doi:10.11959/j.issn.1000-436x.2015131

11 轮 3D 密码算法的中间相遇攻击

任炯炯[1,2]，陈少真[1,2]
(1. 解放军信息工程大学 网络空间安全学院，河南 郑州 450001；2. 数学工程与先进计算国家重点实验室，河南 郑州 450001)

摘 要：引入多重集并结合截断差分和 S 盒的性质，构造出 6 轮中间相遇区分器，实现 11 轮 3D 密码的中间相遇攻击，恢复密钥所需的时间复杂度为 2^{329}，并结合时空折中的方法降低了数据复杂度。此外，利用新的区分器有效改进了 3D 算法 10 轮中间相遇攻击的时间复杂度，约 2^{201} 次 10 轮加密运算。
关键词：分组密码；3D 算法；中间相遇攻击；预计算；多重集
中图分类号：TN918.1 **文献标识码**：A

Meet-in-the-middle attack on 11-round 3D cipher

REN Jiong-jiong[1,2], CHEN Shao-zhen[1,2]
(1. Faculty of Cyberspace Secrity, PLA Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract: A new 6-round meet-in-the-middle distinguisher was constructed by introducing multiset, making use of properties of the S-box was proposed and the truncated differential characteristic. Based on the distinguisher, a meet-in-the-middle attack on 11-round 3D cipher and the time complexity of recovering the key was about 2^{329}. Furthermore, the data complexity was reduced using the time/memory tradeoff technique. Besides, by utilizing the new distinguisher, the time complexity of 10-round attack on 3D cipher is reduced to 2^{201}.
Key words: block cipher; 3D cipher; meet-in-the-middle attack; precomputation; multiset

1 引言

3D 密码算法[1]是在 CANS 2008 上提出的一个 SPN 型结构的分组密码，其设计思想主要受 AES 密码算法的启发。3D 密码分组长度与密钥长度都为 512 bit，数据加密过程利用了 AES 轮函数设计的优势，将数据表示为 4×4×4 的三维字节矩阵。由于 3D 密码新的设计理念，加上现代科学技术的发展以及计算能力的不断刷新，分组密码的趋势也是朝更长的分组以及密钥长度发展，出于其安全性以及潜在应用考虑，3D 密码算法的分析已备受关注。

对 3D 密码的安全性分析首先由设计者 Nakahara[1]提出，其中包括传统的差分与线性分析、截断差分分析、相关密钥攻击、积分攻击、不可能差分攻击等。2010 年王美一等[2]对 9 轮 3D 密码算法进行了积分攻击。同年，唐学海等[3]给出了 9 轮 3D 密码算法的不可能差分攻击，随后 Nakahara[4]给出了 10 轮 3D 密码算法的不可能差分新攻击。2012 年苏崇茂等[5]利用 3D 算法结构，构造出 5 轮中间相遇区分器，并由此给出 10 轮 3D 算法的中间相遇攻击。2012 年在 ISPEC 会上，Takuma Koyama 等[6]利用 3D 密码新的截断差分路径，以约 24%的成功概率首次给出了 11 轮的分析结果。2014 年谢作敏等[7]构造出 3D 密码算法一类新的 6 轮不可能差分区分器，最大程度利用 Hash 存储的预计算技术，将 3D 密码的不可能差分攻击扩展到 11 轮，但攻击需要的时间复杂度较大。

中间相遇攻击[8~10]是一种选择明文攻击，其主要思想是首先建立特殊明文对应的筛选集合，接着利用满足特殊明文形式要求明密对的若干字节或者比特，经过正向加密和逆向解密后，通过中间数据的相遇构成碰撞，形成一个有效的攻击。在多数

收稿日期：2014-06-10；**修回日期**：2014-11-20
基金项目：信息保障技术重点实验室开放基金资助项目（KJ-13-010）
Foundation Item: The Foundation of Science and Technology on Information Assurance Laboratory(KJ-13-010)

情况下，中间相遇攻击需要大量的预计算复杂度和时间复杂度，虽然预计算只需要一次，但如果涉及的参数数量太多，预计算复杂度就会超过穷举密钥搜索的复杂度。因此如何减少预计算的复杂度和需要猜测的密钥量，以及如何降低攻击的时间复杂度，一直以来是密码学界不懈探讨的问题。

中间相遇攻击“多重集”的概念最初是由 Dunkelman 等[11]在 ASIACRYPT 2010 分析 AES 时引入。他们的思想是不存储整个输出序列，而是存储相关无序的差分筛选集合，并利用截断差分的性质，减少需要猜测区分器的参数量，从而有效降低存储复杂度。

本文主要研究 3D 密码算法的中间相遇攻击，利用 3D 算法截断差分的性质，构造了 6 轮多重集。进一步，利用 3D 算法 S 盒的性质和有效的枚举技术，将预计算的参数由 104 个减少到 42 个，大幅度地降低了预计算复杂度，构造了新的中间相遇区分器，首次实现 11 轮 3D 密码算法的中间相遇攻击，密钥恢复所需的时间复杂度低至 2^{329}。同时利用时空折中的思想，通过增加活动字节的个数和改变活动字节的位置，给出 2 个改进数据复杂度的攻击结果。此外利用构造的 6 轮中间相遇区分器，将 10 轮中间相遇攻击的时间复杂度降为 2^{201}。

2　3D 密码算法

2.1　3D 密码加密算法

分组密码 3D 算法是 SPN 型的密码体制，分组长度与密钥长度均为 512 bit，中间状态可用 4×4×4 的三维字节矩阵表示。对于 64 个字节的分组数据 $\boldsymbol{A}=(a_0,a_1,\cdots,a_{63})$，按列存放可以表示成

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

3D 密码算法建议的加密轮数是 22 轮，轮函数由轮密钥加 (k_i)、置换层 (γ)、行移位 (θ_1,θ_2) 和列混合 (π) 4 个部件构成。

1) 轮密钥加 (k_i)：将每轮的分组数据与 512 bit 的轮子密钥相异或，轮子密钥由密钥扩展算法产生。

2) 置换层 (γ)：将分组状态的 64 个字节进行相同的 S 盒操作，采用的 S 盒与 AES 相同。

3) 行移位 (θ_1,θ_2)：θ_1 作用于奇数轮，θ_2 作用于偶数轮。其中，θ_1 对状态矩阵每一小块进行相同的行移位，将式(1)变换成

$$\boldsymbol{A}'=\left(\begin{array}{cccc|cccc|cccc|cccc} a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\ a_5 & a_9 & a_{13} & a_1 & a_{21} & a_{25} & a_{29} & a_{17} & a_{37} & a_{41} & a_{45} & a_{33} & a_{53} & a_{57} & a_{61} & a_{49} \\ a_{10} & a_{14} & a_2 & a_6 & a_{26} & a_{30} & a_{18} & a_{22} & a_{42} & a_{46} & a_{34} & a_{37} & a_{58} & a_{62} & a_{50} & a_{54} \\ a_{15} & a_3 & a_7 & a_{11} & a_{31} & a_{19} & a_{23} & a_{27} & a_{47} & a_{35} & a_{39} & a_{43} & a_{63} & a_{51} & a_{55} & a_{59} \end{array}\right) \tag{2}$$

θ_2 对整个大矩阵进行行移位，将式(1)变换成

$$\boldsymbol{A}''=\left(\begin{array}{cccc|cccc|cccc|cccc} a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\ a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} & a_1 & a_5 & a_9 & a_{13} \\ a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} & a_2 & a_6 & a_{10} & a_{14} & a_{18} & a_{22} & a_{26} & a_{30} \\ a_{51} & a_{55} & a_{59} & a_{63} & a_3 & a_7 & a_{11} & a_{15} & a_{19} & a_{23} & a_{27} & a_{31} & a_{35} & a_{39} & a_{43} & a_{47} \end{array}\right) \tag{3}$$

4) 列混合 (π)：类似 AES 的列混合，用 4×4 的 MDS 可逆矩阵对状态矩阵每一列进行相乘操作。

3D 密码的第 i 轮加密可以表示成

$$\tau_i(X)=\pi\circ\theta_{(i \bmod 2)+1}\circ\gamma\circ k_i(X),0\leqslant i\leqslant r-1 \tag{4}$$

注意最后一轮以轮密钥加代替列混合。

3D 密码有个重要的性质[1]：对于 3D 的轮密钥加 k_i 与列混合 π，由于都是线性变换，因而可以交换顺序，$k_i\circ\pi=\pi\circ k_i^*$，此时 k_i^* 是 k_i 的等效密钥，$k_i^*=\pi^{-1}(k_i)$。

2.2　3D 算法的密钥编排方案

设种子密钥 $K=(K_0,K_1,\cdots,K_{63})$，则轮子密钥 K_i 可以通过以下方式得到

$$K_0=K,K_i=\pi\circ\theta_{(i \bmod 2)+1}\circ\gamma\circ K^*(K_{i-1}),i\geqslant 1 \tag{5}$$

其中，K^* 是将 K_{i-1} 异或一个 512 bit 的固定值，γ 是对状态矩阵分组数据的一部分字节作 S 盒变换，(θ_1,θ_2)、(π) 与加密算法轮函数的变化相同。由密钥编排方案可知种子密钥可以通过任何一个轮子密钥计算出来。

3 3D 密码算法 6 轮中间相遇区分器

本文符号及标注：P 表示明文，C 表示密文，R_i 表示第 i 轮，X_m 表示第 m 轮的输入，X_m^i 表示 X_m 的第 i 个取值状态，$X_{m,n}$ 表示 X_m 的第 n 个字节，$X_{m,n}^i$ 表示 $X_{m,n}$ 的第 i 个取值，$X_m(IN)$ 表示第 m 轮置换层 γ 变换前的状态，$X_m(\gamma)$ 表示第 m 轮置换层 γ 变换后的状态，$X_m^i(IN)$ 表示 X_m^i 在第 m 轮置换层 γ 变换前的状态，$X_m^i(\gamma)$ 表示 X_m^i 在第 m 轮置换层 γ 变换后的状态，$\Delta X_m^i(IN)$ 表示状态差分值 $X_m^i(IN)\oplus X_m^0(IN)$。

本节利用 3D 算法的结构特点，首先给出 6 轮多重集，但参数个数多，超过穷举复杂度，不能作为中间相遇区分器；接着利用截断差分和 S 盒的性质，通过有效的枚举，将预计算的参数由 104 个减少到 42 个，大幅降低了预计算复杂度，构造了 11 轮中间相遇攻击利用的区分器。

在定义多重集前，给出 3D 密码算法 δ-集[8]的定义。

定义 1 3D 算法一组明文的 1 个活动字节遍历 256 个所有可能值，其他 63 个字节取固定值(可以相同)，这样得到一个结构称为 δ-集，表示为 $\{X_m^0,X_m^1,\cdots,X_m^{255}\}$，其中，$X_m^i$ 是 512 bit 的一个状态值，$0\leqslant i\leqslant 255$，$m$ 为 3D 算法的轮数，$1\leqslant m\leqslant 22$。

由 δ-集的概念，给出 3D 密码算法的 6 轮多重集。

性质 1 (6 轮多重集) 对定义的 3D 算法的 δ-集进行 6 轮加密，对每个 $0\leqslant n\leqslant 63$，无序的多重集 $\{X_{m+6,n}^0\oplus X_{m+6,n}^0,X_{m+6,n}^1\oplus X_{m+6,n}^0,\cdots,X_{m+6,n}^{255}\oplus X_{m+6,n}^0\}$ 完全由以下 104 个字节变量决定。

1) 状态 $X_{m+1}^0(IN)$ 的 4 个字节；

2) 状态 $X_{m+2}^0(IN)$ 的 16 个字节；

3) 状态 $X_{m+3}^0(IN)$ 的全部 64 个字节；

4) 状态 $X_{m+4}^0(IN)$ 的 16 个字节；

5) 状态 $X_{m+5}^0(IN)$ 的 4 个字节。

证明 以第 0 个字节是活动字节，其他 63 个字节是非活动字节为例来证明。对 δ-集 $\{X_m^0,X_m^1,\cdots,X_m^{255}\}$ 进行 6 轮 3D 算法加密，从第一轮开始推导。由于 δ-集遍历 256 个状态，经过密钥加、γ 变换后仍遍历 256 个无序的状态，差分 $\Delta X_m^i(\gamma)=X_m^i(\gamma)\oplus X_m^0(\gamma)$，$0\leqslant i\leqslant 255$ 也遍历 256 个无序的状态，记为 $\{\Delta X_m^0(\gamma),\Delta X_m^1(\gamma),\cdots,\Delta X_m^{255}(\gamma)\}$。

由于 3D 密码算法轮密钥加，行移位和列混合变换都是线性变换，故由第 m 轮 γ 变换后的差分值 $\{\Delta X_m^0(\gamma),\Delta X_m^1(\gamma),\cdots,\Delta X_m^{255}(\gamma)\}$ 可以得到第 $m+1$ 轮密钥加后的差分值：

$$\{\Delta X_{m+1}^0(IN),\Delta X_{m+1}^1(IN),\cdots,\Delta X_{m+1}^{255}(IN)\}$$

因为 δ-集的第 0 个字节是活动字节，经过行移位、列混合和轮密钥加变换后，这些差分值 $\{\Delta X_{m+1}^0(IN),\Delta X_{m+1}^1(IN),\cdots,\Delta X_{m+1}^{255}(IN)\}$ 的活动字节扩散到第 0、1、2、3 字节，其他字节仍是非活动字节。由于 $X_{m+1}^0(IN)$ 的第 0、1、2、3 字节作为参数的一部分给出，则可以得到 $\{X_{m+1}^0(IN),\ X_{m+1}^1(IN),\cdots,X_{m+1}^{255}(IN)\}$ 的第 0、1、2、3 字节的值，经 γ 变换后得到 $\{X_{m+1}^0(\gamma),X_{m+1}^1(\gamma),\cdots,X_{m+1}^{255}(\gamma)\}$ 的第 0, 1, 2, 3 字节值。其他非活动字节差分值为 0，且有 $\Delta X_{m+1}^0(\gamma)=X_{m+1}^0(\gamma)\oplus X_{m+1}^0(\gamma)=0$。由此可得第 $m+1$ 轮 γ 变换后的差分值

$$\{\Delta X_{m+1}^0(\gamma),\Delta X_{m+1}^1(\gamma),\cdots,\Delta X_{m+1}^{255}(\gamma)\}$$

同上推导，由于 $X_{m+2}^0(IN)$ 的 16 字节值、$X_{m+3}^0(IN)$ 全部 64 字节值和 $X_{m+4}^0(IN)$ 的 16 字节值也作为参数的一部分给出，所以可得第 $m+4$ 轮 γ 变换后的差分值

$$\{\Delta X_{m+4}^0(\gamma),\Delta X_{m+4}^1(\gamma),\cdots,\Delta X_{m+4}^{255}(\gamma)\}$$

经过行移位、列混合和轮密钥加变换后，得到第 $m+5$ 轮 γ 变换前的差分值

$$\{\Delta X_{m+5}^0(IN),\Delta X_{m+5}^1(IN),\cdots,\Delta X_{m+5}^{255}(IN)\}$$

由于 $X_{m+5}^0(IN)$ 的第 0、17、34、51 字节作为参数的一部分给出，所以可以得到 $\{X_{m+5}^0(IN),X_{m+5}^1(IN),\cdots,X_{m+5}^{255}(IN)\}$ 和 γ 变换后的这 4 个字节值。由此可得第 $m+5$ 轮 γ 变换后的差分值

$$\{\Delta X_{m+5}^0(\gamma),\Delta X_{m+5}^1(\gamma),\cdots,\Delta X_{m+5}^{255}(\gamma)\}$$

经过行移位、列混合变换后可以得到多重集 $\{\Delta X_{m+6,0}^0,\Delta X_{m+6,0}^1,\cdots,\Delta X_{m+6,0}^{255}\}$ 的值。

从上面的分析过程可以看出，多重集 $\{\Delta X_{m+6,0}^0,\Delta X_{m+6,0}^1,\cdots,\Delta X_{m+6,0}^{255}\}$ 由 104 个字节变量决定。

证毕。

当活动字节为第 0 个字节，对应δ-集为$\{X_3^0, X_3^1,\cdots,X_3^{255}\}$，对$\delta$-集进行 6 轮 3D 算法的加密，即性质 1 取 m=3，$n=0$时，得到以下结果。

性质 2　用 6 轮 3D 密码算法加密δ-集$\{X_3^0, X_3^1,\cdots,X_3^{255}\}$，多重集$\{\Delta X_{9,0}^0,\Delta X_{9,0}^1,\cdots,\Delta X_{9,0}^{255}\}$完全由下面 104 个字节变量决定。

1) 状态$X_4^0(IN)$的第 0、1、2、3 字节；

2) 状态$X_5^0(IN)$的第 0、1、2、3、16、17、18、19、32、33、34、35、48、49、50、51 字节；

3) 状态$X_6^0(IN)$的全部字节；

4) 状态$X_7^0(IN)$的第 0、5、10、15、16、21、26、31、32、37、42、47、48、53、58、63 字节；

5) 状态$X_8^0(IN)$的第 0、17、34、51 字节。

如果攻击过程中涉及的多重集参数多，那么多重集的预计算复杂度是巨大的，为了减少预计算的存储量，有如下性质。

性质 3　(多重集的存储)[12]多重集的元素可以重复出现，任给一个含有 256 个字节的重集，其所有可能的取值数量为$2^{506.17}$，而存储这些可能的多重集仅需要 512 bit。

证明　对于任给的多重集 M，M中的每个元素出现的次数不止一个，记为$M=\{x_1^{\infty},x_2^{\infty},\cdots,x_{2^8}^{\infty}\}$。多重集 M 上一个无序的 256 个字节的重集，记为$M^*=\{x_1^{n_1},x_2^{n_2},\cdots,x_m^{n_m}\}$，其中$\sum_{i=1}^{m}n_i=256$，$M^*$所有取值的个数相当于 M上的一个 256-组合。利用组合数学的已有结论，一个含有 256 个字节的重集所有取值的个数约为$\binom{2^8+2^8-1}{2^8}\approx 2^{506.17}$。

下面考虑多重集的存储，M^*的序列可以表示成如下形式

$$\underbrace{x_1x_1\cdots x_1}_{n_1}\mid\underbrace{x_2x_2\cdots x_2}_{n_2}\mid\cdots\mid\underbrace{x_mx_m\cdots x_m}_{n_m}$$

考虑M^*的缩减集合$S=\{x_1,x_2,\cdots,x_m\}$，S 至多有 256 个元素，不妨按从小到大的顺序排列，即$x_{i+1}\geqslant x_i$ $(i=1,2,\cdots,255)$。设 256 bit 的元素组$e_0=(0,0,\cdots,0),\cdots,e_{255}=(1,1,\cdots,1)$，其中，$e_i\in F_{2^8}$ $(i=0,1,\cdots,255)$，则缩减集合$S=\{x_1,x_2,\cdots,x_m\}$的元素$x_1,x_2,\cdots,x_m$可以用$(e_0,e_1,\cdots,e_{255})$以 0 或者 1 对应表出，用 256 bit 存储这些表出的系数。接下来考虑重数$\{n_1,n_2,\cdots,n_m\}$的存储。设$(\xi_1,\xi_2,\cdots,\xi_{256})$对应$(1,2,\cdots,256)$这 256 个数值，递增序列$\{n_1,n_1+n_2,n_1+n_2+n_3,\cdots,\sum_{j=1}^{m}n_j\}$的元素可以用$(\xi_1,\xi_2,\cdots,\xi_{256})$以 0 或者 1 对应表出，而$\{n_1,n_2,\cdots,n_m\}$与$\{n_1,n_1+n_2,n_1+n_2+n_3,\cdots,\sum_{j=1}^{m}n_j\}$一一对应，则可以用另外的 256 bit 存储表出的系数。所以仅需要 512 bit 来存储这些可能的多重集。

证毕。

基于 6 轮多重集构造的 3D 密码中间相遇区分器，涉及的参数较多，不能实现有效的攻击。为了精简参数个数，分析 3D 算法 S 盒，有以下结果。

性质 4　(S 盒的性质)[12]对于 3D 算法的 S 盒，与 AES 相同，给定大量 S 盒的非零输入差分Δ_i和输出差分Δ_0，等式

$$S(x)+S(x+\Delta_i)=\Delta_0 \tag{6}$$

平均有一个解。

性质 2 得到的 6 轮多重集由 104 个字节变量决定，在此截断差分路径的基础上，利用性质 4，通过有效的枚举技术，剔除中间重复计算的参数，构造新的 6 轮中间相遇区分器，如图 1 所示。图 1 中区分器变量参数减少到 42 个字节，实现了预计算复杂度的大幅度减少。

性质 5　(新的 6 轮中间相遇区分器)用 6 轮 3D 密码算法加密δ-集$\{X_3^0,X_3^1,\cdots,X_3^{255}\}$，多重集$\{\Delta X_{9,0}^0,\Delta X_{9,0}^1,\cdots,\Delta X_{9,0}^{255}\}$完全由以下 42 个字节变量决定：

1) $\Delta z_3[0]$；

2) $x_4[0,1,2,3]$；

3) $x_5[0,1,2,3,16,17,18,19,32,33,34,35,48,49,50,51]$；

4) $z_7[0,1,2,3,16,17,18,19,32,33,34,35,48,49,50,51]$；

5) $z_8[0,1,2,3]$；

6) $\Delta w_8[0]$。

注：Δz是行移位(θ_1,θ_2)后的差分，Δw是列混合(π)变换后的差分。

证明　只需证明，通过图 1 状态中上述 42 个字节可以求出性质 2 中决定 6 轮多重集的 104 个变量。由给出的$\Delta z_3[0]$，通过线性运算列混合和密钥加可以得到图 1 差分值非 0 的$\Delta x_4[0,1,2,3]$。已知$x_4[0,1,2,3]$这 4 个字节值，经过 S 盒置换可以计算出Δy_4。再经过行移位、列混合和密钥加可以得到图 1 中Δx_5差分值非 0 的 16 个字节值。已知$x_5[0,1,2,3,16,17,18,19,32,33,34,35,48,49,50,51]$，计算出经过 S 盒后的差分值$\Delta y_5$，再经过线性变化后

可以得到 Δx_6。

反过来，从图 1 的解密方向，同样由给出的 $\Delta w_8[0]$、$z_8[0,1,2,3]$ 这些字节可以得到 $x_8[0,17,34,51]$。再由 $z_7[0,1,2,3,16,17,18,19,32,33,34,35,48,49,50,51]$ 这些字节，可以得到 $x_7[0,5,10,15,16,21,26,31,32,37,42,47,48,53,58,63]$ 和 Δy_6 的值。现在由性质 4，知道 S 盒的输入差分 Δx_6 与输出差分 Δy_6，平均可以得到一个 x_6 的全部字节值。所以决定性质 2 中 6 轮多重集的 104 个字节变量可以由性质 5 这 42 个字节求出。

证毕。

4 11 轮 3D 密码算法的中间相遇攻击

本节利用构造的新的 6 轮中间相遇区分器作为 3~8 轮，前面加 2 轮，后面加 3 轮，并且交换第 9 与第 10 轮的轮密钥加 k_i 与列混合操作 $\pi_i(9\leqslant i\leqslant 10)$ 的次序，构成 11 轮的攻击路径。首先给出 11 轮 3D 算法的基本中间相遇攻击，时间复杂度主要集中在选择满足截断差分路径的明文上。接着通过时空折中，增加选择明文的活动字节个数和改变活动字节的位置，给出改进的中间相遇攻击，降低了数据复杂度。

4.1 11 轮 3D 算法的基本中间相遇攻击

为了使第 3 轮的输入和第 8 轮的输出状态符合性质 5 中间相遇区分器的输入和输出，11 轮中间相遇路线需要以概率实现，具体攻击路径如图 2 所示。

1) $*$ 为固定字节，不同的位置不一定相等。

2) $w_i(i=0,5,10,15,16,21,26,31,32,37,42,47,48,53,58,63)$，$\tau_j(j=0,1,2,3,16,17,18,19,32,33,34,35,48,49,50,51)$，$\sigma_0$，$\sigma_{17},\sigma_{34},\sigma_{51},\rho_0,\rho_1$，$\rho_2,\rho_3$ 取遍 0 到 255 所有值。

3) $E_i(i=0,7,10,13,16,23,26,29,32,39,42,45,48,55,58,61)$，$D_0,D_{19},D_{34},D_{49},C_0,C_{19},C_{34},C_{49},B_0,A_0$ 为解密中所需涉及的部分字节。

具体攻击步骤可以分为预计算和密钥恢复过程。首先穷举构造中间相遇区分器所需的参数，与多重集的所有可能取值构成映射，并以多重集的取值为索引存储到一个散列表中；然后选择并加密满足特殊形式的明文集得到密文集，穷举涉及到的轮子密钥，对密文进行部分解密，检验解密所得的值是否在预计算生成的散列表中。如果是，猜测的密钥极有可能是正确密钥值。

4.1.1 预计算阶段

定义一个明文空间结构 P，满足在字节 $(0,5,10,15,16,21,26,31,32,37,42,47,48,53,58,63)$ 取遍所有值，其余字节取固定值，并且满足图 2 的攻击路径，进行选择明文攻击，其中，第 3~8 轮为 11 轮 3D 算法中间相遇攻击的预计算阶段。

穷举性质 5 区分器中 42 个字节 2^{336} 个所有可能的取值，求出 6 轮多重集 104 个参数的值。根据所求得 104 个参数，求出 $\{\Delta X_{9,0}^0,\Delta X_{9,0}^1,\cdots,\Delta X_{9,0}^{255}\}$ 并存储在散列表中。由 3D 算法 S 盒的性质，如果分别给定 2^8-1 个 S 盒非零输入差分以及 2^8-1 个 S 盒非零输出差分，有 $(2^7-1-1)(2^8-1)$ 个输入输出差分使得性质 4 中式(6)解的个数为 2，有 2^8-1 个输入输出差分使式(6)解的个数为 4，则需要预计算的多重集的个数为

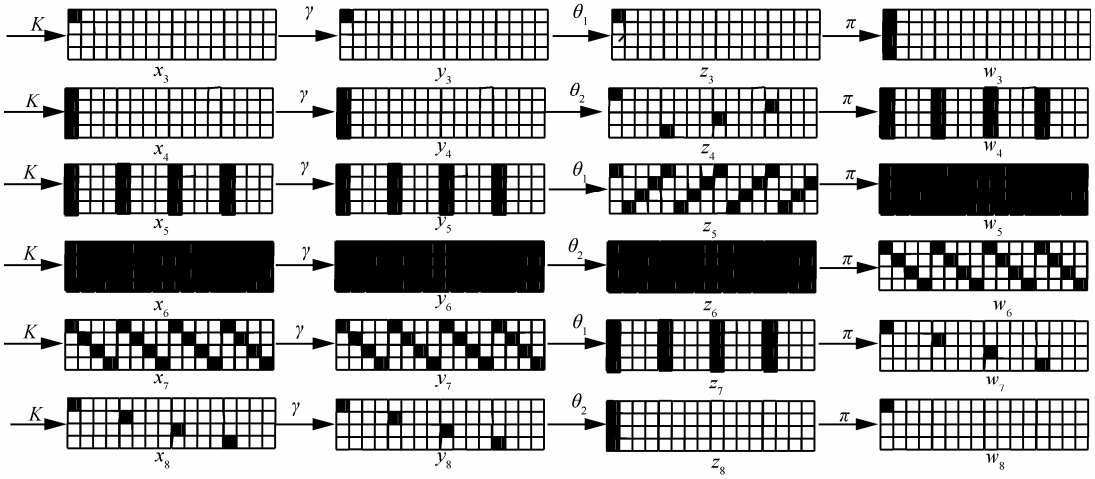

图 1 3D 算法 6 轮中间相遇区分器

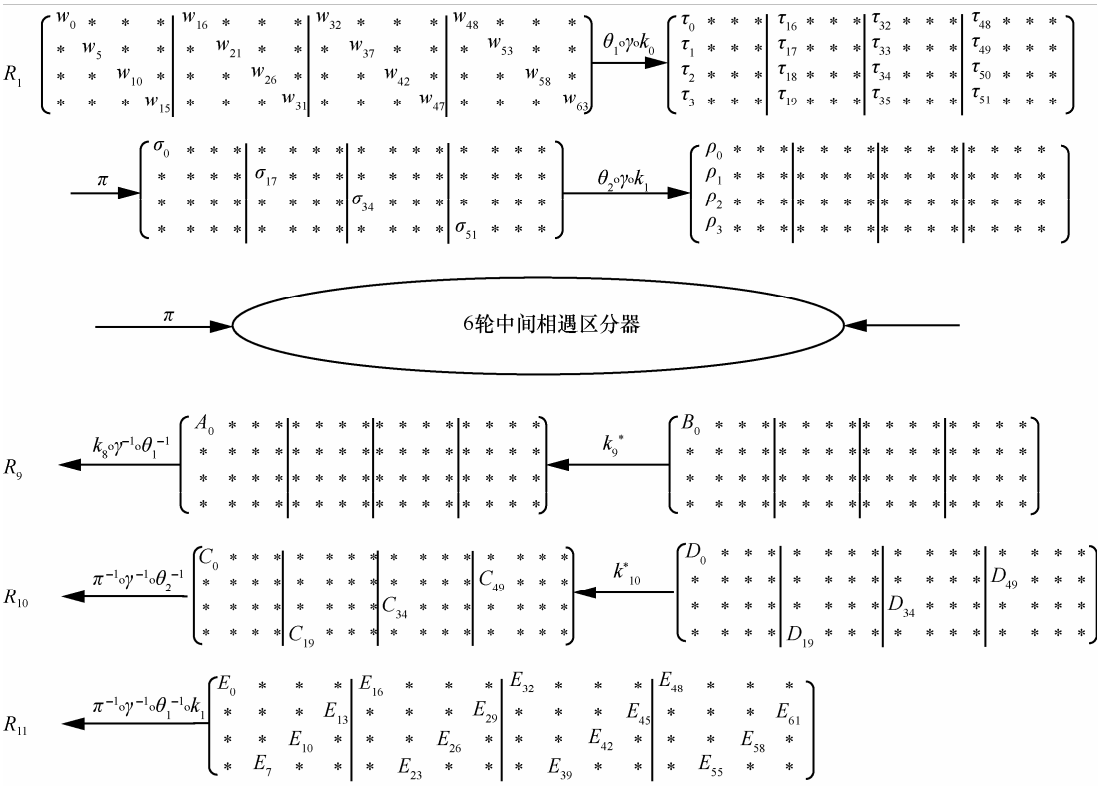

图 2　11 轮 3D 的中间相遇攻击路径

$$2^{336}\left(4\frac{2^8-1}{(2^8-1)^2}+2\frac{(2^8-1)(2^7-1-1)}{(2^8-1)^2}\right)^{64}\approx 2^{336.36}$$

依据性质 3，大约需要 $2^{336.36}$ 个 512 bit 分组长度的存储。为了构建存储的散列表，对 2^8(δ集的个数)个明文进行 $2^{336.36}$ 次部分加密，需要的预计算复杂度约为 $2^{336.36}2^8\frac{1}{2}=2^{343.36}$。

4.1.2　密钥恢复过程

步骤 1　首先猜测密钥 k_0 的 16 个字节(0,5,10, 15, 16,21,26,31,32,37,42,47,48,53,58,63)、k_1 的 4 个字节(0,17,34,51)。对于 $X_{3,0}$ 的 256 个可能值，不妨设 $X_{3,0}^0=0, X_{3,0}^1=1,\cdots,X_{3,0}^{255}=255$，满足定义的$\delta$-集 $=\{X_{3,0}^0,X_{3,0}^1,\cdots,X_{3,0}^{255}\}$。把 $X_{3,0}^i$ 的 256 个值代入下面的状态中，可以得到相应的 $P^0,P^1,\cdots,P^{255}$ 值。

$$\boldsymbol{P}=\begin{pmatrix}p_0&p_4&p_8&p_{12}&p_{16}&p_{20}&p_{24}&p_{28}&p_{32}&p_{36}&p_{40}&p_{44}&p_{48}&p_{52}&p_{56}&p_{60}\\p_1&p_5&p_9&p_{13}&p_{17}&p_{21}&p_{25}&p_{29}&p_{33}&p_{37}&p_{41}&p_{45}&p_{49}&p_{53}&p_{57}&p_{61}\\p_2&p_6&p_{10}&p_{14}&p_{18}&p_{22}&p_{26}&p_{30}&p_{34}&p_{38}&p_{42}&p_{46}&p_{50}&p_{54}&p_{58}&p_{62}\\p_3&p_7&p_{11}&p_{15}&p_{19}&p_{23}&p_{27}&p_{31}&p_{35}&p_{39}&p_{43}&p_{47}&p_{51}&p_{55}&p_{59}&p_{63}\end{pmatrix}$$

其中，

$$p_l=(\gamma^{-1}\theta_1^{-1}\pi^{-1}(\gamma^{-1}\theta_2^{-1}\pi^{-1}(X_{3,0}^i)\oplus k_{1,0}))_l\oplus k_{0,l},\quad l=0,5,10,15 \tag{7}$$

$$p_m=(\gamma^{-1}\theta_1^{-1}\pi^{-1}(\gamma^{-1}\theta_2^{-1}\pi^{-1}(X_{3,0}^i)\oplus k_{1,17}))_m\oplus k_{0,m},\quad m=16,21,26,31 \tag{8}$$

$$p_n=(\gamma^{-1}\theta_1^{-1}\pi^{-1}(\gamma^{-1}\theta_2^{-1}\pi^{-1}(X_{3,0}^i)\oplus k_{1,34}))_n\oplus k_{0,n},\quad n=32,37,42,47 \tag{9}$$

$$p_j=(\gamma^{-1}\theta_1^{-1}\pi^{-1}(\gamma^{-1}\theta_2^{-1}\pi^{-1}(X_{3,0}^i)\oplus k_{1,51}))_j\oplus k_{0,j},\quad j=48,53,58,63 \tag{10}$$

其他位置的 p_i 取常数，这样就得到了选择明文的形式。

然后猜测密钥 k_{10}^* 的 4 个字节(0,19,34,49)和 k_{11} 的 16 个字节(0,7,10,13,16,23,26,29,32,39,42,45,48,55, 58,61)及 k_9^* 的第 0 字节的值，利用猜测的这 21 个字节部分解密 $P^0,P^1,\cdots P^{255}$ 对应的密文，得到第 9 轮第 0

个字节的值，进而得到多重集$\{\Delta X_{9,0}^0,\Delta X_{9,0}^1,\cdots,\Delta X_{9,0}^{255}\}$的值。

步骤 2 检测计算出来的值是否在预计算散列表，如果匹配成功就恢复出相关的子密钥。通过猜测步骤 1 中 41 个密钥字节，可以得到$(2^8)^{41}=2^{328}$个可能值。由性质 3 可知，一个多重集共有$2^{506.17}$种取值，则一个错误密钥匹配成功的概率为$2^{328}2^{-506.17}=2^{-178.17}\approx 0$。因此，如果存在一个碰撞，就认为其所涉及到的轮子密钥是正确密钥。

4.1.3 11 轮基本攻击的复杂度分析

为了保证找到 1 对明文满足图 2 中整个 11 轮的攻击路径，首先由图 2 的明文和密文状态只有 16 个活动字节，对于 4.1.1 节定义的明文空间P，有$2^{128}\frac{(2^{128}-1)}{2}\approx 2^{255}$对满足明文的差分状态，对应的密文结构$C$只有$2^{255}2^{-48\times 8}=2^{-129}$满足截断差分的密文状态，则需要$2^{129}$种明文结构 P 可以保证其中 1 对满足截断差分路径的明密文状态，这样共需$2^{129}2^{128}=2^{257}$种可能的明文。其次由于第 1 轮、第 2 轮和第 9 轮、第 10 轮中，扩散层操作均以概率成立，所以需要增加选择明文量。第 1 轮和第 10 轮扩散层操作成立的概率为2^{-96}，第 2 轮和第 9 轮扩散层操作成立的概率为2^{-24}，整个截断差分路径成立的概率为$2^{-(96+24+96+24)}=2^{-240}$，通过重复选择$2^{240}$次上述明文结构$P$，就可以保证有 1 对明文满足整个 11 轮的截断差分路径。所以一共需要选择明文量为$2^{240}2^{257}=2^{497}$。

在密钥恢复阶段，4.1.2 节步骤 1 需要猜k_0、k_{11}的 16 个字节，k_1、k_{10}^*的 4 个字节和k_9^* [0]的所有值。事实上，对于k_0的2^{128}种所有取值，经过列混合变化后影响的活动字节只有 4 个$(\sigma_0,\sigma_{17},\sigma_{34},\sigma_{51})$，则$k_0$只有$2^{128}2^{-96}=2^{32}$种可能值符合截断路径。同样，对于$k_1$、$k_{10}^*$和$k_{11}$经过列混合变化后影响的活动字节分别只有 1 个、1 个和 4 个，则涉及到轮子密钥总共的取值为$2^{8(4+1+1+1+4)}=2^{88}$。

对于时间复杂度，首先加密2^{497}个选择明文，需要2^{497}次 11 轮 3D 加密，然后恢复密钥时，对找到的2^{240}个明文结构，由构造出来的δ集计算出多重集的值，需要相关轮子密钥的数据量是2^{88}，涉及 64 个字节的其中 1 个字节，约$\frac{1}{2}$的 11 轮加解密，所以时间复杂度为$2^{240}2^8 2^{88}2^{-6}2^{-1}=2^{329}$次 11 轮加密。

综上可知，11 轮基本中间相遇攻击需要的明文量为2^{497}个选择明文，预计算复杂度约为$2^{343.36}$次 11 轮 3D 加密运算，时间复杂度约为2^{329}次 11 轮 3D 加密运算。

4.2 改进的 11 轮 3D 密码算法的中间相遇攻击

4.1 节对 11 轮 3D 密码攻击的时间复杂度集中在选择满足截断差分路径的明文上。通过时空折中，首先增加选择明文活动字节的个数，接着改变活动字节的位置给出 2 种改进的中间相遇攻击，降低了数据复杂度。

将图 1 中 6 轮截断差分路径x_3状态的活动字节增加 1 个，经过行移位和列混合后活动字节都扩散到第 1 列，具体如图 3 所示。

活动字节数随轮数的变化序列为

$$32\xrightarrow{R_1}8\xrightarrow{R_2}2\xrightarrow{R_3}4\xrightarrow{R_4}$$
$$16\xrightarrow{R_5}64\xrightarrow{R_6}16\xrightarrow{R_7}4\xrightarrow{R_8}$$
$$1\xrightarrow{R_9}4\xrightarrow{R_{10}}16\xrightarrow{R_{11}}16$$

根据活动字节的变化，在图 3 的 6 轮截断差分路径前面加 2 轮，后面加 3 轮得到 11 轮 3D 密码改进的中间相遇攻击路径，如图 4 所示。

1) ＊为固定字节，不同的位置不一定相等。

2) $w_i(i=0,2,5,7,8,10,13,15,16,18,21,23,24,26,29,31,32,34,37,39,40,42,45,\ 47,48,50,53,55,56,58,61,63)$，$\tau_j(j=0,1,2,3,8,9,10,11,16,17,18,19,24,25,26,27,32,\ 33,34,35,40,41,42,43,48,49,50,51,56,\ 57,58,59)$，$\sigma_i(i=0,8,17,25,34,42,51,59)$，$\rho_j(j=0,\ 1,2,3,8,9,10,11)$均取遍 0 到 255 所有值。

3) $E_i(i=0,7,10,13,16,23,26,29,32,39,42,45,48,55,58,61)$，$D_0$，$D_{19}$，$D_{34}$，$D_{49}$，$C_0$，$C_{19}$，$C_{34}$，$C_{49}$，$B_0$，$A_0$为解密中所需涉及的部分字节。

满足图 4 截断差分路径的明文状态的明文空间P有$2^{32\times 8}=2^{256}$种可能的取值，对应的密文结构C有$2^{256}\frac{(2^{256}-1)}{2}\approx 2^{511}$对，有$2^{511}2^{-384}=2^{127}$满足截断差分路径的密文状态。此外，排除第 3~8 轮，第 1、2 轮扩散层操作成立的概率分别为$(2^{-24})^8=2^{-192}$和2^{-48}，第 9、10 轮扩散层操作成立的概率为2^{-24}和$(2^{-24})^4=2^{-96}$，整个截断差分路径成立的概率为$2^{-(192+48+24+96)}=2^{-360}$，只需要继续选择$2^{360-127}=2^{233}$次明文结构$P$，就可以保证有 1 对明文满足图 4 中整个 11 轮的攻击路径。一共需要选择明文量$2^{233+256}=2^{489}$，比 4.1 节基本中间相遇攻击的选择明文量降低了2^8个数量级。

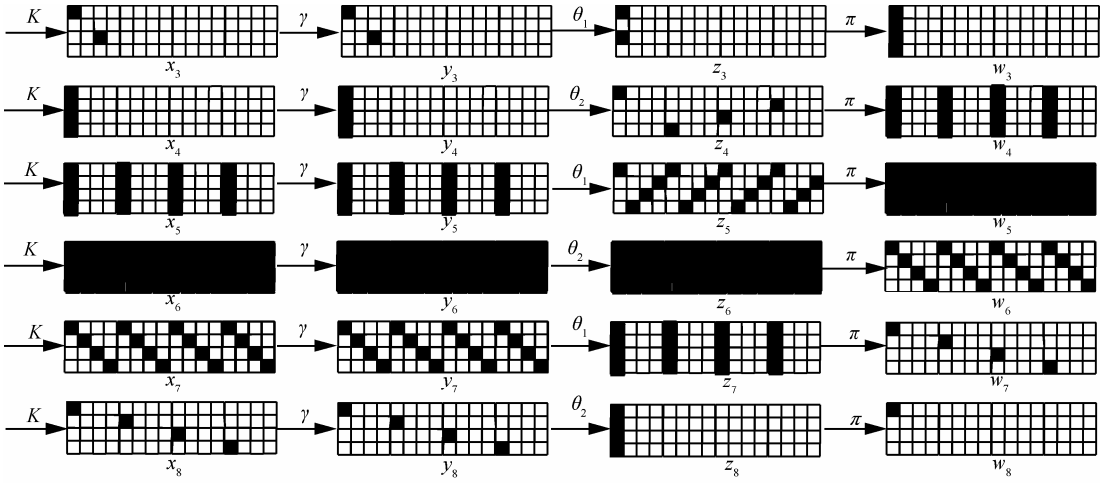

图 3　3D 算法改进的 6 轮中间相遇区分器

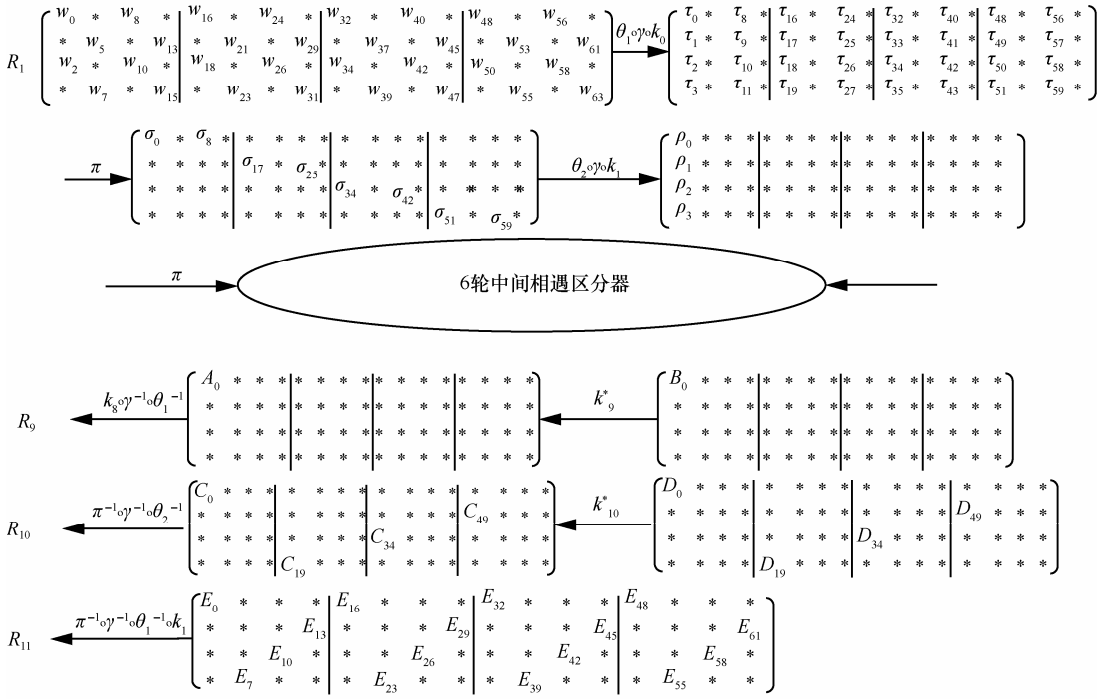

图 4　改进的 11 轮 3D 的中间相遇攻击路径

需要猜测的密钥比 4.1 节多了 20 个字节，但是 k_0 的 32 个字节经过列混合变化后影响的活动字节只有 8 个，同样 k_1 的 8 个字节经过列混合变化后影响的活动字节只有 2 个，则涉及到轮子密钥较 4.1 节多了 5 个，总共的取值为 $2^{8(8+2+1+1+4)}=2^{128}$。

对于时间复杂度，首先加密 2^{489} 个选择明文，需要 2^{489} 次 11 轮 3D 加密。接着需要恢复密钥，对改进的攻击，通过构造的 δ 集计算多重集的值时，图 3 中 6 轮截断差分路径输入状态 x_3 有 2 个活动字节，有 $2^{16}\dfrac{(2^{16}-1)}{2}$ 种差分结构，而 6 轮加密后对应的输出状态 w_8 只有 1 个活动字节，有 $2^8\dfrac{(2^8-1)}{2}$ 种差分结构，所以对于找到的 2^{360} 个明文结构，恢复密钥需要时间复杂度约为 $2^{360-16}2^{8\cdot 2}2^{128}2^{-6}\ 2^{-1}=2^{481}$ 次 11 轮加密。

对于存储复杂度，需要穷举 42+1=43 个字节的取值，求出多重集 104 个参数所有可能的值。需要存储较 4.1 节增加 2^8 个数量级，为 $2^{336.36+8}=2^{344.36}$ 个 512 bit 分组长度的存储。

进一步注意到，第 3 节构造的 6 轮中间相遇区分器是关于输入第 0 个字节到输出第 0 个字节的映

射关系。在攻击路径的选择中，改变输入输出活动字节的位置，中间相遇的性质不会发生改变。对于图 4 中 11 轮中间相遇路径第 3~8 轮，第 3 轮的输入活动字节的位置可以取为(0,10)，(1,11)，(2,8)，(3,9)，同样第 8 轮输出的活动字节可以取 3D 状态表示矩阵中第 1 块 16 个字节的任意位置。通过这样的处理，适当增加了散列表的存储规模，可以进一步减少选择明文量。此时，需要建立 4·16=64 个原有的存储表，存储复杂度增加 2^6 个数量级，为 $2^{350.36}$ 个 512 分组长度的存储，但是选择明文量减少到 2^{483}，降低了 2^6 个数量级。

5 10 轮 3D 密码算法的中间相遇攻击

本节在性质 5 的 6 轮中间相遇区分器基础上，前面加 1 轮，后面加 2 轮，交换第 8 和第 9 轮的轮密钥加与列混合操作的次序得到 10 轮 3D 中间相遇攻击的路径。第 1 轮、第 8 轮扩散层操作成立的概率为 2^{-24}，第 9 轮扩散层操作成立的概率为 2^{-96}，并且满足第 10 轮密文状态的概率为 $\frac{2^{16\cdot 8}}{2^{64\cdot 8}}=2^{-384}$。具体如图 5 所示。

1) $*$ 为固定字节，不同的位置不一定相等。

2) $w_i(i=0,5,10,15)$，$\tau_j(j=0,1,2,3)$ 取遍 0 到 255 所有值。

3) $E_i(i=0,4,8,12,19,23,27,31,34,38,42,46,49,53,57,61)$，$D_0, D_7, D_{10}, D_{13}, C_0, C_7, C_{10}, C_{13}, B_0, A_0$ 为解密中所需涉及的部分字节。

利用 4.1 节的攻击方法，通过定义满足图 5 截断差分路径的明文空间结构 P，进行选择明文攻击，预计算阶段和密钥恢复与 11 轮攻击过程类似。

10 轮中间相遇复杂度的计算。

1) 预计算阶段需要的存储不变，为 $2^{336.36}$ 个 512 bit 分组长度的存储，预计算复杂度为 $2^{343.36}$。

2) 满足明文差分状态的明文空间 P 有 2^{32} 种可能的取值，对应的密文结构 C 有 $2^{32}(2^{32}-1)/2\approx 2^{63}$ 对，只有 $2^{63}2^{-384}=2^{-321}$ 满足截断差分路径的密文状态。此外第 1 轮、第 8 轮和第 9 轮截断差分成立的总的概率为 2^{-144}，所以一共需要选择 $2^{321+32}2^{144}=2^{497}$ 明文量，才能保证有 1 对明文满足整个 10 轮的截断差分路径。

3) 需要猜测密钥 k_0、k_9^* 的 4 个字节、k_8^* [0]和 k_{10} 的 16 个字节的可能值。但对于 k_0、k_9^* 和 k_{10} 经过列混合变化后影响的活动字节分别只有 1 个、1 个和 4 个，则涉及到轮子密钥总共的取值只有 $2^{8(1+1+1+4)}=2^{56}$。对于时间复杂度，首先加密 2^{497} 个选择明文，需要 2^{497} 次 10 轮 3D 加密，然后恢复涉及的轮子密钥需要的时间复杂度约为 $2^{144}2^8 2^{56}2^{-6}2^{-1}=2^{201}$ 次 10 轮加密。

6 结束语

本文研究了 3D 算法的中间相遇攻击，首先利用 3D 算法截断差分的性质，构造了 6 轮多重集，但涉及参数个数多，预计算量大。接着利用 3D 算

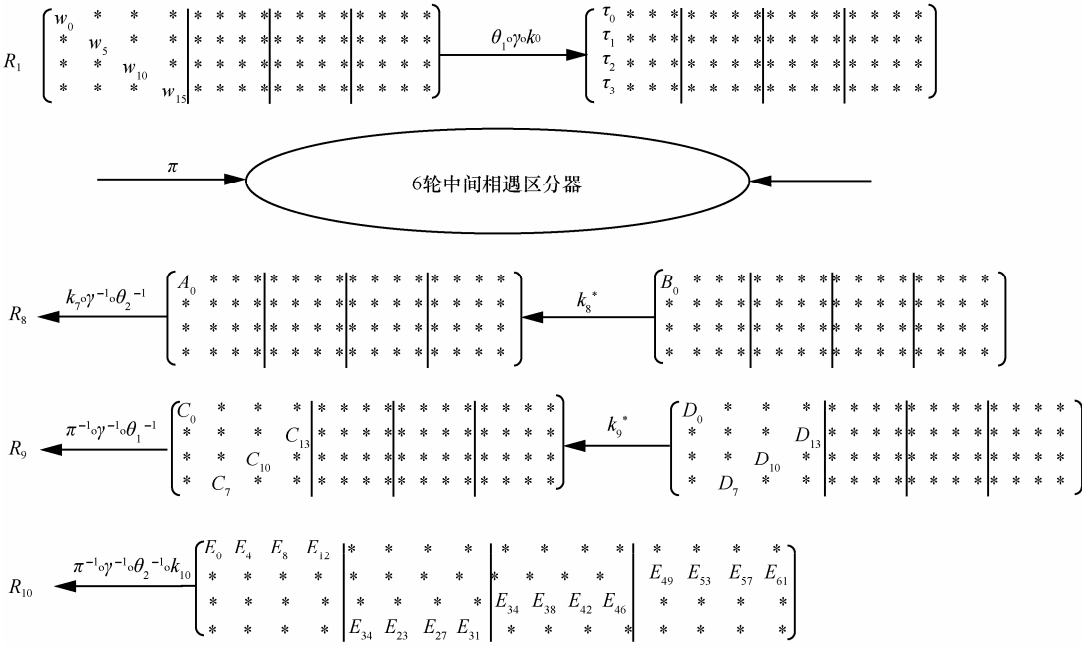

图 5 10 轮中间相遇攻击的路线

法 S 盒的性质和有效的枚举技术，构造了新的中间相遇区分器，将预计算的参数大幅度减少，从而首次实现了对 11 轮 3D 密码的中间相遇攻击，所需时间复杂度为 2^{329}。在此基础上利用时空折中的思想，通过增加活动字节的个数和改变活动字节的位置，给出了 2 个改进数据复杂度的结果。此外，利用新的 6 轮区分器给出了低时间复杂度的 10 轮中间相遇攻击的新结果。表 1 给出了本文与现有 3D 密码攻击结果的比较。

表 1　本文与现有 3D 密码攻击结果的比较

攻击方法	攻击轮数	选择明文量	时间复杂度	存储(分组长度)	相关文献
积分攻击	7	2^{35}	2^{96}	—	文献[2]
积分攻击	8	2^{131}	2^{189}	—	文献[2]
积分攻击	9	2^{133}	2^{414}	—	文献[2]
不可能差分	7	2^{126}	2^{52}	2^{32}	文献[3]
不可能差分	8	2^{317}	2^{345}	2^{256}	文献[3]
不可能差分	9	2^{445}	2^{473}	2^{384}	文献[3]
不可能差分	10	2^{501}	2^{464}	2^{311}	文献[4]
不可能差分	11	2^{493}	$2^{511.2}$	2^{388}	文献[7]
中间相遇	10	2^{128}	$2^{331.1}$	2^{325}	文献[5]
中间相遇	10	2^{497}	2^{201}	$2^{336.36}$	本文的 5 节
中间相遇	11	2^{497}	2^{329}	$2^{336.36}$	本文的 4.1 节
中间相遇	11	2^{489}	2^{481}	$2^{344.36}$	本文的 4.2 节
中间相遇	11	2^{483}	2^{481}	$2^{350.36}$	本文的 4.2 节

本文对 3D 密码 11 轮中间相遇攻击的结果优于现有的其他攻击结果。本文没有利用 3D 密码的密钥扩展，如何结合密钥算法构造较长轮数的中间相遇区分器，并结合其他攻击方法减少复杂度并增加成功的概率将是值得进一步研究的工作。

参考文献：

[1] NAKAHARA J J. 3D: a three-dimensional block cipher[A]. Cryptology and Network Security-CANS 2008[C]. Hongkong, China, 2008. 252-267.

[2] 王美一, 唐学海, 李超等. 3D 密码的 Square 攻击[J]. 电子与信息学报, 2010, 32(1): 157-161.
WANG M Y, TANG X H, LI C, *et al*. Square attacks on 3D cipher[J]. Journal of Electronics & Information Technology, 2010, 32(1): 157-161.

[3] 唐学海, 李超, 王美一. 3D 密码的不可能差分攻击[J]. 电子与信息学报, 2010, 32(10): 2516-2520.
TANG X H, LI C, WANG M Y, *et al*. Impossible differential attack on 3D cipher[J]. Journal of Electronics & Information Technology, 2010, 32(10): 2516 - 2520.

[4] NAKAHARA J J. New impossible differential and known-key distinguishers for the 3D cipher[A]. Information Security Practice and Experience-ISPEC 2011[C]. Guangzhou, China, 2011. 208-221.

[5] 苏崇茂, 韦永壮, 马春波. 10 轮 3D 分组密码算法的中间相遇攻击[J]. 电子与信息学报, 2012, 34(3): 694-697.
SU C M, WEI Y Z, MA C B. Meet-in-the-middle attack on 10-round reduced 3D block cipher[J]. Journal of Electronics & Information Technology, 2012, 34(3): 694- 697.

[6] TAKUMA K, WANG L, SASAKI Y. New truncated differential cryptanalysis on 3D block cipher[A]. Information Security Practice and Experience–ISPEC 2012[C]. Hangzhou, China, 2012. 109-125.

[7] 谢作敏, 陈少真, 鲁林真. 11 轮 3D 密码的不可能差分攻击[J]. 电子与信息学报, 2014, 36(5): 1215-1220.
XIE Z M, CHEN S Z, LU L Z. Meet-in-the-middle attack on 10-round reduced 3D block cipher[J]. Journal of Electronics & Information Technology, 2014, 36(5): 1215-1220.

[8] GILBERT H, MINIER M. A collision attack on 7 rounds of Rijndael[A]. Proceedings of the Third AES Candidate Conference[C]. New York, USA, 2000.

[9] HUSEVIN D, AYDIN S. A meet-in-the-middle attack on 8-round AES[A]. Fast Software Encryption–FSE 2008[C]. Lausanne, Switzerland, 2008.116-126.

[10] DEMIRCI H, TASKIN I, COBAN M. Improved meet-in-the-middle attacks on AES[A]. Advances in Cryptology– INDOCRYPT 2009[C]. New Dehli, India, 2009. 144-156.

[11] DUNKELMAN O, KELLER N, SHAMIR A. Improved single-key attacks on 8-round AES-192 and AES-256[A]. Advances in Cryptology-ASIACRYPT 2010[C]. 2010. 158-176.

[12] PATRICK D, PIERRE F, JEREMY J. Improved key recovery attacks on reduced-round AES in the single-key setting[A]. Advances in Cryptology-EUROCRYPT 2013[C]. Athens, Greece, 2013. 371-387.

作者简介：

任炯炯（1994-），男，甘肃天水人，信息工程大学硕士生，主要研究方向为密码学与信息安全。

陈少真（1967-），女，河南郑州人，信息工程大学教授，主要研究方向为密码学与信息安全。