即可.

为便于区分器的分类,不妨以状态 z_1 为初始输入状态,按加密过程和解密过程,证明分为第 2.1 节与第 2.2 节两部分.

2.1 Midori算法加密过程差分路径

引理 2.1. 初始输入状态 z_1 只在某一列存在差分活动的比特块时,经过 3.5 轮 Midori 算法加密后,输出状态 w_4 的每个比特块都可能差分活动.

为证明该引理,分别讨论初始输入状态 z_1 只在某一列存在 1 个差分活动、2 个差分活动、3 个差分活动、4 个差分活动比特块这 4 种情况.本文中如不加特殊说明,我们考虑的初始状态 z_1 其差分活动比特块的差分值都是相同的,这是因为差分值不同先于差分值相同的情况输出每个比特块都可能差分活动的状态.由于 *KeyAdd* 不改变原状态截断差分活动位置,为表述简洁,性质 2.1~性质 2.4 中都省去了最后 1/4 轮.

性质 2.1. 初始输入状态 z_1 只存在 1 个差分活动比特块时,经过 2.5 轮 Midori 算法加密后,输出状态 w_3 的每个比特块都可能差分活动.

证明:设 z_1 唯一的差分活动比特块在第 i 列,其中,$0\leqslant i\leqslant 3$.z_1 经 3/4 轮 Midori 算法加密后,非线性变换 *SB* 输出状态 y_2 必定仅在第 i 列有 3 个比特块差分活动.以 z_1 仅在第 6 个比特块有差分活动为例,给出其 2.5 轮 Midori 算法加密过程,如图 3 所示,其中,白色表示差分为 0 的半字节,黑色表示差分活动的半字节,斜线表示可能存在差分的半字节.

由性质 1.5 可知,y_2 经一轮 Midori 算法加密后,再经 *SC*,输出状态 z_3 必定其中 3 列有两个比特块差分活动,一列有 3 个比特块差分活动.z_3 再经 *MC*,输出状态 w_3 的每个比特块都可能差分活动.证毕. □

性质 2.2. 初始输入状态 z_1 只在某一列存在 2 个比特块差分活动时,经过 3.5 轮 Midori 算法加密后,输出状态 w_4 的每个比特块都可能差分活动.

证明:z_1 经 3/4 轮 Midori 算法加密后,输出状态 y_2 必定仅在某一列有 2 个比特块差分活动,其余列没有比特块差分活动.以 z_1 仅在第 5、第 6 个比特块有差分活动为例,给出其 3.5 轮 Midori 算法加密过程,如图 4 所示.

由性质 1.6 可知,y_2 经一轮 Midori 算法加密后,再经一次 *SC*,输出状态 z_3 必定其中两列各有两个比特块差分活动,其余两列各有一个比特块差分活动.故易知:再经 1.5 轮,输出状态 w_4 不存在确定有无差分活动的比特块.证毕. □

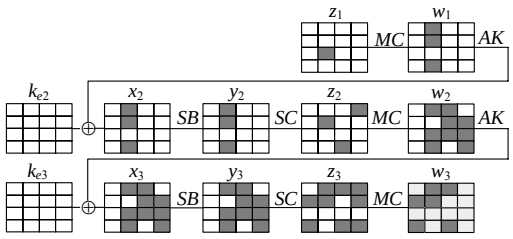

Fig.3 2.5-round differential path of Midori in encryption direction I

图 3 2.5 轮 Midori 算法加密方向差分路径 I

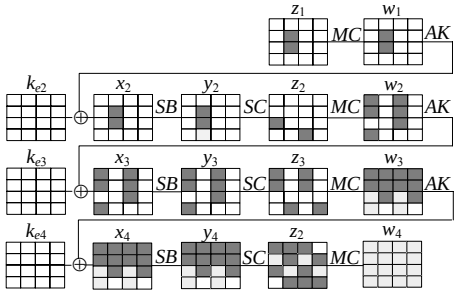

Fig.4 3.5-round differential path of Midori in encryption direction I

图 4 3.5 轮 Midori 算法加密方向差分路径 I

性质 2.3. 初始输入状态 z_1 只在某一列存在 3 个比特块差分活动时,经过 3.5 轮 Midori 算法加密后,输出状态 w_4 的每个比特块都可能差分活动.

证明:z_1 经一轮 Midori 算法加密后,输出状态 z_2 必定只有 1 个比特块差分活动,由性质 2.2 可知,z_2 再经 2.5 轮 Midori 算法加密,输出状态 w_4 的每个比特块都可能存在差分活动.以 z_1 仅在第 5~第 7 个比特块差分活动为例,给出其 3.5 轮 Midori 算法加密过程,如图 5 所示. □

性质 2.4. 初始输入状态 z_1 只在某一列存在 4 个比特块差分活动,经过 3.5 轮 Midori 算法加密后,输出状态 w_3 的每个比特块都可能差分活动.

证明:z_1 经一轮 Midori 算法加密后,输出状态 z_2 必定每一列各有一个比特块差分活动.易知:再经 1.5 轮算法加密,输出状态 w_3 不存在确定有无差分活动的比特块.以 z_1 仅在第 4~第 7 个比特块有差分活动为例,给出其 3.5 轮 Midori 算法加密过程,如图 6 所示. □

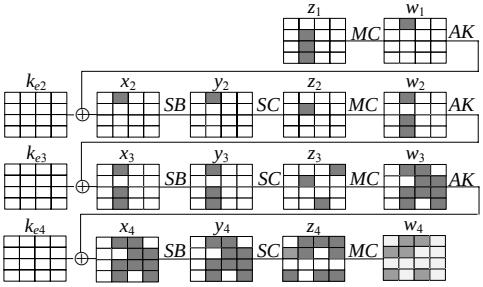

Fig.5 3.5-round differential path of Midori in encryption direction II

图 5 3.5 轮 Midori 算法加密方向差分路径 II

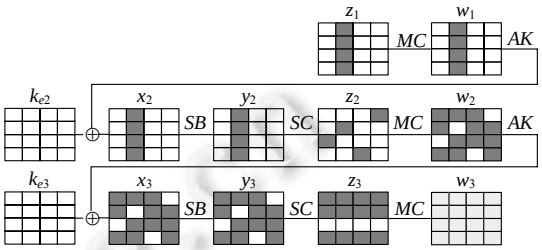

Fig.6 2.5-round differential path of Midori in encryption direction II

图 6 2.5 轮 Midori 算法加密方向差分路径 II

引理 2.2. 假设初始输入状态 z_1 只在某一列存在比特块差分活动时,若经过 n+1/2 轮 Midori 算法后,输出状态 w_{n+1} 的每个比特块都可能差分活动,则任意增加 z_1 中其他差分为零列的差分活动得到状态 z_1',z_1' 经过 n+1/2 轮 Midori 算法后的输出状态 w'_{n+1} 也必定每个比特块都可能差分活动.

证明:由 *SC*,*SB*,*KeyAdd*,*MC* 的性质可知,任意状态,其列与列之间的这 4 种变换是相互独立的.故 z_1 和 z_1' 经相同的变换,z_1' 经变换后,输出状态有差分活动的比特块集合必定包含 z_1 的输出状态有差分活动的比特块集合,所以该结论是显然的. □

由引理 2.1 和引理 2.2 可得出如下定理.

定理 2.1. 任一初始输入状态 z_1 经过 3.5 轮 Midori 算法加密后,输出状态 w_4 的每个比特块都可能差分活动.

2.2 Midori算法解密过程差分路径

引理 2.3. 状态 z_m 只存在 1 个比特块差分活动时,经过 3.5 轮 Midori 解密算法后,输出状态 x_{m-3} 的每个比特块都可能差分活动.

证明:z_m 经一轮 Midori 算法解密后,输出状态 z_{m-1} 必定其中一列有 3 个比特块差分活动,其余列无差分活动比特块.依据性质 1.5,同理可证:再经过 1.5 轮,输出状态 x_{m-2} 必定其中 3 列有两个比特块差分活动,一列有 3 个比特块差分活动.故 x_{m-2} 再经一轮解密算法,输出状态 x_{m-3} 每个比特块都可能差分活动.以 z_m 仅在第 5 个比特块有差分活动为例,给出其 3.5 轮 Midori 算法解密方向差分路径,如图 7 所示. □

引理 2.4. 假设状态 z_m 只存在 1 个比特块差分活动时,若经过 n+1/2 轮 Midori 解密算法后,输出状态 x_{m-n} 的每个比特块都可能差分活动,则任意增加 z_m 上其他比特块的差分得到的状态 z'_m,经过 n+1/2 轮 Midori 解密算法后,输出状态 x'_{m-n} 每个比特块也必定都可能差分活动.

证明:不妨将状态上可能有差分活动的所有比特块用集合 H 表示,例如 z_m 上可能有差分活动的所有个比特块集合用 H_{z_m} 表示,状态 z'_m 上可能有差分活动的所有个比特块用集合 $H_{z'_m}$ 表示,显然有 $H_{z_m} \subset H_{z'_m}$. 由 *SC*,*SB*,*KeyAdd*,*MC* 的性质可知,$H_{y_m} \subset H_{y'_m}$,$H_{x_m} \subset H_{x'_m}$,$H_{w_{m-1}} \subset H_{w'_{m-1}}$,$H_{z_{m-1}} \subset H_{z'_{m-1}}$.故 z_m 和 z'_m 经相同的变换,z'_m 经变换后输出状态有差分活动的比特块集合,必定包含 z_m 经变换后的输出状态有差分活动的比特块集合,所以该结论是成立的. □

由引理 2.3 和引理 2.4 可得出如下定理.

定理 2.2. 任一状态 z_n 经过 3.5 轮 Midori 解密算法后,输出状态 x_{n-3} 的每个比特块都可能差分活动.

再由定理 2.1 和定理 2.2 可得出本文一个重要的结论,如定理 2.3 所示.

定理 2.3. Midori 算法在单密钥条件下的截断不可能差分区分器至多 6 轮.

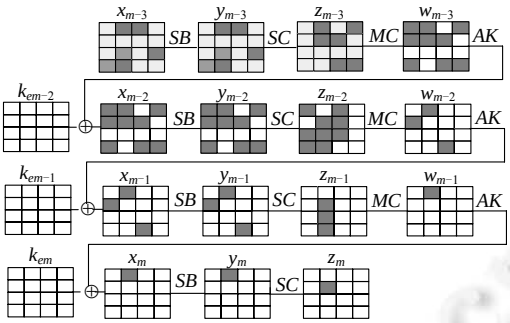

Fig.7 3.5-round differential path of Midori in decryption direction

图 7 3.5 轮 Midori 算法解密方向差分路径

3 Midori 算法 6 轮截断不可能差分区分器的分类

在接下来分类过程中将用到一个概念——列最小差分活动比特块数,其定义如下.

定义 3.1. 设状态 z 各列的差分活动比特块数分别为 $t_{col(0)},t_{col(1)},t_{col(2)},t_{col(3)}$,该状态的列最小差分活动比特块数,是指非零差分列中最小差分活动的比特块数,即 $\min\{t_{col(i)}|t_{col(i)}>0,i=0,1,2,3\}$.

接下来,我们以输入状态 z_1 的列最小差分活动比特块数进行分类讨论如下.

性质 3.1. 输入状态 z_1 的列最小差分活动比特块数为 1 时,不可能构造出 6 轮截断不可能差分区分器.

证明:由性质 2.1 和引理 2.2 可知,此时,输入状态 z_1 经过 2.5 轮 Midori 算法加密后,输出状态 w_3 的每个比特块都可能差分活动;再由定理 2.2 可知,任意状态经 3.5 轮解密算法后,输出状态的每个比特块都可能差分活动,故不可能构造出一条 6 轮截断不可能差分路径. □

性质 3.2. 输入状态 z_1 的列最小差分活动比特块数为 2 时,若要构造一条 6 轮不可能差分路径,输出状态 z_7 必定仅有 1 个比特块差分活动.

证明:要想构造出一条不可能差分路径,由性质 2.2 可知,输入状态 z_1 只能向下加密 2.5 轮,所以输出状态 z_7 要向上解密 3.5 轮,且满足存在确定有无差分活动的比特块,故 z_7 必定仅有 1 个比特块差分活动. □

性质 3.3. 输入状态 z_1 的列最小差分活动比特块数为 3 时,要构造一条 6 轮不可能差分路径,若 z_1 经过 2.5 轮 Midori 算法加密,则输出状态 z_7 必定仅有 1 个比特块差分活动.若输入状态 z_1 经过 3.5 轮 Midori 算法加密,则 z_7 经一次 SC^{-1} 输出状态 y_7 有如下 4 种情形:(1) y_7 只有 1 列有比特块差分活动;(2) y_7 有两列有比特块差分活动,且其中一列差分活动比特块数必定为 1;(3) y_7 有 3 列有比特块差分活动,且其中两列差分活动比特块数必定为 1;(4) y_7 每一列都有比特块差分活动时,且必定有 3 列其差分活动比特块数为 1.

证明:若输入状态 z_1 经过 2.5 轮 Midori 算法加密,输出状态 z_7 必定仅有 1 个比特块差分活动.若输入状态 z_1 经过 3.5 轮 Midori 算法加密,则加密后输出状态 w_4 的每个比特块都可能存在差分活动,则 z_7 必定满足解密 2.5 轮后存在一定没有差分活动的比特块.对于输出状态 z_7 经一次 SC^{-1} 的输出状态 y_7 分如下 4 种情形讨论.

- 情形 1:当 y_7 只有 1 列有比特块差分活动时,显然是满足要求的.
- 情形 2:当 y_7 仅有 2 列有比特块差分活动时,若这两列都有两个以上比特块差分活动,容易推导出 x_5 每个比特块都可能存在差分活动,故不符合要求,所以此时 y_7 必须有一列差分活动比特块数为 1.
- 情形 3:当 y_7 仅在 3 列有比特块差分活动时,若有两列差分活动比特块数超过一个,由情形 2 可知不符合要求,所以 y_7 其中两列差分活动比特块数必定为 1.
- 情形 4:当 y_7 在每一列都有比特块差分活动时,同样由情形 2 可知,有 3 列差分活动比特块数必定为 1.

综上所述,性质 3.3 得证. □

性质 3.4. 输入状态 z_1 列最小差分活动半字节数为 4 时,不可能构造出 6 轮截断不可能差分区分器.

该证明过程同性质 3.1.

综上所述,Midori 算法 6 轮截断不可能差分区分器可分为性质 3.2 与性质 3.3 两大类.由引理 2.2 和引理 2.4 可知,z_1,z_7 仅有 1 列有比特块差分活动的情况下,区分器能向下加密及向上解密更多轮数.故简单考虑 z_1,z_7 仅有 1 列有比特块差分活动的情况,此时按输入状态 z_1 存在的差分活动比特块数将 Midori 算法 6 轮截断不可能差分区分器分为如下两大类.

1) 输入状态 z_1 仅在某一列存在 2 个比特块差分活动时,输出状态 z_7 必定仅有 1 个比特块差分活动.具体不可能差分差分路径为输入状态 z_1 向下加密 2.5 轮,输出状态 z_7 向上解密 3.5 轮.
2) 输入状态 z_1 仅在某一列存在 3 个比特块差分活动时:(1) 若输入状态 z_1 经过 2.5 轮 Midori 算法加密,则输出状态 z_7 必定仅有 1 个比特块差分活动;(2) 若输入状态 z_1 经过 3.5 轮 Midori 算法加密,则输出状态 z_7 必定仅有 1 个或者 2 个比特块差分活动(证明略).

4 Midori-64 算法的不可能差分分析

根据 Midori 算法 6 轮截断不可能差分区分器的分类结果,可构造相应的 6 轮不可能差分区分器.第 4.1 节将给出一个 6 轮不可能差分区分器;第 4.2 节进一步给出 Midori-64 算法的 11 轮不可能差分分析.

4.1 Midori算法的6轮不可能差分区分器

定理 4.1. 当初始输入状态 z_1 仅在第 0~第 2 这 3 个比特块差分活动,且满足$\Delta z_1[0]=\Delta z_1[1]=\Delta z_1[2]$时,经过 6 轮 Midori 算法加密后,输出状态 z_7 仅在第 6、第 7 比特块处差分活动,且满足$\Delta z_1[6]=\Delta z_1[7]$是不可能的.具体形式如图 8 所示.

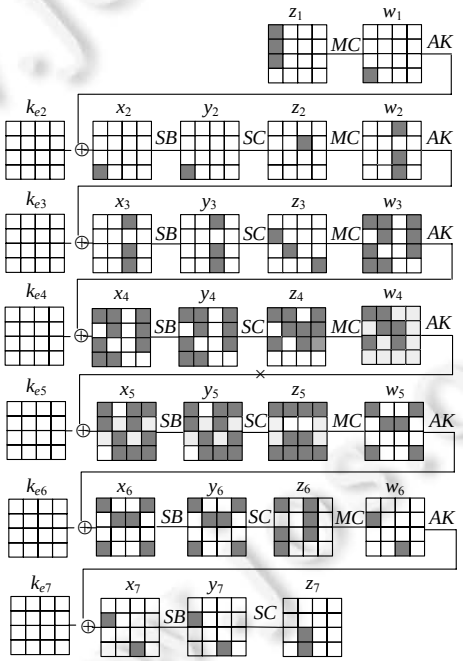

Fig.8 6-round impossible differential distinguisher of Midori

图 8 Midori 算法的 6 轮不可能差分区分器

证明:当输入状态 z_1 仅在第 0~第 2 这 3 个比特块差分活动,且满足$\Delta z_1[0]=\Delta z_1[1]=\Delta z_1[2]$时,经 3.5 轮 Midori 算法加密后,输出状态 w_4 的第 4 比特块必定差分活动;当输出状态 z_7 仅在第 6、第 7 比特块处差分活动,且满足$\Delta z_1[6]=\Delta z_1[7]$时,经 2.5 轮 Midori 算法解密后,输出状态 x_5 的第 4 比特块差分为 0,故产生矛盾,所以结论成立.

证毕. □

4.2 11轮Midori-64算法的不可能差分分析

利用定理 4.1 中给出的 Midori 算法 6 轮不可能差分区分器,向上解密 1.5 轮,向下加密 3.5 轮,给出 11 轮 Midori-64 算法的不可能差分分析结果.攻击过程分为预计算与在线攻击两个阶段.

(一) 在预计算阶段,共需要预计算并存储 4 个表.

- 表 T_1:仅在 $w'_9[1,3]$ 处差分活动的 $\Delta w'_{9,col(0)}$ 共有 2^8 种取值,故 $\Delta x_{10,col(0)}$ 有 2^8 种取值.以 $\Delta y_{10,col(0)}$ 的 2^{16} 种可能取值为索引,根据性质 2.2,平均每个索引值对应 2^8 个 $y_{10,col(0)}$ 及对应的 $w'_9[1,3]$.因 $\Delta y_{10,col(0)}=\Delta C_{col(0)}$ 和 $w'_9[1,3]=z'_9[10,15]$,以 2^{16} 个密文差分 $\Delta C_{col(0)}$ 为索引,平均可以得到 2^8 个 $y_{10,col(0)}$ 和 $(z'_9[10,15],z''_9[10,15])$,将其存储在表 T_1 中.
- 表 T_2:仅在 $w'_9[4]$ 处差分活动的 $\Delta w'_{9,col(1)}$ 共有 2^4 种取值.Δy_{10} 第 1 列中仅在第 5~第 7 半字节差分活动,以 2^{12} 个 $\Delta C_{col(1)}$ 为索引,存储 2^4 个 $y_{10}[5,6,7]$ 和 $(z'_9[14],z''_9[14])$ 在表 T_2 中.
- 表 T_3:在 $w'_9[8]$ 处差分活动的 $\Delta w'_{9,col(2)}$ 共有 2^4 种取值.Δy_{10} 第 2 列中仅在第 9~第 11 半字节差分活动,以 2^{12} 个 $\Delta C_{col(2)}$ 为索引,存储 2^8 个 $y_{10}[9,10,11]$ 和 $(z'_9[9],z''_9[9])$ 在表 T_3 中.
- 表 T_4:在 $w'_9[13,15]$ 处差分活动的 $\Delta w'_{9,col(3)}$ 共有 2^8 种取值.以 2^{16} 个 $\Delta C_{col(3)}$ 为索引,存储 2^8 个 $y_{10,col(3)}$ 和 $(z'_9[8,13],z''_9[8,13])$ 在表 T_4 中.

(二) 在线攻击阶段.

1. 选择 2^n 个明文结构,其中的明文满足在第 1、第 3、第 5、第 6、第 9~第 11、第 14、第 15 半字节上取所有的值,其余半字节取固定值.故一个明文结构包含 2^{36} 个明文,可以构造 2^{71} 个明文对.因此,攻击的选择明文量为 2^{n+36},其中包含 2^{n+71} 个明文对.
2. 运用快速排序算法筛选明文对.筛选出密文在第 4、第 8 半字节差分不活动,在第 1、第 3、第 5~第 7、第 9~第 11、第 13、第 15 半字节差分活动的明文对,剩余 2^{n+63} 个明文对.以明文对序号作索引,将筛选得到的明文对存储在表 Ω 中,只需要存储明文第 1、第 3、第 5、第 6、第 9~第 11、第 14、第 15 半字节与密文第 1~第 3、第 5~第 7、第 9~第 15 半字节.
3. 猜测出口白化密钥 $k_{e11}[0,1,2,3]$.对于表 Ω 中的 2^{n+63} 个明文对,利用明文对序号可以得到其对应的密文差分 $\Delta C_{col(0)}$.利用 $\Delta C_{col(0)}$ 查表 T_1,得到 2^8 个 $y_{10,col(0)}$ 和 $(z'_9[10,15],z''_9[10,15])$,可以确定密钥 $k_{e11}[0,1,2,3]=C_{col(0)}\oplus y_{10,col(0)}$.以 2^{16} 个 $k_{e11}[0,1,2,3]$ 的可能值为索引,平均存储 $2^{n+63}\times 2^8/2^{16}=2^{n+55}$ 个明文对序号和 $(z'_9[10,15],z''_9[10,15])$ 在表 Ω_1 中.
4. 猜测出口白化密钥 $k_{e11}[5,6,7]$.已知 $k_{e11}[0,1,2,3]$,对表 Ω_1 中的 2^{n+55} 个明文对,利用明文对序号可得其对应的密文差分 $\Delta C_{col(1)}$.利用 $\Delta C_{col(1)}$ 查表 T_2,得到 2^4 个 $y_{10}[5,6,7]$ 和 $(z'_9[14],z''_9[14])$,可确定密钥 $k_{e11}[5,6,7]$.以 $k_{e11}[5,6,7]$ 为索引,平均存储 $2^{n+55}\times 2^4/2^{12}=2^{n+47}$ 个明文对序号和 $(z'_9[10,14,15],z''_9[10,14,15])$ 在表 Ω_2 中.
5. 猜测出口白化密钥 $k_{e11}[9,10,11]$.已知 $k_{e11}[0,1,2,3,5,6,7]$,对于表 Ω_2 中的 2^{n+47} 个明文对,利用明文对序号可以得到其对应的密文差分 $\Delta C_{col(2)}$.利用 $\Delta C_{col(2)}$ 查表 T_3,得到 2^8 个 $y_{10}[9,10,11]$ 和 $(z'_9[9],z''_9[9])$,可以确定密钥 $k_{e11}[9,10,11]$;以 $k_{e11}[9,10,11]$ 为索引,平均存储 $2^{n+47}\times 2^4/2^{12}=2^{n+39}$ 个明文对和 $(z'_9[9,10,14,15],z''_9[9,10,14,15])$ 存储在表 Ω_3 中.
6. 猜测出口白化密钥 $k_{e11}[12,13,14,15]$.已知 $k_{e11}[0,1,2,3,5,6,7,9,10,11]$,对于表 Ω_3 中的 2^{n+39} 个明文对,可以得到其对应的密文差分 $\Delta C_{col(3)}$.利用 $\Delta C_{col(3)}$ 查表 T_4,得到 2^8 个 $y_{10,col(3)}$ 和 $(z'_9[8,13],z''_9[8,13])$,可以确定密钥 $k_{e11}[12,13,14,15]$;以 $k_{e11}[12,13,14,15]$ 为索引,平均存储 $2^{n+39}\times 2^8/2^{16}=2^{n+31}$ 个明文对序号和 $(z'_9[8,9,10,13,14,15],z''_9[8,9,10,13,14,15])$ 存储在表 Ω_4 中.
7. 猜测 $k^*_{e10}[8,9,10,13,14,15]$.已知 $k_{e11}[0,1,2,3,5,6,7,9,10,11,12,13,14,15]$,利用表 Ω_4 中 2^{n+31} 个明文对,穷举 $\Delta z'_8[6,7]$,根据性质 1.2 可以得到 2^8 个 $y_9[8,9,10,13,14,15]$,故可以确定 $k^*_{e10}[8,9,10,13,14,15]=y_9[8,9,10,13,14,15]\oplus z'_9[8,9,10,13,14,15]$.以 $k^*_{e10}[8,9,10,13,14,15]$ 为索引,表 Ω_5 平均存储 $2^{n+31}\times 2^8/2^{24}=2^{n+15}$ 个明文

序号和 $(z'_8[6,7], z''_8[6,7])$.

8. 猜测 $k^*_{e9}[2,3]$.已知 $k_{e11}[0,1,2,3,5,6,7,9,10,11,12,13,14,15]$与 $k^*_{e10}[8,9,10,13,14,15]$,利用表$\Omega_5$ 中 2^{n+15} 个明文对穷举 $\Delta z'_7[1,11]$,可得 2^4 个 $k^*_{e9}[2,3]$.以 $k^*_{e9}[2,3]$ 为索引,表Ω_6 中存储 $2^{n+15}\times 2^4/2^8=2^{n+11}$ 个明文对序号.

9. 已知 $k_{e11}[0,1,2,3,5,6,7,9,10,11,12,13,14,15]$与 $k^*_{e10}[8,9,10,13,14,15]$ 及 $k^*_{e9}[2,3]$ 取值,根据密钥扩展算法,由出口白化密钥 $k_{e11}[0,1,2,3,5,6,7,9,10,11,12,13,14,15]$可以直接得到入口白化密钥 $k_{e0}[1,3,5,6,9,10,11,14,15]$,利用上述密钥对$\Omega_6$ 中 2^{n+11} 个明文对加密 1 轮,筛选出满足使得仅在$\Delta w_0[0,5,10]$处活动的明文对.以 $k^*_{e9}[2,3]$ 为索引,表Ω_7 中存储 $2^{n+11}\times 2^{-24}=2^{n-13}$ 个明文对序号.

10. 已知密钥 $k_{e11}[0,1,2,3,5,6,7,9,10,11,12,13,14,15]$与 $k^*_{e10}[8,9,10,13,14,15]$ 及 $k^*_{e9}[2,3]$ 取值,穷举 2^{12} 个密钥 $k_{e1}[0,5,15]$.利用上述密钥对Ω_7 中 2^{n-13} 个明文对加密 1/2 轮,以 2^{-8} 的概率得到不可能差分区分器的输入.将通过检测的密钥列为候选密钥,最后对候选密钥穷举 10 个半字节密钥 $k^*_{e10}[0,1,4,5,6,7,11,12]$ 及 $k_{e11}[4,8]$,进行 11 轮 Midori 算法加密检测得到的 128 比特密钥是否正确.

具体的攻击路径如图 9 所示,其中,网状表示猜解的密钥半字节.

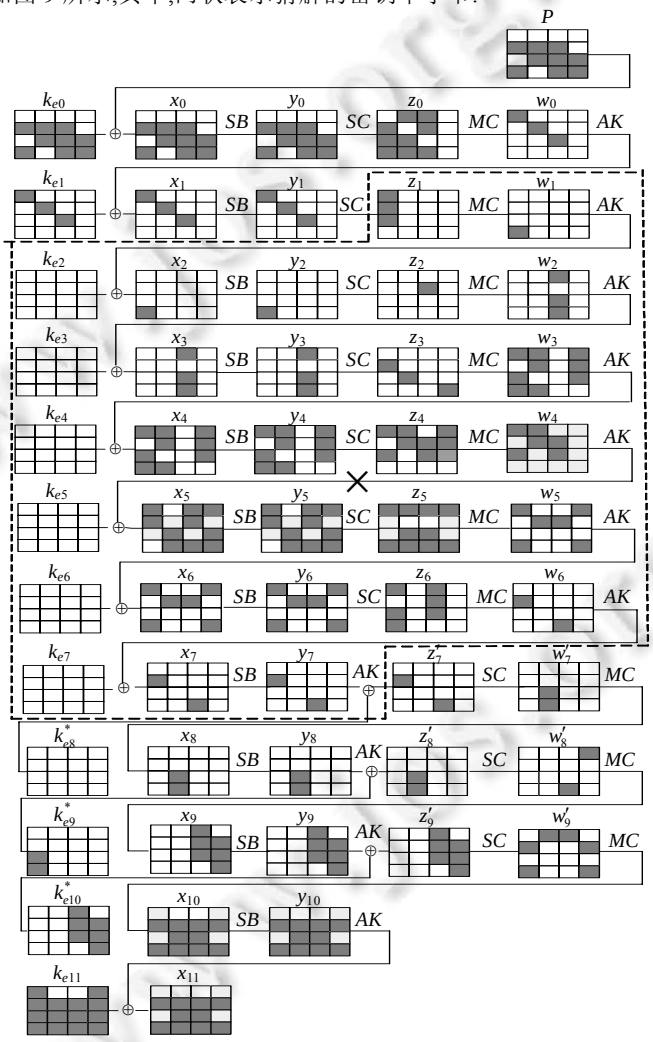

Fig.9 11-round impossible differential cryptanalysis of Midori-64

图 9 11 轮 Midori-64 算法不可能差分分析

由定理 4.2 给出上述 11 轮 Midori-64 算法不可能差分分析的复杂度分析结果.

定理 4.2. 利用 6 轮不可能差分区分器对 11 轮 Midori-64 算法进行不可能差分分析,恢复 128 比特主密钥,其时间复杂度为 $2^{121.4}$ 次 11 轮 Midori-64 算法加密,数据复杂度为 $2^{60.8}$ 个选择明文,存储复杂度为 $2^{96.5}$ 个 Midori-64 状态.

证明:下面给出 11 轮 Midori-64 算法不可能差分分析中步骤 1~步骤 9 各步骤的复杂度,见表 3.证毕. □

Table 3 Complexity of 11-round impossible differential cryptanalysis on Midori-64

表 3 11 轮 Midori-64 算法不可能差分分析复杂度

步骤	时间复杂度	存储复杂度
1	–	$2^{n+71}\times 9$
2	$2^{n+71}\times 2^{6.2}$	$2^{n+63}\times(9+13)$
3	$2^{n+63}\times 2^{8}$	$2^{16}\times 2^{n+55}\times(4+(n+63)/4)$
4	$2^{16}\times 2^{n+55}\times 2^{4}$	$2^{12}\times 2^{n+47}\times(6+(n+63)/4)$
5	$2^{28}\times 2^{n+47}\times 2^{4}$	$2^{12}\times 2^{n+39}\times(8+(n+63)/4)$
6	$2^{40}\times 2^{n+39}\times 2^{8}$	$2^{16}\times 2^{n+31}\times(12+(n+63)/4)$
7	$2^{56}\times 2^{n+31}\times 2^{8}$	$2^{24}\times 2^{n+15}\times(4+(n+63)/4)$
8	$2^{80}\times 2^{n+15}\times 2^{4}$	$2^{8}\times 2^{n+11}\times(n+63)/4$
9	$2^{88}\times 2^{n+11}$	$2^{8}\times 2^{n-13}\times(n+63)/4$

由表 3 可知,前 9 个分析步骤,其时间复杂度大约为 $2^{n+96.6}$ 次 11 轮 Midori-64 算法加密.对于第 10 步,在 88 比特已知密钥下,对 2^{n-13} 个明文对加密 0.5 轮的时间复杂度为 $2^{88}\times 2^{12}\times 2^{n-13}\times 0.5\times 2/11\approx 2^{n+83.5}$ 次 11 轮 Midori-64 算法加密;经过检测后候选密钥集规模 $\varepsilon=2^{100}\times(1-2^{-8})^{2^{n-13}}$,对剩余 40 比特密钥进行穷举恢复主密钥的时间复杂度为 $\varepsilon\times 2^{40}$.当 n=24.8 时,11 轮 Midori-64 算法不可能差分分析总时间复杂度为 $2^{96.6+24.8}+2^{83.5+24.8}+2^{100}\times(1-2^{-8})^{2^{24.8-13}}\times 2^{40}\approx 2^{121.4}$ 次 11 轮 Midori-64 算法加密,数据复杂度为 $2^{60.8}$ 个选择明文,存储复杂度约为 $2^{95.8}\times(4+87.8/4)/16\approx 2^{95.5}$ 个 Midori-64 状态.

5 结 论

本文证明了在单密钥条件下 Midori 算法的截断不可能差分区分器至多 6 轮,并对 6 轮截断不可能差分区分器进行分类;其次,根据 Midori 算法 6 轮截断不可能差分区分器的分类构造了一个较优的 6 轮区分器,并给出了 11 轮 Midori-64 算法的不可能差分分析,其时间复杂度为 $2^{121.4}$,数据复杂度为 $2^{60.8}$,存储复杂度为 $2^{96.5}$.该结果表明,本文给出了一个较好的 11 轮 Midori-64 算法的分析.对于 Midori-128 算法是否也可以根据 Midori 算法 6 轮截断不可能差分区分器的分类构造出较优的区分器,以得到较好的不可能差分分析结果,这是我们下一步要考虑的问题.

作者注 本文是我们于 2018 年 4 月 24 日投到《软件学报》的论文.该文是战略支援部队信息工程大学郭建胜老师(本文第二作者)指导的 2018 届(2018 年 12 月)毕业的研究生李明明(本文第一作者)的硕士学位论文《典型轻量级分组密码算法不可能差分分析研究》工作成果的一部分,特此说明.

References:

[1] Knudsen L. DEAL—A 128-bit block cipher. Technical Report, No.151, Department of Informatics, University of Bergen, 1998.

[2] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Proc. of the EUROCRYPT'99. Berlin, Heidelberg: Springer-Verlag, 1999. 12–23.

[3] Kim J, Hong S, Lim J. Impossible differential cryptanalysis using matrix method. Discrete Mathematics, 2010,310(5):988–1002.

[4] Luo YY, Lai XJ, Wu ZM, Gong G. A unified method for finding impossible differentials of block cipher structures. Information Sciences, 2014,263(1):211–220.

[5] Sun B, Liu M, Guo J, Rijmen V, Li RL. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In: Proc. of the Advances in Cryptology (EUROCRYPT 2016). Berlin, Heidelberg: Springer-Verlag, 2016. 196–213.

[6] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJB, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher. In: Proc. of the CHES 2007. Berlin, Heidelberg: Springer-Verlag, 2007. 450–466.

[7] Izadi M, Sadeghiyan B, Sadeghian SS, Khanook HA. MIBS: A new lightweight block cipher. In: Proc. of the CANS 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 334–348.

[8] Dolmatov V. GOST 28147-89 encryption, decryption and MAC algorithms. RFC 5830, IETF, 2010. http://tools.ietf.org/html/rfc5830

[9] Gong Z, Nikova S, Law YW. KLEIN: A new family of lightweight block ciphers. In: Proc. of the Int'l Workshop on Radio Frequency Identification: Security and Privacy Issues. Berlin, Heidelberg: Springer-Verlag, 2011. 1–18.

[10] Guo J, Peyrin T, Poschmann A, Robshaw M. The LED block cipher. In: Proc. of the CHES 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 326–341.

[11] Shibutani K, Isobe T, Hiwatari H, Mitsuda A, Akishita T, Shirai T. Piccolo: An ultra-lightweight block cipher. In: Proc. of the CHES 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 342–357.

[12] Wu WL, Zhang L. LBlock: A lightweight block cipher. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer-Verlag, 2011. 327–344.

[13] Borghoff J, Canteaut A, Güneysu T, Kavun EB, Knezevic M, Knudsen LR, Leander G, Nikov V, Paar C, Rechberger C, Rombouts P, Thomsen SS, Yalçin T. PRINCE—A low-latency block cipher for pervasive computing applications. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer-Verlag, 2012. 208–225.

[14] Banik S, Bogdanov A, Isobe T, Shibutani K, Hiwatari H, Akishita T, Regazzoni F. Midori: A block cipher for low energy. In: Proc. of the ASIACRYPT 2015. Berlin, Heidelberg: Springer-Verlag, 2015. 411–436.

[15] Lin L, Wu WL. Meet-in-the-Middle attacks on reduced-round Midori64. IACR Trans. on Symmetric Cryptology, 2017,2017(1): 215–239.

[16] Guo J, Jean J, Nikolić I, Qiao K, Sasaki Y, Sim SM. Invariant subspace attack against full midori64. In: Proc. of the IACR Cryptology ePrint Archive. 2015. https://eprint.iacr.org/2015/1189.pdf

[17] Chen Z, Wang XY. Impossible differential cryptanalysis of Midori. In: Proc. of the Int'l Conf. on Mechatronics and Automation, World Scientific. 2017. 221–229. [doi: 10.1142/9789813208537_0028]

[18] Cui JY. Research on cryptanalysis based on meet-in-the-middle [MS. Thesis]. Zhengzhou: Information Engineering University, 2017 (in Chinese with English abstract).

附中文参考文献:

[18] 崔竞一.基于中间相遇思想的攻击方法研究[硕士学位论文].郑州:信息工程大学,2017.

李明明(1995－),男,湖南衡阳人,硕士,主要研究领域为分组密码的设计与分析.

崔竞一(1992－),男,博士生,主要研究领域为分组密码的设计与分析.

郭建胜(1972－),男,博士,教授,主要研究领域为信息安全,密码学.

徐林宏(1995－),男,硕士,主要研究领域为分组密码的设计与分析.