3D 密码的不可能差分攻击

唐学海[①] 李 超[①②] 王美一[①] 屈龙江[①]
[①](国防科技大学数学与系统科学系 长沙 410073)
[②](信息安全国家重点实验室 北京 100190)

摘 要：3D 密码是在 CANS2008 上提出的一个新的分组密码算法，与以往的分组密码算法不同，它采用了 3 维结构。密码设计者给出了 3D 密码的一个 5 轮不可能差分并对 6 轮 3D 密码进行了不可能差分攻击。该文通过 3D 密码的结构特性找到了新的 6 轮不可能差分。基于新的不可能差分和 3D 密码的等价结构，可以对 7 轮和 8 轮 3D 密码进行有效的不可能差分攻击。此外，结合其密钥扩展规则，可以将攻击轮数提高至 9 轮。该文的攻击结果优于密码设计者的结果。

关键词：分组密码；3D 密码；不可能差分攻击
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2010)10-2516-05
DOI: 10.3724/SP.J.1146.2009.01375

Impossible Differential Attack on 3D Cipher

Tang Xue-hai[①] Li Chao[①②] Wang Mei-yi[①] Qu Long-jiang[①]
[①](*Department of Mathematics and System Science*, *National University of Defense Technology*, *Changsha* 410073, *China*)
[②](*State Key Laboratory of Information Security*, *Beijing* 100190, *China*)

Abstract: 3D cipher is a new block cipher proposed in CANS2008. It is different from all known block cipher as it uses the three dimension structure. The designers give out a 5-round impossible differential and make an impossible differential attack on 6-round 3D cipher. In this paper, some new 6-round impossible differentials are found according to its structure properties. Based on these new impossible differentials and the equivalent structure of 3D cipher, effective impossible differential attacks can be made on 7 and 8-round 3D cipher. Moreover, according to some properties of the key schedule, these attacks can be extended to 9-round 3D cipher. These attack results are better than the designer's.

Key words: Block cipher; 3D cipher; Impossible differential attack

1 引言

3D 密码[1]是 CANS 2008 上提出的一个新的迭代分组密码算法，它的主要设计思想来源于 AES，采用了 SPN 型结构。AES 中数据被表示为 4×4 的 2 维字节矩阵，而 3D 密码的数据分组长度及密钥长度均为 512 bit，将数据表示为 $4\times4\times4$ 的字节矩阵，可形象地看成是一个 3 维立方体。密码设计者指出了 3D 密码由于具有 3 维结构特性，使得它在密码设计、安全性能和潜在的应用(哈希函数，MAC，流密码，伪随机数生成器)等方面都有很大的改进。目前对 3D 算法的安全性评估仅限于密码设计者在文献[1]中给出的相关密钥分析，截断差分分析，积分攻击及不可能差分分析等，其中效果最好的是不可能差分分析。

不可能差分分析最早由 Biham 等人[2]在用不可能差分分析方法分析 31 轮 Skipjack 算法时首次提出的，是目前分组密码分析中最有效的分析方法之一，如近年来对 AES 的分析[3,4]，对 Camellia 的分析[5,6]以及对 CLEFIA 的分析[7−9]等。它与经典差分密码分析利用高概率差分特征来恢复密钥相反，它是利用概率为 0 的差分(不可能差分)，其基本思想是排除那些导致概率为 0 的差分出现的候选密钥。文献[1]中给出了 3D 算法的一条 5 轮不可能差分，并对其进行了 6 轮的分析。本文根据 3D 算法的加密结构特性找到了新的 6 轮不可能差分，并据此对 3D 算法进行了 7–9 轮的攻击。

本文结构如下：第 2 节简要介绍 3D 密码的加密规则及密钥扩展规则；第 3 节给出 3D 密码新的 6 轮不可能差分区分器；第 4 节详细描述对 3D 密码 7–9 轮的不可能差分攻击；第 5 节是结论。

2009-10-26 收到，2010-03-15 改回
国家自然科学基金(60803156)和信息安全国家重点实验室开放基金(01-07)资助课题
通信作者：唐学海 txh0203@163.com

2　3D 密码简介

2.1 加密规则

3D 密码的数据分组长度及密钥长度均为 512 bit，把数据表示为 $4\times4\times4$ 的字节矩阵，可形象的看成是一个立方体。512 bit 的数据 $A=(a_0,a_1,\cdots,a_{63})$ 被表示为

$$\left(\begin{array}{cccc|cccc} a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} \\ a_1 & a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} \\ a_2 & a_6 & a_{10} & a_{14} & a_{18} & a_{22} & a_{26} & a_{30} \\ a_3 & a_7 & a_{11} & a_{15} & a_{19} & a_{23} & a_{27} & a_{31} \end{array}\right. \quad (1)$$
$$\left.\begin{array}{cccc|cccc} a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\ a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} \\ a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} \\ a_{35} & a_{39} & a_{43} & a_{47} & a_{51} & a_{55} & a_{59} & a_{63} \end{array}\right)$$

每一轮加密依次进行 4 种变换：

(1)轮密钥加($\boldsymbol{\kappa}_i$)：将 512 bit 的轮密钥 K_i 直接与数据按比特位异或；

(2)置换层($\boldsymbol{\gamma}$)：将数据每一字节作用于相同的 S 盒(与 AES 的 S 盒一样)；

(3)行移位($\boldsymbol{\theta}_1,\boldsymbol{\theta}_2$)：其中 $\boldsymbol{\theta}_1,\boldsymbol{\theta}_2$ 的定义如下：

$\boldsymbol{\theta}_1$ 对(1)中每一小块进行相同的行移位，把式(1)变换为

$$\left(\begin{array}{cccc|cccc} \boldsymbol{a}_0 & a_4 & a_8 & a_{12} & \boldsymbol{a}_{16} & a_{20} & a_{24} & a_{28} \\ a_5 & a_9 & a_{13} & \boldsymbol{a}_1 & a_{21} & a_{25} & a_{29} & \boldsymbol{a}_{17} \\ a_{10} & a_{14} & \boldsymbol{a}_2 & a_6 & a_{26} & a_{30} & \boldsymbol{a}_{18} & a_{22} \\ a_{15} & \boldsymbol{a}_3 & a_7 & a_{11} & a_{31} & \boldsymbol{a}_{19} & a_{23} & a_{27} \end{array}\right.$$
$$\left.\begin{array}{cccc|cccc} \boldsymbol{a}_{32} & a_{36} & a_{40} & a_{44} & \boldsymbol{a}_{48} & a_{52} & a_{56} & a_{60} \\ a_{37} & a_{41} & a_{45} & \boldsymbol{a}_{33} & a_{53} & a_{57} & a_{61} & \boldsymbol{a}_{49} \\ a_{42} & a_{46} & \boldsymbol{a}_{34} & a_{38} & a_{58} & a_{62} & \boldsymbol{a}_{50} & a_{54} \\ a_{47} & \boldsymbol{a}_{35} & a_{39} & a_{43} & a_{63} & \boldsymbol{a}_{51} & a_{55} & a_{59} \end{array}\right)$$

θ_2 对整个大矩阵进行行移位，把式(1)变换为

$$\left(\begin{array}{cccc|cccc} \boldsymbol{a}_0 & a_4 & a_8 & a_{12} & \boldsymbol{a}_{16} & a_{20} & a_{24} & a_{28} \\ \boldsymbol{a}_{17} & a_{21} & a_{25} & a_{29} & \boldsymbol{a}_{33} & a_{37} & a_{41} & a_{45} \\ \boldsymbol{a}_{34} & a_{38} & a_{42} & a_{46} & \boldsymbol{a}_{50} & a_{54} & a_{58} & a_{62} \\ \boldsymbol{a}_{51} & a_{55} & a_{59} & a_{63} & \boldsymbol{a}_3 & a_7 & a_{11} & a_{15} \end{array}\right.$$
$$\left.\begin{array}{cccc|cccc} \boldsymbol{a}_{32} & a_{36} & a_{40} & a_{44} & \boldsymbol{a}_{48} & a_{52} & a_{56} & a_{60} \\ \boldsymbol{a}_{49} & a_{53} & a_{57} & a_{61} & \boldsymbol{a}_1 & a_5 & a_9 & a_{13} \\ \boldsymbol{a}_2 & a_6 & a_{10} & a_{14} & \boldsymbol{a}_{18} & a_{22} & a_{26} & a_{30} \\ \boldsymbol{a}_{19} & a_{23} & a_{27} & a_{31} & \boldsymbol{a}_{35} & a_{39} & a_{43} & a_{47} \end{array}\right)$$

(4)列混合($\boldsymbol{\pi}$)：类似 AES 中的列混合，用一个固定的 4×4 矩阵 $\boldsymbol{M}$ 乘以数据的每一列，且这个矩阵满足 $\boldsymbol{M}=\boldsymbol{M}^{-1}$。

设 X 为第 i 轮的输入，则第 i 轮数据加密定义为 $\boldsymbol{\tau}_i(X)=\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(i \bmod 2)+1}\circ\boldsymbol{\gamma}\circ\boldsymbol{\kappa}_i(X)=\boldsymbol{\pi}(\boldsymbol{\theta}_{(i \bmod 2)+1}(\boldsymbol{\gamma}(\boldsymbol{\kappa}_i(\boldsymbol{X}))))$，$0\le i\le r-2$，注意最后一轮没有列混合 $\boldsymbol{\pi}$，以 $\boldsymbol{\kappa}_r$ 代替，即 $\boldsymbol{\eta}_{r-1}(X)=\boldsymbol{\kappa}_r\circ\boldsymbol{\theta}_{(r-1 \bmod 2)+1}\circ\boldsymbol{\gamma}\circ\boldsymbol{\kappa}_{r-1}(X)$。从而给定明文 P，经过 3D 算法加密后的密文为

$$\begin{aligned} C&=\boldsymbol{\kappa}_r\circ\boldsymbol{\eta}_{r-1}\circ\bigcirc_{i=0}^{r-2}\boldsymbol{\tau}_i(P)\\ &=\boldsymbol{\kappa}_r\circ\boldsymbol{\theta}_{(r-1 \bmod 2)+1}\circ\boldsymbol{\gamma}\circ\boldsymbol{\kappa}_{r-1}\\ &\quad\circ\bigcirc_{i=0}^{r-2}(\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(i \bmod 2)+1}\circ\boldsymbol{\gamma}\circ\boldsymbol{\kappa}_i)(P) \end{aligned} \quad (2)$$

易知式(2)等价于

$$\begin{aligned} C&=\boldsymbol{\kappa}_r\circ\boldsymbol{\theta}_{(r-1 \bmod 2)+1}\circ\gamma\\ &\quad\circ\bigcirc_{i=1}^{r-1}(\boldsymbol{\kappa}_i\circ\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(i \bmod 2)+1}\circ\boldsymbol{\gamma})\circ\kappa_0(P) \end{aligned} \quad (3)$$

记第 i 轮加密的轮函数为 $\boldsymbol{\tau}_i^{'}=\boldsymbol{\kappa}_i\circ\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(i \bmod 2)+1}\circ\boldsymbol{\gamma}$，$1\le i\le r-1$，第 1 轮之前有个白化密钥 $\boldsymbol{\kappa}_0$，最后一轮没有列混合，这与 AES 类似。下文的分析中均采用等价结构式(3)。

2.2 密钥扩展算法

设种子密钥 $K=(k_0,k_1,\cdots,k_{63})$，那么轮密钥 K_i 按下述方式得到：

$K_0=K$，$K_i=\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(i \bmod 2)+1}\circ\boldsymbol{\gamma}'\circ\boldsymbol{\kappa}^*(K_{i-1})$，$i\ge1$。其中 $\boldsymbol{\gamma}'$ 对数据的部分字节作 S 盒(与 AES 中的 S 盒相同)变换，$\boldsymbol{\kappa}^*$ 将一个固定的 512 bit 值与 K_{i-1} 异或。由此可知当知道任何一个轮密钥时就可以计算出种子密钥。

2.3 一些有用的性质

文献[1]中给出了 3D 密码加密函数的一些性质，现将下文将要用到的几条性质列出来：

(a) $\boldsymbol{\kappa}_i=\boldsymbol{\kappa}_i^{-1}$，这是因为异或运算是可逆运算；

(b) $\boldsymbol{\pi}=\boldsymbol{\pi}^{-1}$，这是因为 $\boldsymbol{M}=\boldsymbol{M}^{-1}$；

(c) $\boldsymbol{\kappa}_i(K_i)\circ\boldsymbol{\pi}=\boldsymbol{\pi}\circ\boldsymbol{\kappa}_i^{'}(K_i^{'})$，其中 $K_i^{'}=\boldsymbol{\pi}^{-1}(K_i)$。

3　3D 密码的 6 轮不可能差分区分器

文献[1]中给出了 3D 算法的一条 5 轮不可能差分区分器并对 3D 算法进行了 6 轮的不可能差分攻击。下面，我们利用 3D 算法的等价结构式(3)，从第 2 轮开始，考虑 6 轮加密，最后一轮不考虑列混合 π，可以得到3D算法的6轮不可能差分区分器(如图 1 所示)。其中 δ 表示此位置差分非零，“？”表示此位置的差分值未知。

此不可能差分由两段构成，前 3 轮差分按加密方向以概率 1 成立，后 3 轮差分按解密方向以概率 1 成立，它们在中间相遇处矛盾，从而构成 3D 算法的 6 轮不可能差分区分器。易知最前面的 δ 在任意位置时此不可能差分都成立，即第 2 轮的输入差分仅有 1 个字节位置不为零时，经过 6 轮的加密，输出差分不可能同时在(3，6，9，12，19，22，25，28，35，38，41，44，51，54，57，60)这 16 个位

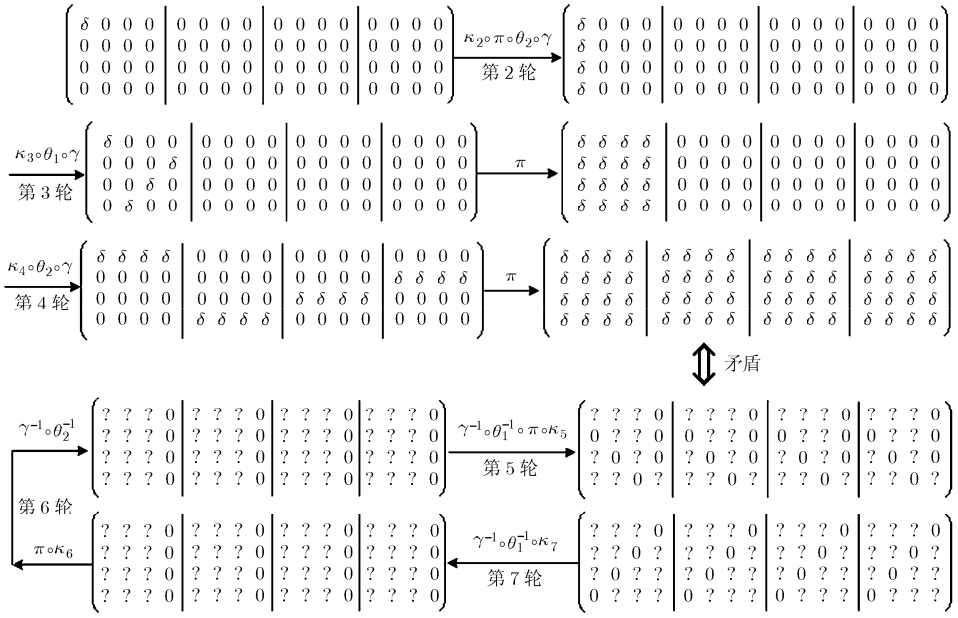

图 1 3D 密码的 6 轮不可能差分

置为 0。同理可以得到其它 3 条不可能差分，即第 2 轮的输入差分仅有一个字节位置不为零时，经过 6 轮的加密，输出差分不可能在(2，5，8，15，18，21，24，31，34，37，40，47，50，53，56，63)，(1，4，11，14，17，20，27，30，33，36，43，46，49，52，59，62)及(0，7，10，13，16，23，26，29，32，39，42，45，48，55，58，61)三者之一的 16 个位置同时为 0。

4 3D 密码的 7–9 轮不可能差分攻击

利用上节中的 6 轮不可能差分区分器，我们可以对 3D 算法进行 7/8/9 轮的不可能差分攻击。

4.1 3D 密码的 7 轮不可能差分攻击

对 3D 算法进行 7 轮不可能差分攻击的基本思想是：在算法的后 6 轮利用 6 轮不可能差分区分器，猜测 K_0 的部分字节进行一轮加密，利用 6 轮不可能差分淘汰错误密钥。注意第 1 轮的密钥 K_1 不需要猜测，因为我们可以将其放入 6 轮不可能差分区分器，这对 6 轮不可能差分没有影响(见图 2 的前 7 轮)。

攻击过程如下：

步骤 1　选择一组明文满足除第 0，5，10，15 个字节外，其余字节取值均相同，第 0，5，10，15 个字节取遍 2^{32} 种取值，故这样一组明文共 2^{32} 个，可以组成 $\binom{2^{32}}{2}\approx 2^{63}$ 对，取 m 组明文共有 $m\times 2^{32}$ 个明文，组成 $m\times 2^{63}$ 对。

步骤 2　对上述明文加密 7 轮，选取满足在(3，6，9，12，19，22，25，28，35，38，41，44，51，54，57，60)，(2，5，8，15，18，21，24，31，34，37，40，47，50，53，56，63)，(1，4，11，14，17，20，27，30，33，36，43，46，49，52，59，62)及(0，7，10，13，16，23，26，29，32，39，42，45，48，55，58，61)四者之一的 16 个字节全为 0 的密文对留下来，其余舍弃，共有 $m\times 2^{63}\times(2^{-8})^{16}\times 4=2^{-63}\times m$ 对留下。

步骤 3　任取步骤 2 留下的一个密文对相应的明文对，猜测密钥 K_0 的第 0，5，10，15 个字节的值，经过第 1 轮“部分加密”，若第 1 列 4 个字节有 3 个字节的差分值为 0(概率为 $(2^{-8})^3\times 4=2^{-22}$)，则由不可能差分知所猜密钥是错误的。分析完步骤 2 留下的所有对，剩下的错误密钥数大概为 $(2^{32}-1)(1-2^{-22})^{2^{-63}\times m}$，当 $m=2^{90}$ 时，$(2^{32}-1)(1-2^{-22})^{2^{-63}\times m}=2^{-14}$，这时可认为错误密钥被全部排除，留下的即为正确的密钥。

步骤 4　重复步骤 1–3，位置(0，5，10，15)换为别的 4 字节位置使得第 1 轮加密后的非零差分字节全部在某一列，如选取(3，4，9，14)，(16，21，26，31)等 15 个位置组合，就可恢复出 K_0 在这些位置的值，从而恢复出 K_0 的所有字节值，即为种子密钥。

复杂度计算：数据复杂度为 $2^{32}\times m\times 16=2^{126}$；步骤 3 总的“部分加密”次数为 $[2^{32}+2^{32}(1-2^{-22})+2^{32}(1-2^{-22})^2+\cdots+2^{32}(1-2^{-22})^{2^{-63}\times m}]\times 2\approx 2^{55}$，一次“部分加密”相当于 1/16 轮加密，故总的时间复杂度为 $16\times 2^{55}/(16\times 7)\approx 2^{52}$ 次 7 轮加密。

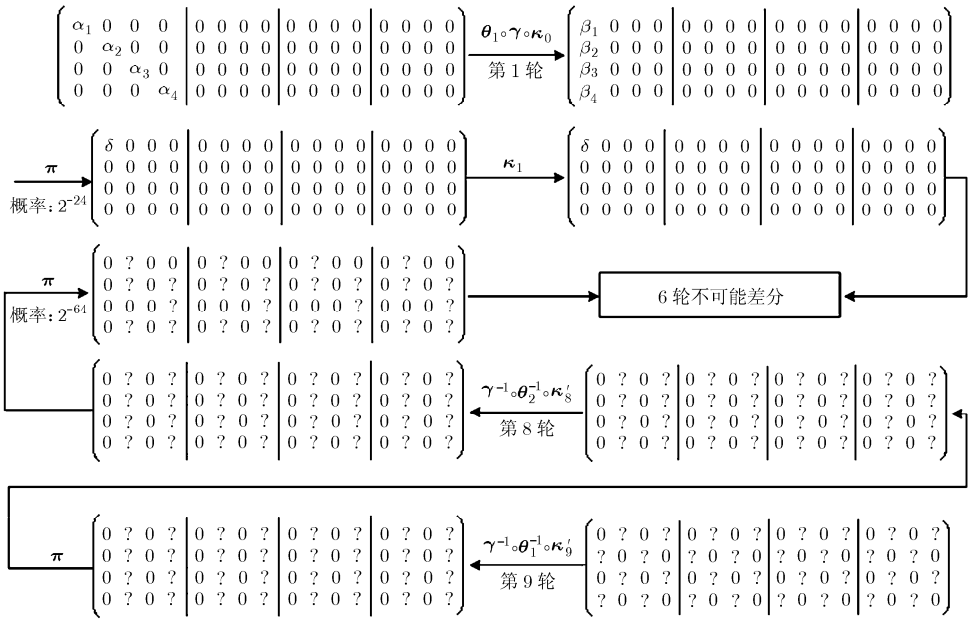

图2 3D密码的7/8/9轮不可能差分分析

4.2 3D密码的8轮不可能差分攻击

在7轮攻击的基础上在后面再加一轮可以得到8轮的攻击。注意第3节中的6轮不可能差分的最后一轮(第7轮)没有列混合$\boldsymbol{\pi}$，而8轮的3D算法在第7轮有列混合，所以这里不能直接用6轮不可能差分。这个问题可以这样解决：利用第2.3节的性质(c)，设$K_7'=\boldsymbol{\pi}^{-1}(K_7)$，则有$\boldsymbol{\kappa}_7\circ\boldsymbol{\pi}=\boldsymbol{\pi}\circ\boldsymbol{\kappa}_7'$，从而第7轮的轮函数为$\boldsymbol{\kappa}_7\circ\boldsymbol{\pi}\circ\boldsymbol{\theta}_1\circ\boldsymbol{\gamma}=\boldsymbol{\pi}\circ\boldsymbol{\kappa}_7'\circ\boldsymbol{\theta}_1\circ\boldsymbol{\gamma}$。所以这相当于将6轮区分器中的$\boldsymbol{\kappa}_7$换为$\boldsymbol{\kappa}_7'$，对上述不可能差分没有影响，这样就可以将7轮的攻击扩展至8轮了，注意此时第8轮作为最后一轮没有列混合$\boldsymbol{\pi}$。具体攻击过程(如图2前8轮所示)如下：

步骤1　与7轮攻击一样首先选择$m\times 2^{63}$对明文。

步骤2　对上述明文进行8轮加密，选取密文对差分满足所有奇数列字节为0的对留下，共有$m\times 2^{63}\times(2^{-8})^{32}=2^{-193}\times m$对。

步骤3　猜轮密钥K_8的偶数列字节的一个值(256 bit)，进行如下操作：

(a)对步骤2中留下的对进行一轮部分解密$(\boldsymbol{\pi}\circ\boldsymbol{\gamma}^{-1}\circ\boldsymbol{\theta}_2^{-1}\circ\boldsymbol{\kappa}_8)$。

(b)若密文对的差分在(6，12，22，28，38，44，54，60)这8个位置处的值为0，则其也满足在(3，6，9，12，19，22，25，28，35，38，41，44，51，54，57，60)这16个字节的差分值为0，同理，适当选取8个字节处的差分值为0也可以使得(2，5，8，15，18，21，24，31，34，37，40，47，50，53，56，63)，(1，4，11，14，17，20，27，30，33，36，43，46，49，52，59，62)及(0，7，10，13，16，23，26，29，32，39，42，45，48，55，58，61)三者之一的16个字节全为0，满足这样条件的对有$2^{-193}\times m\times(2^{-8})^8\times 4=2^{-255}\times m$对。

(c)任取步骤3(b)中留下的一个密文对相应的明文对，猜测密钥K_0的第0，5，10，15个字节的值(32 bit)，经过第1轮“部分加密”，若第1列4个字节有3个字节为0(概率为$(2^{-8})^3\times 4=2^{-22}$)，则根据6轮不可能差分知所测猜$K_0$的32 bit值是错误的。分析完$2^{-255}\times m$对，剩下的错误密钥数大概为$(2^{32}-1)(1-2^{-22})^{2^{-255}\times m}$。若$K_0$的所有这32 bit值都是错误的，转向第4步。

步骤4　重复步骤3，直到有唯一正确的密钥留下，输出K_0的32 bit值和K_8的相应256 bit值。

复杂度计算：从上面的攻击过程知，分析完第4步后，K_8的256 bit错误值大概还有$r=(2^{256}-1)(2^{32}-1)(1-2^{-22})^{2^{-255}\times m}$个，当$m=2^{285}$时，$r\approx 2^{-81}<1$，可认为错误密钥被全部排除。这时可得到$K_8$的256 bit值，剩下的另外256 bit值可通过穷举搜索得到。整个攻击过程的数据复杂度为$2^{32}\times m=2^{317}$个选择明文；步骤3(a)中的一轮部分解密次数为$2^{256}\times 2^{-193}\times m\times 2=2^{349}$，而一次部分解密相当于1/2轮加密，步骤3(c)中的一轮部分加密次数为$2^{256}\times[2^{32}\times 2+2^{32}(1-2^{-22})\times 2+\cdots+2^{32}(1-2^{-22})^{2^{-255}\times m}\times 2]\approx 2^{311}$，一轮部分加密相当于1/16轮加密，故总的时间复杂度为$(2^{349}\times 1/2+2^{311}\times 1/16)/8\simeq 2^{345}$次8轮加密。

4.3 3D 密码的 9 轮不可能差分攻击

基于 4.2 节的 8 轮攻击，我们可以攻击 9 轮 3D 密码，如图 2 所示。注意这里第 9 轮作为最后一轮没有列混合 $\boldsymbol{\pi}$，第 8 轮有列混合 $\boldsymbol{\pi}$，为了同时用于 8 轮的攻击，图中将第 8 轮的列混合 $\boldsymbol{\pi}$ 与密钥加 $\boldsymbol{\kappa}_8$ 交换了，这对 9 轮的攻击没有影响。攻击过程中如果同时猜测第 8 轮和第 9 轮中非零差分字节处的密钥值，则共需要猜测 512 bit 的值，复杂度将超过穷举搜索，但注意第 2.2 节的密钥扩展规则，有

$$K_9=\boldsymbol{\pi}\circ\boldsymbol{\theta}_{(9 \bmod 2)+1}\circ\boldsymbol{\gamma}'\circ\boldsymbol{\kappa}^*(K_8)=\boldsymbol{\pi}\circ\boldsymbol{\theta}_2\circ\boldsymbol{\gamma}'\circ\boldsymbol{\kappa}^*(K_8) \tag{4}$$

由 $\boldsymbol{\theta}_2$ 的性质知，如果我们猜测 K_8 的偶数列字节的值(256 bit)，由式(4)就可求出 K_9 的偶数列字节的值，从而只需再猜测 K_9 的奇数列的非零差分字节(1，3，9，11，17，19，25，27，33，35，41，43，49，51，57，59 这 16 个字节)处的值即可。

从上面的分析可知，我们只需要猜测 K_9 的 16 字节(128 bit)值和 K_8 的 256 bit 值共 384 bit 密钥值。9 攻击的主要思想是：用所猜测的密钥值进行两轮部分解密，剩下的步骤与 8 轮的攻击完全相同。

复杂度分析：由上面的分析知 9 轮的攻击与 8 轮的相比，只增加了猜测 K_9 的 16 字节(128 bit)值，其余几乎完全一样，故攻击的数据复杂度和时间复杂度相对于 8 轮的攻击也只增加一个因子 2^{128}。从而数据复杂度为 $2^{317}\times 2^{128}=2^{445}$ 个选择明文，时间复杂度为 $2^{345}\times 2^{128}=2^{473}$ 次 9 轮加密。

对于更多轮数的 3D 算法，需要猜测更多的密钥，攻击复杂度将超过穷举搜索。所以用上述 6 轮不可能差分只能攻击到 9 轮 3D 算法。

5 结论

本文研究了 3D 密码的不可能差分攻击，找到了 3D 密码新的 6 轮不可能差分，并利用此不可能差分结合密钥扩展算法及 3D 密码的等价结构对 3D 密码进行了 7–9 轮的攻击。表 1 列出了原作者的分析结果与本文的结果。攻击结果表明 9 轮及 9 轮以下的 3D 算法不抵抗不可能差分攻击。

表 1 对 3D 密码的各种攻击结果

文献	攻击方法	攻击轮数	数据复杂度(选择明文数)	时间复杂度(加密次数)
文献[1]	积分攻击	5	2^9	$2^{19.5}$
文献[1]	不可能差分	6	2^{36}	$2^{65.5}$
文献[1]	积分攻击	6	2^{129}	2^{139}
本文	不可能差分	7	2^{126}	2^{52}
本文	不可能差分	8	2^{317}	2^{345}
本文	不可能差分	9	2^{445}	2^{473}

参 考 文 献

[1] Nakahara J Jr. 3D: A three-dimensional block cipher[C]. CANS 2008, Springer-Verlag, 2008, LNCS 5339: 252–267.

[2] Biham E, Biryukov A, and Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]. EUROCRYPT'99, Springer-Verlag, 1999, LNCS 1592: 12–23.

[3] Nakahara J Jr and Ivan Carlos Pavao. Impossible-differential attacks on large-block rijndael[C]. ISC 2007, Springer-Verlag, 2007, LNCS 4779: 104–117.

[4] Zhang Wen-tao, Wu Wen-ling, and Feng Deng-guo. New results on impossible differential cryptanalysis of reduced AES[C]. ICISC 2007, Springer-Verlag, 2007, LNCS 4817: 239–250.

[5] 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.

[6] Lu Ji-qiang and Kim J, *et al*.. Improving the efficiency of impossible differential cryptanalysis of reduced camellia and MISTY1[C]. CT-RSA 2008, Springer-Verlag, 2008, LNCS 4964: 370–386.

[7] Tsunoo Y, Tsujihara E, and Shigeri M, *et al*.. Impossible differential cryptanalysis of CLEFIA[C]. FSE 2008, Springer-Verlag, 2008, LNCS 5086: 398–411

[8] Wang Wei and Wang Xiao-yun. Impossible differential cryptanalysis of CLEFIA-128/192/256[J]. *Journal of Software*, 2009, 20(9): 2587–2596.

[9] Zhang Wen-ying and Han Jing. Impossible differential cryptanalysis of reduced round CLEFIA[C], Inscrypt 2008, Springer-Verlag, 2009, LNCS 5487: 181–191.

唐学海： 男，1984 年生，博士生，研究方向为编码密码理论及其应用.

李 超： 男，1966 年生，博士生导师，教授，研究方向为编码密码理论及其应用.

王美一： 女，1985 年生，硕士生，研究方向为编码密码理论及其应用.