

3D 密码的 Square 攻击

王美一^① 唐学海^① 李超^① 屈龙江^{①②}

^①(国防科技大学数学与系统科学系 长沙 410073)

^②(东南大学移动通信国家重点实验室 南京 210096)

摘要: 3D 密码是 CANS 2008 提出的新的分组密码算法, 与以往的分组密码算法不同, 该密码采用 3 维结构。该文根据 3D 密码的结构特性, 得到了 3D 密码的 5.25 轮和 6.25 轮新的 Square 区分器, 重新评估了其抗 Square 攻击的强度。攻击结果表明: 新区分器对 6 轮 3D 密码攻击的数据复杂度和时间复杂度比已有的结果好, 并且还可应用到 7 轮, 8 轮和 9 轮的 3D 密码攻击中。

关键词: 分组密码; 3D 密码; Square 攻击

中图分类号: TN918.1

文献标识码: A

文章编号: 1009-5896(2010)01-0157-05

DOI: 10.3724/SP.J.1146.2008.01846

Square Attacks on 3D Cipher

Wang Mei-yi^① Tang Xue-hai^① Li Chao^① Qu Long-jiang^{①②}

^①(Department of Mathematics and System Science, National University of Defense Technology, Changsha 410073, China)

^②(National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

Abstract: 3D cipher is a new block cipher proposed in CANS 2008. It is different from all known block cipher as it uses the three dimension structure. According to the structure properties of 3D cipher, a new 5.25-round and a new 6.25-round square distinguishers are presented, and the square attacks on reduced- round 3D are improved. Attacking results demonstrate that 6-round attack is better than the known square attacks in data complexity and time complexity. Moreover, these two new distinguishers can be applied to 7/8/9-round 3D cipher.

Key words: Block cipher; 3D cipher; Square attack

1 引言

3D 密码是 Nakahara Jr. J 在 CANS 2008 上提出的一种新的 SPN 型分组密码算法^[1], 其主要设计思想来源于 AES 密码^[2]。在 AES 中, 明文、密文、中间状态都被表示为一个 2 维的 4×4 字节矩阵进行处理。3D 密码则把它们表示为 $4 \times 4 \times 4$ 的 3 维字节矩阵, 因而可形象地把它们看作是一个立方体。作者指出了 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。3D 密码的安全性仅在原文中给出了粗略的评估, 主要的评估结果见表 1。

Square 攻击最初是由 Knudsen 等人在文献^[3]中提出来的, 用来分析基于 SPN 结构的分组密码 Square。Lucks 等将此攻击应用于具有 Feistel 结构的 Twofish 密码^[4]。此后, Square 攻击被广泛地应用到各种结构的分组密码中, 并且取得了较好的结果^[5-8], 现在, Square 攻击被普遍认为是最有效的密码分析方法之一, 抗 Square 攻击的强度已经成为衡量新的分组密码安全性的重要标准。

表 1 文献[1]对 3D 密码的主要攻击结果

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)
低阶 Square 攻击	5	2^9	$2^{19.5}$
不可能差分攻击	6	2^{36}	$2^{65.5}$
高阶 Square 攻击	6	2^{129}	2^{139}

本文主要分析了 3D 密码的 Square 攻击, 发现了 5.25 轮和 6.25 轮新的 Square 区分器, 并给出了低轮 3D 密码的 Square 攻击, 这些结果都优于原文献, 见表 2。这表示低轮的 3D 密码对 Square 攻击是不抵抗的, 但这并不能表明完整的 3D 密码是不安全的, 其安全性有待进一步的研究。

2 3D 密码简介

本文中所涉及到的符号如下: X 为 512-bit 的明文, C 为 512-bit 的密文, $C_{(j)}^i$ 为第 i 个密文的第 j 个字节, τ_i 为 i 轮的轮函数, k_i 为第 i 轮的密钥, $k_{i(j)}$ 为 k_i 的第 j 个字节, $f \circ g$ 为表示函数 f 和 g 的复合运算, 即 $f \circ g(x) = f(g(x))$ 。

3D 密码的分组长度和密钥长度均为 512 bit, 都可表示为 $4 \times 4 \times 4$ 的 3 维字节矩阵。

对于 64 个字节的数据分组, 按照图 1 排列。

2008-12-31 收到, 2009-06-29 改回
国家自然科学基金(60803156)和东南大学移动通信国家重点实验室
开放基金(w200807)资助课题
通信作者: 王美一 tomorrow_selly@163.com

表 2 3D 密码的 Square 攻击的比较

攻击 轮数	文献[1]		本文	
	数据 复杂度	时间 复杂度	数据 复杂度	时间 复杂度
6	2^{129}	2^{130}	$2^{33} \textcircled{1}$	$2^{38} \textcircled{1}$
7	-	-	$2^{35} \textcircled{1}$	$2^{94} \textcircled{1}$
8	-	-	$2^{131} \textcircled{2}$	$2^{189} \textcircled{2}$
9	-	-	$2^{133} \textcircled{2}$	$2^{414} \textcircled{2}$

注：下标①表示应用的是 5.25 轮区分器，②表示应用的是 6.25 轮区分器

$$\begin{pmatrix} x_0 & x_4 & x_8 & x_{12} & x_{16} & x_{20} & x_{24} & x_{28} & x_{32} & x_{36} & x_{40} & x_{44} & x_{48} & x_{52} & x_{56} & x_{60} \\ x_1 & x_5 & x_9 & x_{13} & x_{17} & x_{21} & x_{25} & x_{29} & x_{33} & x_{37} & x_{41} & x_{45} & x_{49} & x_{53} & x_{57} & x_{61} \\ x_2 & x_6 & x_{10} & x_{14} & x_{18} & x_{22} & x_{26} & x_{30} & x_{34} & x_{38} & x_{42} & x_{46} & x_{50} & x_{54} & x_{58} & x_{62} \\ x_3 & x_7 & x_{11} & x_{15} & x_{19} & x_{23} & x_{27} & x_{31} & x_{35} & x_{39} & x_{43} & x_{47} & x_{51} & x_{55} & x_{59} & x_{63} \end{pmatrix}$$

图 1

3D 密码的加密轮数是 22 轮。r 轮 ($0 < r \leq 22$) 的加密过程如下：设明文分组为 X，第 i 轮的轮函数为： $\tau_i(X) = \pi \circ \theta_{i \bmod 2+1} \circ \gamma \circ \kappa_i(X) = \pi(\theta_{i \bmod 2+1}(\gamma(\kappa_i(X))))$ ， $0 \leq i \leq r-2$ 。最后一轮没有 π 但增加了 κ_r ，即最后一轮的轮函数为 $\tau_{r-1}(X) = \kappa_r \circ \theta_{(r-1) \bmod 2+1} \circ \gamma \circ \kappa_{r-1}(X)$ 。其中 κ_i 是将 512-bit 密钥 k_i 按比特位直接与数据进行异或； γ 是对数据的每一个字节都进行相同的 S 盒操作，采用的是 AES 中的 S 盒； θ_1, θ_2 相当于 AES 中的行移位操作； θ_1 把图 1 变换为图 2 排列； θ_2 把图 1 变换为图 3 排列。

$$\begin{pmatrix} x_0 & x_4 & x_8 & x_{12} & x_{16} & x_{20} & x_{24} & x_{28} & x_{32} & x_{36} & x_{40} & x_{44} & x_{48} & x_{52} & x_{56} & x_{60} \\ x_5 & x_9 & x_{13} & x_1 & x_{21} & x_{25} & x_{29} & x_{17} & x_{37} & x_{41} & x_{45} & x_{33} & x_{53} & x_{57} & x_{61} & x_{49} \\ x_{10} & x_{14} & x_2 & x_6 & x_{26} & x_{30} & x_{18} & x_{22} & x_{42} & x_{46} & x_{34} & x_{38} & x_{58} & x_{62} & x_{50} & x_{54} \\ x_{15} & x_3 & x_7 & x_{11} & x_{31} & x_{19} & x_{23} & x_{27} & x_{47} & x_{35} & x_{39} & x_{43} & x_{63} & x_{51} & x_{55} & x_{59} \end{pmatrix}$$

图 2

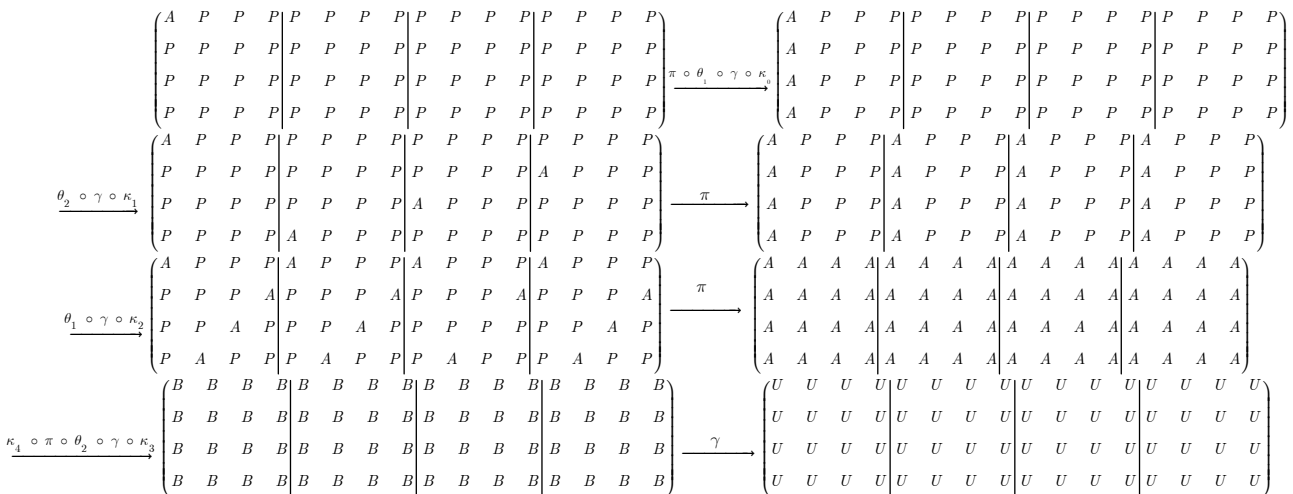


图 4 文献[1]中的 4.25 轮区分器

$$\begin{pmatrix} x_0 & x_4 & x_8 & x_{12} & x_{16} & x_{20} & x_{24} & x_{28} & x_{32} & x_{36} & x_{40} & x_{44} & x_{48} & x_{52} & x_{56} & x_{60} \\ x_{17} & x_{21} & x_{25} & x_{29} & x_{33} & x_{37} & x_{41} & x_{45} & x_{49} & x_{53} & x_{57} & x_{61} & x_1 & x_5 & x_9 & x_{13} \\ x_{34} & x_{38} & x_{42} & x_{46} & x_{50} & x_{54} & x_{58} & x_{62} & x_2 & x_6 & x_{10} & x_{14} & x_{18} & x_{22} & x_{26} & x_{30} \\ x_{51} & x_{55} & x_{59} & x_{63} & x_3 & x_7 & x_{11} & x_{15} & x_{19} & x_{23} & x_{27} & x_{31} & x_{35} & x_{39} & x_{43} & x_{47} \end{pmatrix}$$

图 3

π 相当于 AES 中的列混合操作，这里使用的是 Anubis 密码^[9]中 4×4 的 MDS 矩阵。密钥扩展算法与本文分析无关，不再赘述。

3 3D 密码的 Square 攻击

首先给出 Λ 集的概念：

Square 攻击和 Λ 集的概念是由 Knudsen 等人在文献[3]中引入的。记 Γ 集是一个字节集的 256 个状态集。状态集的元素是 $i \in \{0, 1, \dots, 255\}$ ，其中 $\gamma^{(i,j)}$ 是 $\gamma^{(i)}$ 的第 j 个字节。如果 Γ 集中的第 j 个字节各不相同，即 $\gamma^{(i,j)} \neq \gamma^{(i',j)}, \forall i, i' \in \{0, 1, \dots, 255\}, i \neq i'$ ，称之为活跃字节。如果第 j 个字节保持不变，即 $\gamma^{(i,j)} = \gamma^{(i',j)}, \forall i, i' \in \{0, 1, \dots, 255\}, i \neq i'$ ，称之为固定字节，而如果第 j 个字节的模二加和为 0，即 $\sum_{i \in \{0, 1, \dots, 255\}} \gamma^{(i,j)} = 0$ ，则称之为平衡字节。为后续讨

论方便，A 代表活跃字节，P 代表固定字节，而 B 代表平衡字节，其它字节用 U 表示。如果所有字节为活跃字节和固定字节，称之为 Λ 集。

下面给出文献[1]中的 4.25 轮区分器(图 4)，即若选取明文为只有一个字节是活跃字节的 Λ 集，则可得以下 4.25 轮的区分器：

3.1 5.25 轮区分器和基于该区分器对 3D 密码的 6 轮, 7 轮, 8 轮的攻击

假设算法从第 2 轮开始, 则若选取输入为一个

只有一个字节是活跃字节的 Λ 集, 那么容易验证它满足(图 5)中的 4.25 轮区分器:

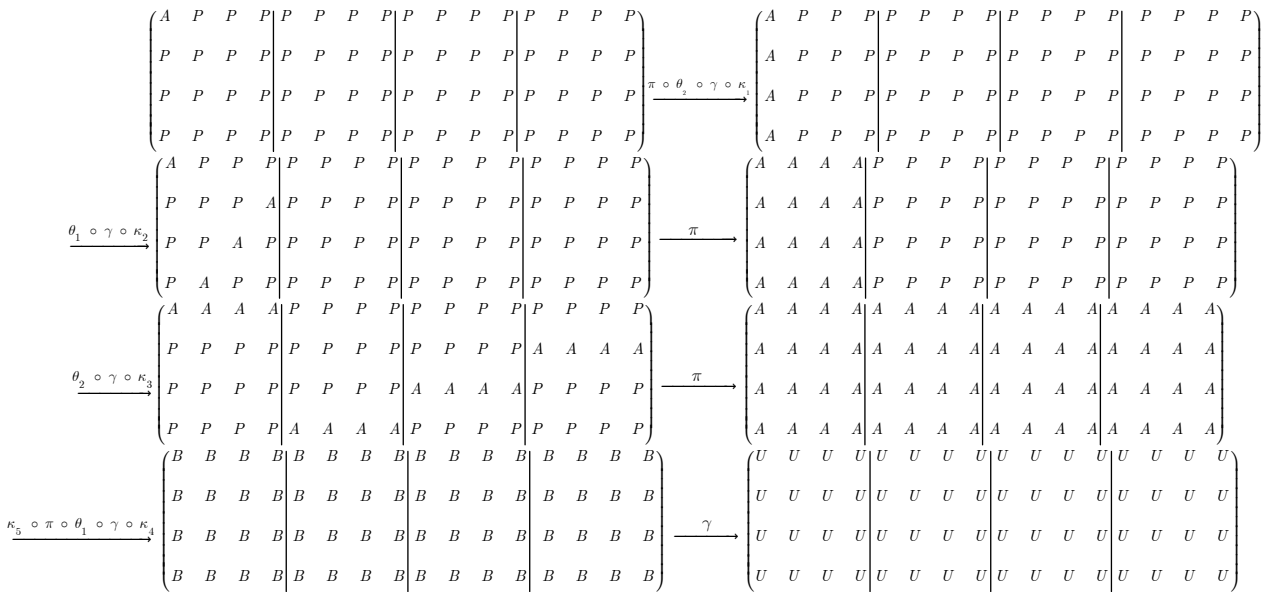


图 5 本文用到的 4.25 轮区分器

然后在此 4.25 轮区分器的基础上, 考虑算法的第 1 轮, 若选取包含 2^{32} 个不同明文的明文组, 其中

4 个字节 ($A_0^*, A_1^*, A_2^*, A_3^*$) 遍历所有 2^{32} 种取值, 其余字节都为常值, 那么在经过第 1 轮以后将会得到图 6 排列。

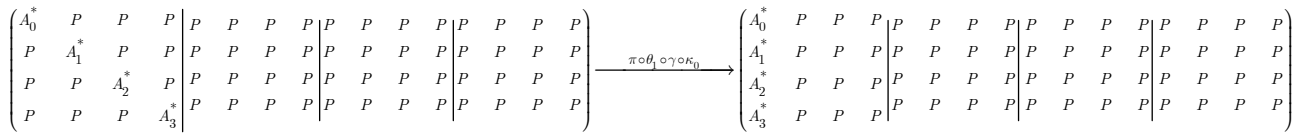


图 6

此时, 可以把它看作是由如下 2^{24} 个不可区分的 Λ 集 (图 7) 组成, 这样便得到了 5.25 轮的区分器。其中, P_i 是常数, $1 \leq i \leq 3$, 但在不同的 Λ 集中不相同。接下来, 应用上述 5.25 轮的区分器对 3D 密码进行 6 轮, 7 轮和 8 轮的攻击。具体的攻击过程如下:

测的第 j 个密钥字节使得 $\bigoplus_{i=0}^{2^{32}-1} S^{-1}(\theta_2^{-1}(C_{(j)}^i \oplus k_{6(j)})) \neq 0, 0 \leq j \leq 63$, 则此次猜测必为错误的, 遍历该字节的候选值, 则剩余的错误密钥有 $(2^8 - 1) \times (1/2^8) < 1$ 个。因此两个上述结构的明文组就可以唯一确定正确密钥。故恢复 k_6 的数据复杂度为 $2 \times 2^{32} = 2^{33}$ 个选择明文, 时间复杂度为 $64 \times (2^8 \times 2^{32} + 2^{32}) \times (1/64) \times (1/6) \approx 2^{38}$ 次 6 轮加密。

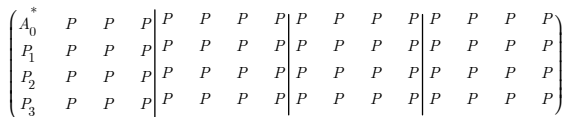


图 7

情形 1 对 3D 密码的 6 轮攻击

6 轮 3D 的加密过程是:

$$C = \kappa_6 \circ \theta_2 \circ \gamma \circ \kappa_5 \circ O_{i=0}^4 (\pi \circ \theta_{i \bmod 2+1} \circ \gamma \circ \kappa_i)(X)$$

使用满足 5.25 轮区分器输入的包含 2^{32} 个不同明文的明文组, 分别恢复第 6 轮的每一个密钥字节。经过分析, 每次只需对 k_6 的一个字节进行猜测, 若猜

情形 2 对 3D 密码的 7 轮攻击

7 轮 3D 的加密过程是:

$$C = \kappa_7 \circ \theta_1 \circ \gamma \circ \kappa_6 \circ \pi \circ \theta_2 \circ \gamma \circ \kappa_5$$

$$\circ O_{i=0}^4 (\pi \circ \theta_{i \bmod 2+1} \circ \gamma \circ \kappa_i)(X)$$

经过对密码结构的分析, 为了应用上述 5.25 轮的区分器, 必须每次猜测 k_6 和 k_7 的各 4 个字节。使用一个包含 2^{32} 个不同明文的明文组对每一次猜测的 8 个字节的的所有可能性进行验证以后, 留下来的错误密钥为 $(2^{64} - 1) \cdot (1/2^8) \approx 2^{56}$ 个, 因此需要 9 个包含 2^{32} 个不同明文的明文组就可以唯一确定正确密钥。

下面以恢复 k_7 的 4 个字节 $k_{7(0)}, k_{7(7)}, k_{7(10)}, k_{7(13)}$ 为例介绍一下具体的攻击过程

步骤1 猜测 $k_{7(0)}, k_{7(7)}, k_{7(10)}, k_{7(13)}, k_{6(0)}, k_{6(1)}, k_{6(2)}, k_{6(3)}$ 的一种可能值。

步骤2 任取一组排列如图 8, 包含 2^{32} 个不同

$$\begin{pmatrix} A_0^* & P & P & P & P & P & P & P & P & P & P & P & P & P & P \\ P & A_1^* & P & P & P & P & P & P & P & P & P & P & P & P & P \\ P & P & A_2^* & P & P & P & P & P & P & P & P & P & P & P & P \\ P & P & P & A_3^* & P & P & P & P & P & P & P & P & P & P & P \end{pmatrix}$$

图 8

明文的明文组, 相应的密文记为 $C_{(j)}^i, (0 \leq i \leq 2^{32} - 1, 0 \leq j \leq 63)$ 。计算

$$\begin{aligned} Z_i = & S^{-1} \left(\left(S^{-1} (k_{7(0)} \oplus C_{(0)}^i) \oplus k_{6(0)} \right) \right. \\ & \oplus 02 \left(S^{-1} (k_{7(13)} \oplus C_{(13)}^i) \oplus k_{6(1)} \right) \\ & \oplus 04 \left(S^{-1} (k_{7(10)} \oplus C_{(10)}^i) \oplus k_{6(2)} \right) \\ & \left. \oplus 06 \left(S^{-1} (k_{7(7)} \oplus C_{(7)}^i) \oplus k_{6(3)} \right) \right) \end{aligned}$$

步骤3 计算 $Z = \bigoplus_{i=0}^{2^{32}-1} Z_i$, 若 $Z \neq 0$, 则此次猜

测的密钥必为错误的。

步骤4 对这 8 个密钥字节猜测的所有可能性一一验证以后, 把剩下的密钥候选值存储在集合 N 中, 然后选取另一个包含 2^{32} 个不同明文的明文组对 N 中的每一种可能进行步骤 2 到步骤 3 的验证, 再用剩下的密钥候选值更新集合 N , 重复此攻击过程

$$\begin{aligned} & \begin{pmatrix} A_0^* & P & P & P & A_4^* & P & P & P & A_8^* & P & P & P & A_{12}^* & P & P & P \\ P & A_1^* & P & P & P & A_5^* & P & P & P & A_9^* & P & P & P & A_{13}^* & P & P \\ P & P & A_2^* & P & P & P & A_6^* & P & P & P & A_{10}^* & P & P & P & A_{14}^* & P \\ P & P & P & A_3^* & P & P & P & A_7^* & P & P & P & A_{11}^* & P & P & P & A_{15}^* \end{pmatrix} \\ & \xrightarrow{\pi \circ \theta_1 \circ \gamma \circ \kappa_0} \begin{pmatrix} A_0^* & P & P & P & A_4^* & P & P & P & A_8^* & P & P & P & A_{12}^* & P & P & P \\ A_1^* & P & P & P & A_5^* & P & P & P & A_9^* & P & P & P & A_{13}^* & P & P & P \\ A_2^* & P & P & P & A_6^* & P & P & P & A_{10}^* & P & P & P & A_{14}^* & P & P & P \\ A_3^* & P & P & P & A_7^* & P & P & P & A_{11}^* & P & P & P & A_{15}^* & P & P & P \end{pmatrix} \\ & \xrightarrow{\pi \circ \theta_2 \circ \gamma \circ \kappa_1} \begin{pmatrix} A_0^* & P & P & P & A_4^* & P & P & P & A_8^* & P & P & P & A_{12}^* & P & P & P \\ A_5^* & P & P & P & A_9^* & P & P & P & A_{13}^* & P & P & P & A_1^* & P & P & P \\ A_{10}^* & P & P & P & A_{14}^* & P & P & P & A_2^* & P & P & P & A_6^* & P & P & P \\ A_{15}^* & P & P & P & A_3^* & P & P & P & A_7^* & P & P & P & A_{11}^* & P & P & P \end{pmatrix} \end{aligned}$$

图 9

可以把图 9 看作是由 2^{120} 个不可区分的 Λ 集(图 10)组成, 便得到了 6.25 轮的区分器。其中, P_i 常数, $1 \leq i \leq 15$, 但在不同的 Λ 集中不相同。

利用上述 6.25 轮的区分器可以对 3D 密码进行 7 轮, 8 轮和 9 轮的攻击。攻击过程与 3.1 小节的类似, 不再详述, 只将攻击结果列举如下:

直到最终把正确密钥唯一确定下来。

攻击复杂度如下:

数据复杂度为 $9 \times 2^{32} \approx 2^{35}$ 个选择明文, 时间复杂度为 $16 \times (2^{64} + 2^{56} + 2^{48} + 2^{40} + 2^{32} + 2^{24} + 2^{16} + 2^8 + 1) \times 2^{32} \times (5/64) \times (1/7) \approx 2^{94}$ 次 7 轮加密。

情形 3 对 3D 密码的 8 轮攻击

8 轮 3D 的加密过程是:

$$C = \kappa_8 \circ \theta_2 \circ \gamma \circ \kappa_7 \circ \pi \circ \theta_1 \circ \gamma \circ \kappa_6 \circ \pi \circ \theta_2 \circ \gamma \circ \kappa_5 \circ O_{i=0}^4 (\pi \circ \theta_{i \bmod 2+1} \circ \gamma \circ \kappa_i)(X)$$

根据密码具体结构的分析, 为了应用上述 5.25 轮的区分器, 必须每次对 k_7, k_8 的各 16 个字节和 k_6 的 4 个字节一同进行猜测, 先恢复出 k_7, k_8 的全部字节和 k_6 的 16 个字节后, 再应用密钥扩展算法恢复 k_6 的剩下 48 个字节。具体的攻击过程与 7 轮的类似。由于每次共猜测 36 个字节则需要 37 个包含 2^{32} 个不同明文的明文组就可以唯一确定正确密钥。因此, 攻击的数据复杂度是 $37 \times 2^{32} \approx 2^{37}$ 个选择明文, 时间复杂度是 $4 \times (2^{288} + 2^{280} + 2^{272} + \dots + 2^8 + 1) \times 2^{32} \times (21/64) \times (1/8) \approx 2^{317}$ 次 8 轮加密。

3.2 6.25 轮区分器和基于该区分器对 3D 密码的 7 轮, 8 轮, 9 轮的攻击

本文在文献[1]中提出的 4.25 轮区分器(图 1)的基础上, 考虑选取有 2^{128} 个明文的明文组, 它的其中 16 个字节 ($A_0^*, A_1^*, A_2^*, A_3^*, A_4^*, A_5^*, A_6^*, A_7^*, A_8^*, A_9^*, A_{10}^*, A_{11}^*, A_{12}^*, A_{13}^*, A_{14}^*, A_{15}^*$) 遍历所有 2^{128} 种取值, 其余字节都为常值, 那么在经过两轮以后得到图 9 排列。

$$\begin{pmatrix} A_0^* & P & P & P & P_4 & P & P & P & P_8 & P & P & P & P_{12} & P & P & P \\ P_1 & P & P & P & P_5 & P & P & P & P_9 & P & P & P & P_{13} & P & P & P \\ P_2 & P & P & P & P_6 & P & P & P & P_{10} & P & P & P & P_{14} & P & P & P \\ P_3 & P & P & P & P_7 & P & P & P & P_{11} & P & P & P & P_{15} & P & P & P \end{pmatrix}$$

图 10

(1)对 3D 密码的 7 轮攻击: 数据复杂度为 2^{129} 个

选择明文, 时间复杂度为 $64 \times (2^8 \times 2^{128} + 2^{128}) \times (1/64) \times (1/7) \approx 2^{133}$ 次 7 轮加密。

(2) 对 3D 密码的 8 轮攻击: 数据复杂度为 $9 \times 2^{128} \approx 2^{131}$ 个选择明文, 时间复杂度为 $16 \times (2^{64} + 2^{56} + 2^{48} + \dots + 2^8 + 1) \times 2^{128} \times (5/64) \times (1/8) \approx 2^{189}$ 次 8 轮加密。

(3) 对 3D 密码的 9 轮攻击: 数据复杂度为 $37 \times 2^{128} \approx 2^{133}$ 个选择明文, 时间复杂度为 $4 \times (2^{288} + 2^{280} + 2^{272} + \dots + 2^8 + 1) \times 2^{128} \times (21/64) \times (1/9) \approx 2^{414}$ 次 9 轮加密。

4 结束语

本文给出了对 3D 密码新的 Square 攻击。表 2 列出了与文献[1]中 Square 攻击的结果比较。文献[1]中只攻击到 6 轮, 本文给出了新的 5.25 轮和 6.25 轮的区分器, 并把攻击扩展到 9 轮的 3D, 同时 6 轮攻击的数据复杂度和时间复杂度都比文献[1]要优越得多。

参考文献

- [1] Nakahara Jr J. A three-dimensional block cipher. CANS 2008, Lecture Notes in Computer Science, 2008, Vol. 5339: 252-267.
- [2] Daemen J and Rijmen V. AES Proposal: Rijndael. http://www.cryptolounge.org/wiki/AES_Proposal:_Rijndael, 1998, 08.
- [3] Daemen J, Knudsen L, and Rijmen V. The block cipher Square. FSE1997, Lecture Notes in Computer Science, Springer-Verlag, 1997, Vol. 1267: 149-165.
- [4] Lucks S. The saturation attack-a bait for twofish. FSE2002, Lecture Notes in Computer Science, Springer-Verlag, 2002, Vol. 2335: 1-15.
- [5] Ferguson N, Kelsey J, and Lucks S, *et al.* Improved cryptanalysis of Rijndael. FSE2000, Lecture Notes in Computer Science, Springer-Verlag, 2001, Vol. 1978: 213-230.
- [6] Duo Lei, Li Chao, and Feng Ke-qin. Square like attack on Camellia. ICICS2007, Lecture Notes in Computer Science, Springer-Verlag, 2007, Vol. 4861: 269-283.
- [7] 王薇, 王小云. 对 CLEFIA 算法的饱和度分析. 通信学报, 2008, 29(10): 88-92.
Wang Wei and Wang Xiao-yun. Saturation cryptanalysis of CLEFIA. *Journal of Communication*, 2008, 29(10): 88-92.
- [8] Muhammad Reza Z'aba, Havard Raddum, and Matt Henriksen, *et al.* Bit-pattern based integral attack. FSE2008, Lecture Notes in Computer Science, Springer-Verlag, 2008, Vol. 5086: 363-381.
- [9] Barreto P and Rijmen V. The ANUBIS Block Cipher. <http://www.sciencecentral.com/site/497719>, 2000, 06.

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。

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。