差分对 G_1，G_2 输出差分无影响的概率为 $10/16$[9]，结合引理 1，第 10 轮 $P_{32/96}^{-1}$输入差分为 $e_{I(j),\pi(j)}$的概率为 $10/16\times p_1p_2p_3$.因此对于固定的 s，t，$(e_j,0)\rightarrow(e_{I(j)},e_{s,t})$的差分传播概率为 $10/16\times p_1p_2p_3^2/C_{32}^2=2^{-21.6}$.

利用定理 1，本文构造出如表 1 左半部分所示的相关密钥-差分路径.

针对 Cobra-H128 算法，利用类似的方法，构造出如表 1 右半部分所示的相关密钥-差分路径.表 1 中两条相关密钥-差分路径的差分特征概率分别为 $2^{-33.5}$和 $2^{-71.0}$.

表 1　相关密钥-差分路径

	Cobra-H64 的相关密钥-差分路径				Cobra-H128 的相关密钥-差分路径		
轮数	ΔX^i	ΔKI^i	概率 q_i	轮数	ΔX^i	ΔKI^i	概率 q_i
白化	(e_{32}, e_{32})	(e_{32}, e_{32})	1	白化	(e_{64}, e_{64})	(e_{64}, e_{64})	1
1	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	1	(0,0)	$(0,0, e_{64}, e_{64})$	2^{-3}
2	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	2	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-3}
3	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	3	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-3}
4	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	4	(0,0)	$(0,0, e_{64}, e_{64})$	2^{-3}
5	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	5	(0,0)	$(0,0, e_{64}, e_{64})$	2^{-3}
6	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	6	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-3}
7	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	7	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-3}
8	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	10/16	8	(0,0)	$(0,0, e_{64}, e_{64})$	2^{-3}
9	(0,0)	$(e_{32}, e_{32}, e_{32}, e_{32})$	$(3/8)2^{-5}$	9	(0,0)	$(0,0, e_{64}, e_{64})$	2^{-3}
10	$(e_j, 0)$	$(e_{32}, e_{32}, e_{32}, e_{32})$	$2^{-21.6}$	10	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-3}
白化	$(e_{I(j)}, e_{s,t})$	(e_{32}, e_{32})	1	11	(0,0)	$(e_{64}, e_{64}, 0, 0)$	2^{-9}
输出	$(e_{I(j),32}, e_{s,t,32})$			12	$(e_j, 0)$	$(0,0, e_{64}, e_{64})$	$2^{-32.0}$
				白化	$(e_j, e_{s,t})$	(0,0)	1
注:若 $t=32$,则输出差分为$(e_{I(j),32}, e_s)$.				输出	$(e_j, e_{s,t})$		

4　Cobra-H64/128 算法的相关密钥-差分攻击

根据表 1,最后一轮 CP 逆变换存在两比特输入差分分别为 $e_{\pi^{(0)}(j),I(j)}$, $e_{\Pi(j),I(j)}$,以下分析 $P_{32/96}^{-1}$, $P_{64/192}^{-1}$的两比特差分传递特性.

4.1　CP 逆变换两比特差分传递特性分析

针对 $P_{32/96}^{-1}$,1 比特差分路径 $e_i \rightarrow e_j$ 存在两种差分传递线路,因此 $e_{\pi^{(0)}(j),I(j)} \rightarrow e_{s,t}$存在 $A_2^2 \times 2^2 = 8$ 种差分传递线路,差分通过每种线路的概率均为 2^{-3}.将利用差分传递线路得到的控制比特与对应密文比特求和即可得到出口白化所用的密钥比特.表 2 给出了利用 $e_{3,20} \rightarrow e_{4,19}$的不同线路恢复出的密钥链.

表 2　线路与恢复出的密钥链

线路编号	恢复出的密钥链(O_1 比特位)
1	14,7,1,29,23,18;6,15,10,22,31,26
2	14,7,1,29,23,18;6,1,12,24,17,26
3	14,9,3,31,25,18;6,15,10,22,31,26
4	14,9,3,31,25,18;6,1,12,24,17,26
5	14,7,2,21,31,26;6,15,9,30,23,18
6	14,7,2,21,31,26;6,1,11,32,25,18
7	14,9,4,23,17,26;6,15,9,30,23,18
8	14,9,4,23,17,26;6,1,11,32,25,18

由表 2,利用 $e_{3,20} \rightarrow e_{4,19}$能够恢复出 ${O_1}^1 \sim {O_1}^4$, ${O_1}^6 \sim {O_1}^7$, ${O_1}^9 \sim {O_1}^{12}$, ${O_1}^{14} \sim {O_1}^{15}$, ${O_1}^{17} \sim {O_1}^{18}$, ${O_1}^{21} \sim {O_1}^{26}$, ${O_1}^{29} \sim {O_1}^{32}$共 24 比特密钥,记为 K_1.同理,利用 $e_{10,28} \rightarrow e_{26,29}$恢复出 ${O_1}^1$, ${O_1}^3$, ${O_1}^5 \sim {O_1}^6$, ${O_1}^8$, ${O_1}^{10} \sim {O_1}^{16}$, ${O_1}^{19} \sim {O_1}^{22}$, ${O_1}^{25} \sim {O_1}^{29}$, ${O_1}^{31}$共 22 比特密钥,记为 K_2. $K_1 \cup K_2$ 即为 O_1.

对于 $P_{64/192}^{-1}$,由于 1 比特差分路径 $e_i \rightarrow e_j$ 仅有一种差分传递线路,因此两比特差分路径 $e_{\Pi(j),I(j)} \rightarrow e_{s,t}$存在 $A_2^2 \times 1^2 = 2$ 种差分传递线路,差分通过每种线路的概率均为 2^{-1}.与 $P_{32/96}^{-1}$类似,利用差分传递线路即可恢复出控制序列 V'.

4.2　Cobra-H64 算法的比特传递特性分析

针对 Cobra-H64 算法,根据第 9 轮 $P_{32/96}^{-1}$变换的 1 比特差分路径 $e_{32} \rightarrow e_j$ 恢复出相应的控制比特;由 1 比特数据在第 10 轮中的传递线路建立密钥方程,在选择密文条件下求解方程组恢复密钥比特.该攻击过程如图 4 所示,图 5 给出了相应的比特传递线路示意图.

定理 2　$P_{32/96}^{-1}$变换 1 比特差分传递线路首尾比特模 2 加和值由差分对完全决定.

证明　对于 $e_i \rightarrow e_j$,两条差分传递线路首尾比特取值分别相反,其和值由 i, j 决定.

对于 $e_{32} \rightarrow e_j$,当 j 为奇数时, $V_2^{16} \oplus V_2^{80+\lceil j/2 \rceil} = 1$;当 j 为偶数时, $V_2^{16} \oplus V_2^{80+\lceil j/2 \rceil} = 0$.

根据图 5 建立密钥方程如下:

$$X_R^{10}(i) \oplus G_1^{P_{V_1}(i)} \oplus G_2^{\pi(P_{V_1}(i))} = Y_R^{10}(P_{V_2^{-1}}(\pi^{(e)}(P_{V_1}(i))))$$

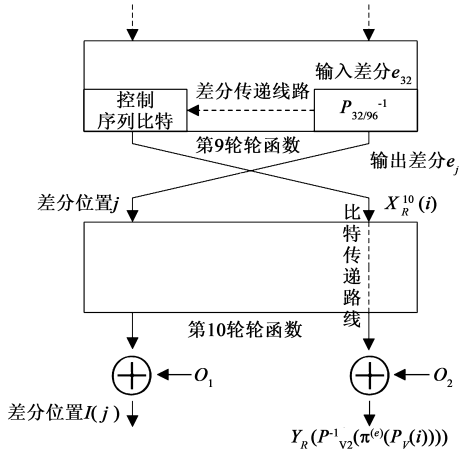


图4 基于比特传递特性的攻击示意图

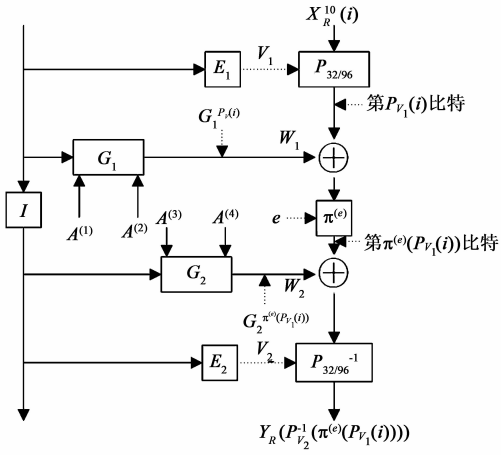


图5 比特传递线路示意图

其中 $P_{V_1}(i)$表示 $X_R^{10}(i)$经过 $P_{32/96}^{(V_1)}$变换后的输出位置.

对于每个满足 $\Delta Y=(e_{I(j),32},e_{s',t',32})$的密文对,将 $V_2^{16},V_2^{80+\lceil j/2\rceil}$ 在第 10 轮建立的密钥方程进行求和,求解求和密钥方程组即可恢复密钥.

4.3 Cobra-H64 的相关密钥-差分攻击

针对 Cobra-H64 算法,结合相关密钥-差分路径和比特传递特性,给出攻击算法 1.

攻击算法 1

Step1 选择 2^n 个明文对(X,X^*),其中 $X\oplus X^*=(e_{32},e_{32})$.

Step2 利用密钥 K,K^* 分别加密明文 X,X^*,得到密文对(Y,Y^*),其中 $K\oplus K^*=(e_{32},e_{32},e_{32},e_{32})$.

Step3 抛弃不满足 $\Delta Y=(e_{I(j),32},e_{s',t',32})$的密文对.

Step4 对于满足 $\Delta Y=(e_{3,32},e_{4,19,32})$,$\Delta Y=(e_{28,32},e_{26,29,32})$的密文对,分别利用线路 i 求解相应的密钥链存入集合 $T_i,i=1,2,\cdots,8$.

Step5 对集合 T_i 中的密钥链进行计数,将计数最多的密钥链作为正确密钥链,整理得到密钥 O_1.

Step6 对 **Step3** 剩余的密文对利用 $V_2^{16}\oplus V_2^{80+\lceil j/2\rceil}$ 建立求和密钥方程.

Step7 通过筛选系数将求和密钥方程简化为关于 O_2,O_3 的一次方程,求解方程组得到 O_2,O_3.

Step8 将 O_2,O_3 代入 **Step6** 建立的求和密钥方程,求解 O_4.

定理 3 $n=39.5$ 时,攻击算法 1 所需的计算复杂度约为 $2^{40.5}$次 10 轮 Cobra-H64 加密,数据复杂度约为 $2^{40.5}$个选择明文,存储复杂度约为 $2^{14.8}$比特,成功率约为 1.

证明 $n=39.5$ 时,**Step3** 和 **Step4** 分别剩余 $2^{39.5}\times 2^{-33.5}\times C_{32}^2\approx 2^{15}$和 $2^{39.5}\times 2^{-33.5}\times 2=2^7$ 个密文对. **Step4** 中正确密钥链在 T_i 中计数期望次数为 $2^6\times 2^{-3}=8$,而错误密钥链的计数期望次数为 $2^6\times 2^{-12}=2^{-6}$,因此 **Step5** 以计数最多的密钥链作为正确密钥链是合理的. **Step6** 利用满足 $\Delta Y=(e_{I(j),32},e_{s',t',32})$的密文对建立 2^{15} 个求和密钥方程,通过 **Step7** 系数筛选剩余 2^9 个方程. **Step7** 中 64(O_2,O_3 共 64 比特密钥)元 1 次方程组系数矩阵满秩的概率为 $p_0=\prod_{i=2^9-64+1}^{2^9}(1-\frac{1}{2^i})$[10],满秩时导出组只有 0 解,方程组有唯一解[11]. 从而 **Step7** 方程组有唯一解的概率为 $p_0\approx 1$. 同理,**Step8** 方程组存在唯一解的概率约为 1. **Step6** ~ **Step8** 恢复出 O_2,O_3,O_4 的成功率约为 1.

由于 **Step4** 求解密钥链的复杂度和 **Step7**,**Step8** 求解方程组的复杂度远小于 **Step2** 加密明文对的复杂度,因此攻击算法 1 的计算复杂度约为 $2^{40.5}$次 Cobra-H64 算法加密,相应的数据复杂度为 $2^{40.5}$个选择明文. 存储密文对和密钥链共需要约 $2^{15}\times 64\times 2+2^7\times 12\times 8\approx 2^{22}$比特.

4.4 Cobra-H128 的相关密钥-差分攻击

针对 Cobra-H128 算法,利用表 1 右半部分的相关密钥-差分路径给出攻击算法 2.

攻击算法 2

对 $j\in M$,$M=\{2,3,6,7,10,11,13,15,29,34,35,38,39,43,47,49,62\}$执行以下步骤:

Step1 选择 2^n 个明文对(X,X^*),其中 $X\oplus X^*=(e_{64},e_{64})$.

Step2 利用密钥 K,K^* 分别加密明文 X,X^*,得到密文对(Y,Y^*),其中 $K\oplus K^*=(0,0,e_{64},e_{64})$.

Step3 抛弃不满足 $Y\oplus Y^*=(e_j,e_{s,t})$的密文对,对剩余的密文对分别利用线路 i 求解相应的数据链存入集合 $T_i^j,i=1,2$.

Step4 对集合 T_i^j 中的数据链进行计数,输出计数最多的数据链,整理得到 D_j.

整理得 $V'=\bigcup_{j\in M}D_j$.

算法分析:

取 $n=75$,正确数据链的计数期望次数为 $2^{75}\times$

$2^{-71.0}\times 2^{-1}=8$,随机数据链的计算期望次数为 $2^{75}\times 2^{-71.0}\times 2^{-12}=2^{-8}$. 利用攻击算法 2 恢复出第 12 轮 $P_{64/192}^{-1}$控制序列 V' 全部 192 比特,即得到了 X_L^{12}, $X_L^{12}\oplus O_3$, $X_L^{12}\oplus O_2$. 利用 $O_1\oplus X_L^{12}=Y_L$ 求解 O_1,进而得到 O_2, O_3;在此基础上,穷尽搜索 64 比特密钥块 O_4,即可完全恢复出 Cobra-H128 算法全部 256 比特密钥,相应的数据复杂度为 2^{76}个选择明文,计算复杂度为 2^{76}次 Cobra-H128 算法加密,存储密文对和数据链共需要约 $2^{75}\times 2^{-71.0}\times 128\times 2\times 17+2^{75}\times 2^{-71.0}\times 12\times 2\times 17\approx 2^{16.2}$比特.

5　结束语

本文对 Cobra-H64/128 算法的安全性进行评估,首次恢复出了算法的全部密钥. 攻击结果表明, Cobra-H64/128 算法在相关密钥-差分条件下是不安全的,类 Feistel 结构和 DDP(Data-Dependent Permutations)结构的结合,使得敌手能够根据 DDP 结构中的差分传递线路恢复出左半部分数据,造成信息泄漏. 与此同时,算法设计者选用简单的子密钥生成算法,容易遭受相关密钥攻击. 因此,利用 DDP 结构设计密码算法时应当充分考虑 DDP 结构与数据块的结合方式,消除 DDP 结构在差分分析下存在的信息泄漏规律,同时避免使用简单的子密钥生成算法.

参考文献

[1] 钱志鸿,王义君. 物联网技术与应用研究[J]. 电子学报, 2012,40(5):1023 – 1029.
Qian Zhi-hong, Wang Yi-jun. IoT technology and application [J]. Acta Electronica Sinica, 2012, 40(5): 1023 – 1029. (in Chinese)

[2] N Sklavos, et al. High speed networking security: design and implementation of two new DDP-based ciphers [J]. Mobile Networks and Applications, 2005, 10: 219 – 231.

[3] A A Moldovyan, N A Moldovyan. A cipher based on data dependent permutations[J]. Journal of Cryptology, 2002, 15(1): 61 – 72.

[4] Ding Lin, Guan Jie. Related-key chosen IV attack on K2* [J]. Chinese Journal of Electronics, 2011, 20(2): 365 – 369.

[5] Changhoon Lee, et al. Security analysis of pure DDP-based cipher proper for multimedia and ubiquitous device[J]. Telecommunication System, 2010, (44): 267 – 279.

[6] Jiali Choy, et al. AES variants secure against related-key differential and boomerang attacks[J]. Lecture Notes in Computer Science, 2011, 6633: 191 – 207.

[7] Liu Shu-sheng, et al. Improved related-key differential attacks on reduced-round LBlock[J]. Information and Communications Security, 2012, 7618/2012: 58 – 69.

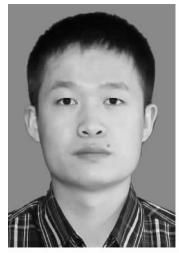
[8] Jinkeon Kang. Related-key attack on the MD-64 block cipher suitable for pervasive computing environments[A]. Advanced Information Networking and Applications Workshops (WAINA)[C]. IEEE Computer Society Washington, DC, USA, 2012. 726 – 731.

[9] Changhoon Lee, et al. Related-key differential attacks on Cobra-H64 and Cobra-H128[J]. Lecture Notes in Computer Science, 2005, 3796: 201 – 219.

[10] K C Zeng, et al. On the linear consistency test (LCT) in cryptanalysis and its applications[A]. CRYPTO'89[C]. LNCS, G. Brassard ed., Springer-Verlag, 1990. 435, 164 – 174.

[11] 王萼芳,石生明. 高等代数[M]. 北京:高等教育出版社, 2003:145 – 146.

作者简介



罗　伟　男,1987 年生,硕士研究生,研究方向为分组密码设计与分析.
E-mail: luowei.crypt@gmail.com

郭建胜(通信作者)　男,1972 年生,教授,硕士生导师,研究方向为密码学与信息安全.
E-mail: guojs_crypt@126.com