基于 MILP 的轻量级密码算法 ACE 的差分分析

刘帅，关杰，胡斌，马宿东
（信息工程大学密码工程学院，河南 郑州 450001）

摘 要：研究了轻量级密码算法 ACE 的差分性质。首先定义了 n 维环形与门组合，充分分析了该结构中与门之间的相互关系，仅利用 $O(n)$个表达式给出其精确的 MILP 差分刻画，将 ACE 算法中的非线性操作转化为 32 维环形与门组合，从而给出了 ACE 算法的 MILP 差分模型。其次根据 MILP 模型求解器 Gurobi 的求解特点，给出了快速求解 ACE 的 MILP 差分模型的方法。对于 3~6 步的 ACE 置换，得到了最优差分链，利用多差分技术给出了更高概率的差分对应，从而给出了 ACE 置换为 3 步的认证加密算法 ACE-$\mathcal{AE}$-128 的差分伪造攻击与哈希算法 ACE-$\mathcal{H}$-256 的差分碰撞攻击，成功概率为 $2^{-90.52}$，并证明了 4 步 ACE 置换达到了 128 bit 的差分安全边界。实际上，n 维环形与门组合的 MILP 差分刻画具有更多的应用场景，可应用于 SIMON、Simeck 等密码算法的分析中。

关键词：轻量级密码算法；混合整数线性规划；环形与门组合；差分分析
中图分类号：TN918.1
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023023

Differential analysis of lightweight cipher algorithm ACE based on MILP

LIU Shuai, GUAN Jie, HU Bin, MA Sudong
School of Cryptography Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: The differential property of the lightweight cipher algorithm ACE was researched. n-dimension ring AND-gate combination was defined and its differential property was described accurately by only $O(n)$ expressions with the MILP method by analyzing the relationship among AND gates. The nonlinear operation of ACE was transformed to the 32-dimension ring AND-gate combination and the MILP differential model of ACE was proposed. According to the characteristics of Gurobi solver, a model for fast solving the MILP differential model of ACE was given. For ACE permutation with 3 to 6 steps, the optimal differential characteristic was obtained and its probability was improved by multi-difference technique. The differential forge attack on authenticated encryption algorithm ACE-$\mathcal{AE}$-128 and the differential collision attack on hash algorithm ACE-$\mathcal{H}$-256 was given with 3-step ACE permutation, and the success probability was $2^{-90.52}$. And it was proved that the 4-steps ACE permutation arrived the differential security bound of 128 bit. Actually, the MILP differential description of ring AND-gate combination can be applied on more cipher algorithms, such as SIMON, Simeck.

Keywords: lightweight cipher algorithm, MILP, ring AND-gate combination, differential analysis

0 引言

随着物联网的发展，如何利用有限的资源保证数据的安全成为当前的重要研究课题，轻量级密码算法（LWCA, lightweight cipher algorithm）[1]应运而生。近年来，涌现出了大量轻量级密码算法[2-5]，其设计与分析得到了研究者的广泛关注[6-8]。2016 年，美国国家标准与技术研究院发起了轻量级密码算法征集活动[9]，要求提交的算法兼具认证与加密功能，这一类算法也被称为认证加密算法[10]。

认证加密算法输入密钥 K、Nonce N、相关数据 A、明文 M，输出密文 C、认证码 T，即

收稿日期：2022−08−25；**修回日期：**2022−11−11
基金项目：国家自然科学基金资助项目（No.61802437, No.62102448）
Foundation Item: The National Natural Science Foundation of China (No.61802437, No.62102448)

$(C,T)=\mathcal{E}(K,N,A,M)$；相应地，解密阶段输入密钥 K、Nonce N、相关数据 A、密文 C、认证码 T，随后生成认证码 T'，如果 $T=T'$ 则认证通过，输出明文 M，否则认证失败输出 $\perp$，即 $\mathcal{D}(K,N,A,C,T)\in\{M,\perp\}$。

随着多种多样的轻量级密码算法被提出，其安全性分析也经历着不断的革新，过去的安全分析往往依赖手工推导，1994 年，Matsui[11]提出了一种强有力的自动化分析工具，利用分支定界搜索算法来搜索最优差分/线性链，从此自动化分析在诸多场景下取代了手工推导[12-15]。2014 年，Sun 等[16]给出了密码算法的混合整数线性规划（MILP, mixed-integer linear programming）差分/线性刻画方法，建立并求解了 MILP 模型来搜索最优差分/线性链，拉开了利用 MILP 自动化搜索技术分析密码算法的序幕[17-21]。MILP 自动化搜索的关键在于 MILP 模型的刻画与快速求解，为了提高求解速度，研究者需要根据密码算法的特点，给出快速求解 MILP 模型的方法，如 Zhou 等[22]针对代换−置换网络（SPN）结构的分组密码算法提出了分而治之策略；刘帅等[23]针对 MORUS 算法的结构特点根据 ΔIV 的重量将 MILP 模型划分为多个子模型，根据 MORUS 算法差分状态的循环等价性省略部分子模型的求解。

LWCA 第二轮的候选算法 ACE 由 Aagaard 等[24]提出，是基于 ACE 置换设计的双工海绵结构轻量级密码算法，包括认证加密算法 ACE-$\mathcal{AE}$-128 和哈希算法 ACE-$\mathcal{H}$-256。研究者在设计报告中做出了较粗略的差分分析，利用最小活动 SB-64 的数量给出了 ACE 置换抗差分分析的安全边界。

2020 年，Liu 等[25]提出了 ACE 置换不可能差分的自动化搜索算法，证明了 ACE 置换不存在 9 步以上的不可能差分，并给出了 8 步不可能差分。2021 年，叶涛等[26]针对 ACE 算法给出了 12 步 ACE 置换的积分区分器，相比于研究者给出的区分器提高了 4 步，取得了较大的改进。2022 年，Chang 等[27]给出了 ACE 算法的伪造攻击。对于差分分析，仍没有第三方给出较精确的分析结果。

差分分析是研究密码算法安全性强有力的分析方法，近几年，针对轻量级密码算法的差分分析得到了广泛的研究。2022 年，蒋梓龙等[28]针对 Saturnin 算法给出了 5.5 轮不可能差分攻击。同年，Dunkelman 等[29]给出了相关密钥下全轮 TinyJUMBU-192/256 的差分伪造攻击。

本文基于自动化分析工具 MILP 对 ACE 算法的差分性质进行研究。利用 MILP 搜索差分链，首先给出算法中非线性操作差分性质的 MILP 刻画，给出的刻画越精确，就能更大程度地确保搜索得到的差分链的概率最大。ACE 算法中的唯一非线性操作为与门，对于 ACE 置换，SB-64 轮函数中的 32 个与门的输入之间存在紧密的关系，如何充分考虑与门之间的相互关系是要解决的首要问题，本文将这 32 个与门转化为环形与门组合，给出了环形与门组合差分性质精确的 MILP 刻画。为了提高 MILP 差分模型的求解速度，本文采用了如下方法：1) 利用最小活跃 SB-64 的数量给出目标函数的下界；2) 利用环形与门组合输入差分重量与差分转移概率之间的关系，增加约束条件，缩减 MILP 模型的可行域与变量的取值范围。最后给出了 ACE 置换的高概率差分链，为了提高差分链的概率，搜索了具有相同输入、输出差分的差分链。利用搜索到的差分链，给出了对 ACE 算法的攻击方法：ACE 置换为 3 步的简化版 ACE-$\mathcal{AE}$-128 的差分伪造攻击，以及简化版 ACE-$\mathcal{H}$-256 的差分碰撞攻击。

1 背景知识

1.1 轻量级密码算法 ACE

ACE 是由 Aagaard 等[24]提出的轻量级密码算法，包括认证加密算法 ACE-$\mathcal{AE}$-128 与哈希算法 ACE-$\mathcal{H}$-256。ACE 算法的设计采用基于 ACE 置换的双工海绵结构，ACE 置换是 ACE 算法的主体部分，其规模为 320 bit，第 i 步状态表示为 5 个 64 bit $(A^i,B^i,C^i,D^i,E^i)(i=0,1,2,\cdots,16)$，ACE 置换由 ACE-step 迭代 16 次，图 1 展示了 ACE-step。其中，第 i 步 ACE-step 中使用了 6 个 8 bit 的轮常数 $\mathrm{rc}_0^i,\mathrm{rc}_1^i,\mathrm{rc}_2^i,\mathrm{sc}_0^i,\mathrm{sc}_1^i,\mathrm{sc}_2^i$。

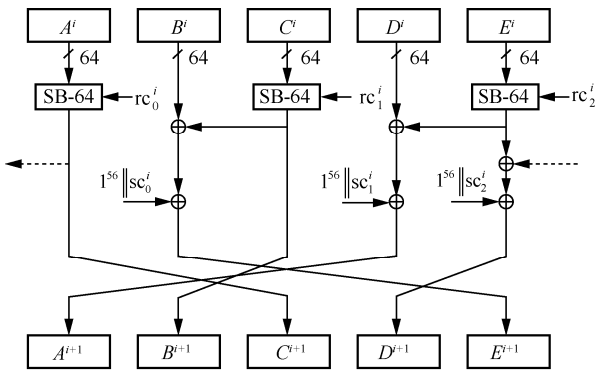

图 1 ACE-step

ACE 置换的非线性环节 SB-64 是一个减轮的不带密钥的分组密码 Simeck[2]，其分组规模为 64 bit，轮数为 8，采用 Feistel 结构，轮函数如图 2 所示。

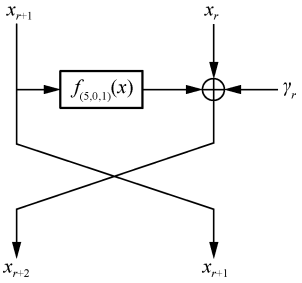

图 2　SB-64 轮函数

图 2 中，$f_{(5,0,1)}(x)=(\mathrm{L}^5(x)\odot x)\oplus \mathrm{L}^1(x)$，$\mathrm{L}^i(x)$ 表示 x 循环左移 i 位，SB-64 输入一个 8 bit 的常数 $\mathrm{rc}=(q_7,q_6,\cdots,q_0)$，$\gamma_r=1^{31}\|q_r(r=0,1,\cdots,7)$ 为其第 r 轮常数。

对于认证加密算法 ACE-$\mathcal{AE}$-128 与哈希算法 ACE-$\mathcal{H}$-256，其状态大小均为 320 bit，状态 S 中有 $r=64$ bit 进行数据的输入与输出，称为比率部分，记为 S_r。比率部分由 320 bit 状态 $S=A\|B\|C\|D\|E$ 中的 8 个字节组成，分别为 A[7]、A[6]、A[5]、A[4]、C[7]、C[6]、C[5]、C[4]，其中，$A[j]$、$C[j]$ 分别表示 A、C 的第 j 个字节。对于算法 ACE-$\mathcal{AE}$-128 与 ACE-$\mathcal{H}$-256 的具体结构，这里不再赘述，可参照其设计报告[24]。

1.2　差分伪造攻击与差分碰撞攻击

对于认证加密算法，伪造攻击的基本思想是如果攻击者能够构造出未经询问的合法消息密文对则伪造成功，按照构造认证码的方式不同，将其分为差分伪造攻击和直接伪造攻击。差分伪造攻击是指攻击者在已掌握消息密文对的情况下，利用差分分析方法，构造出另一对消息密文对且能够通过验证。

哈希算法要求对于不同的消息，必定得到不同的哈希值。差分碰撞攻击的思想是利用高概率差分对应找到一对不同的消息，其对应的哈希值相同，这样哈希算法便是不安全的。

令 S_Δ 表示 320 bit 状态差分，其比率部分差分为 $\Delta\neq 0$，其余比特差分为 0，寻找 ACE 置换一条高概率的差分链 $S_{\Delta_1}\to S_{\Delta_2}$，其差分转移概率为 P，根据该差分链，可以构造认证加密算法 ACE-$\mathcal{AE}$-128 的差分伪造攻击以及哈希算法 ACE-$\mathcal{H}$-256 的差分碰撞攻击。

1) 认证加密算法 ACE-$\mathcal{AE}$-128 的差分伪造攻击

已知 Nonce、相关数据、明文组 $(N,A_0\oplus\Delta_1\|A_1\oplus\Delta_2,M)$，询问 ACE-$\mathcal{AE}$-128 加密机得到认证码 T，则认证码 T 对 $(N,A_0\|A_1,M)$ 以概率 P 有效。同样地，也可以在明文处理阶段加入差分构造攻击。图 3 给出了 ACE-$\mathcal{AE}$-128 的差分伪造攻击示意。

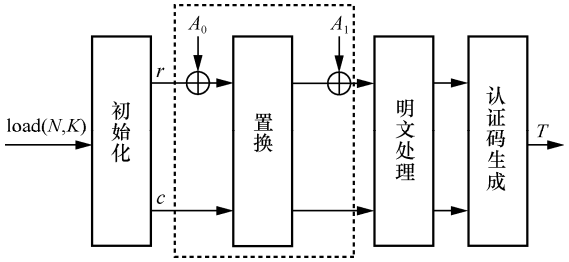

图 3　ACE-$\mathcal{AE}$-128 的差分伪造攻击示意

2) 哈希算法 ACE-$\mathcal{H}$-256 的差分碰撞攻击

已知初始变量、明文对 $(\mathrm{IV},M_0\oplus\Delta_1\|M_1\oplus\Delta_2)$，询问 ACE-$\mathcal{H}$-256 加密机得到哈希值 H，则初始变量、明文对 $(\mathrm{IV},M_0\|M_1)$ 的哈希值与 H 以概率 P 产生碰撞。图 4 给出了 ACE-$\mathcal{H}$-256 的差分碰撞攻击示意。

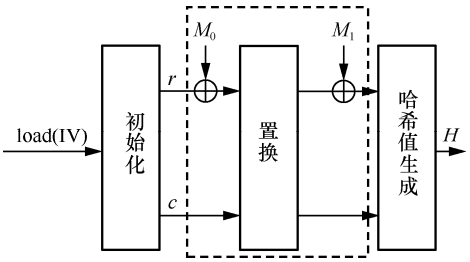

图 4　ACE-$\mathcal{H}$-256 的差分碰撞攻击示意

2　ACE 的 MILP 差分模型

本节给出了 ACE 的 MILP 差分模型，主要研究了其非线性环节差分特性的 MILP 刻画。由于 ACE 的状态较大，每一步迭代多轮 Simeck 轮函数，MILP 模型很难求解，本文利用 ACE 算法中非线性环节差分转移概率与输入差分重量之间的关系给出了 MILP 差分模型的快速求解方法。

2.1　环形与门组合及其 MILP 差分刻画

对于 ACE 的 MILP 差分模型构建，线性环节的刻画是简单的[16]，需要对其非线性环节进行刻画，

由第 1 节可知，ACE 中唯一的非线性操作为 $y=\mathrm{L}^5(x)\odot x$，将该式按比特展开为 $y=(x_{31}x_{26}, x_{30}x_{25}, x_{29}x_{24}, \cdots, x_1x_{28}, x_0x_{27})$，对 y 的 32 bit 做一个置换得到 $y'=(x_0x_{27}, x_{27}x_{22}, x_{22}x_{17}, x_{17}x_{12}, \cdots, x_{10}x_5, x_5x_0)$，用 g 表示这一类函数，即 $g(x_0,x_1,\cdots,x_{n-1})=(x_0x_1,x_1x_2,\cdots,x_{n-2}x_{n-1},x_{n-1}x_0)$，称 $g(x_0,x_1,\cdots,x_{n-1})$ 为 n 维环形与门组合，其中，x_ix_{i+1} 为第 i 个与门 $(i=0,1,\cdots,n-1)$。图 5 给出了环形与门组合的示意。

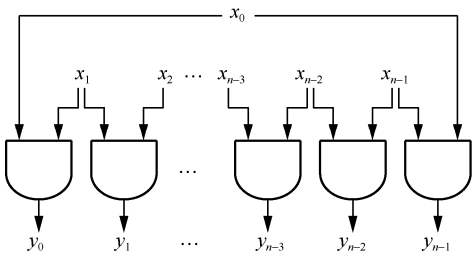

图 5 环形与门组合的示意

从图 5 可以看出，ACE 中的非线性操作实际是一个 32 维环形与门组合，上述转换本质上是将 SB-64 同一轮的 32 个与门利用线性变换进行移位，更直观地展示了 32 个与门之间的相互关系，使 2 个相邻的与门具有一个共同的输入，便于利用数学化的推导进行下一步分析。此外，将 ACE 中的非线性操作归纳为 n 维环形与门组合，对环形与门组合进行研究，使研究结果可以应用于更多的场景，比如 SIMON 算法轮函数中的与门同样可以转化为多维环形与门组合，其维数取决于分组的规模。本节将给出 n 维环形与门组合的 MILP 差分刻画，值得一提的是，Saha 等[21]在分析认证加密算法 TinyJUMBU 时，给出了函数 $f(x_0,x_1,\cdots,x_{n-1})=(x_0x_1,x_1x_2,\cdots,x_{n-2}x_{n-1})$ 的 MILP 差分刻画，称其为链形与门组合。与链形与门组合不同的是，n 维环形与门组合在链形与门组合的基础上增加了一个与门，即最后一个输入 x_{n-1} 与第一个输入 x_0 经过一个与门输出 y_{n-1}，这使 n 个与门之间的相互关系更加复杂，下面给出具体的分析及刻画。

关于 n 维环形与门组合 $g(x_0,x_1,\cdots,x_{n-1})$ 的描述，令下标模 n，为了叙述简洁，下文不再详细标注。表 1 给出了单个与门的差分特性[21]。

令 $\mathrm{id}_i(i=0,1,2,\cdots,n-1)$ 表示输入变量 x_i 的差分，$\mathrm{od}_i(i=0,1,2,\cdots,n-1)$ 表示输出变量 x_ix_{i+1} 的差分，$\lambda_{i,i+1}(i=0,1,2,\cdots,n-1)$ 表示与门 x_ix_{i+1} 的活跃性，则 $g(x_0,x_1,\cdots,x_{n-1})$ 的一个简单的 MILP 差分刻画为

$$\begin{aligned}&\mathrm{id}_i+\mathrm{id}_{i+1}\geqslant \mathrm{od}_i\\&\lambda_{i,i+1}=\mathrm{id}_i\mid \mathrm{id}_{i+1}\end{aligned}\tag{1}$$

其中，$\mid$表示逻辑或，对应的目标函数为

$$\min\sum_{i=0}^{n-1}\lambda_{i,i+1}$$

表 1 单个与门的差分特性

Δx_i	Δx_{i+1}	$\Delta x_i x_{i+1}$	概率
0	0	0	1
		1	0
0	1	x_i	2^{-1}
1	0	x_{i+1}	2^{-1}
1	1	$x_i\oplus x_{i+1}\oplus 1$	2^{-1}

式(1)并没有考虑 n 个与门之间的相关性，实际上，不同与门的输入之间是相互关联的，所以这种简单的刻画显然不准确，为了给出精确的刻画，需要分析环形与门组合中 n 个与门之间的相关性。参考文献[21]，观察 2 个相邻与门 $x_ix_{i+1}, x_{i+1}x_{i+2}$ 的情况，上述刻画认为这 2 个与门相互独立，其差分特性满足

$$\begin{aligned}&\Pr[(\Delta x_i,\Delta x_{i+1},\Delta x_{i+2})\to(\Delta x_ix_{i+1},\Delta x_{i+1}x_{i+2})]=\\&\Pr[(\Delta x_i,\Delta x_{i+1})\to\Delta x_ix_{i+1}]\cdot\\&\Pr[(\Delta x_{i+1},\Delta x_{i+2})\to\Delta x_{i+1}x_{i+2}]\end{aligned}\tag{2}$$

但实际上，式(2)并不一直成立。表 2 给出了输入差取遍所有值时式(2)的成立情况。

表 2 输入差取遍所有值时式(2)的成立情况

Δx_i	Δx_{i+1}	Δx_{i+2}	式(2)是否成立
0	0	0	是
0	0	1	是
0	1	0	是
0	1	1	是
1	0	0	是
1	0	1	否
1	1	0	是
1	1	1	是

由表 2 可知，只有当相邻 2 个与门的输入差为(1,0,1)时，2 个与门的差分传递概率之间存在相关性，这容易从单个与门的差分特性进行解释，当输入差为(1,0,1)，根据表 1，输出差为 $\Delta x_ix_{i+1}=\Delta x_{i+1}x_{i+2}=x_{i+1}$，据此，在 $g(x_0,x_1,\cdots,x_{n-1})$ 的 MILP 差分刻画中增加如下限制条件，其中，$i=0,1,2,\cdots,n-1$。

$$\begin{aligned}&\lambda_{i,i+1,i+2}=\mathrm{id}_i\overline{\mathrm{id}}_{i+1}\mathrm{id}_{i+2}\\&\mathrm{od}_i-\mathrm{od}_{i+1}\leqslant 1-\lambda_{i,i+1,i+2}\\&\mathrm{od}_{i+1}-\mathrm{od}_i\leqslant 1-\lambda_{i,i+1,i+2}\end{aligned}\tag{3}$$

其中，$\overline{\mathrm{id}}_{i+1}$ 表示对 id_{i+1} 取反。当且仅当 $(\mathrm{id}_i,\mathrm{id}_{i+1},\mathrm{id}_{i+2})=(1,0,1)$ 时，第一个等式的 $\lambda_{i,i+1,i+2}=1$，此时第二、三个不等式使 $\mathrm{od}_i=\mathrm{od}_{i+1}$；其他情况下，第二、三个不等式不起作用。$\lambda_{i,i+1,i+2}=\mathrm{id}_i\overline{\mathrm{id}}_{i+1}\mathrm{id}_{i+2}$ 与 $\begin{cases}\mathrm{id}_i+\mathrm{id}_{i+2}-\mathrm{id}_{i+1}-3\lambda_{i,i+1,i+2}\geqslant -1\\ \mathrm{id}_i+\mathrm{id}_{i+2}-\mathrm{id}_{i+1}-2\lambda_{i,i+1,i+2}\leqslant 1\end{cases}$ 线性表达式等价。

另外，将目标函数减去 $\sum_{i=0}^{n-1}\lambda_{i,i+1,i+2}$，以刻画这种相关性带来的影响，这是容易理解的，当且仅当 $(\mathrm{id}_i,\mathrm{id}_{i+1},\mathrm{id}_{i+2})=(1,0,1)$ 时，$\lambda_{i,i+1,i+2}=1$，如果不考虑相关性，其差分转移概率为 2^{-2}；考虑相关性后，其差分转移概率实际为 2^{-1}。

最后，还需要考虑一种特殊情况，即输入差为全 1 的情况。定理 1 给出了这种情况下不同输出差对应的差分转移概率。

定理 1　对于 n 维环形与门组合 $g(x_0,x_1,\cdots,x_{n-1})$，当其输入差为 $(1,1,1,\cdots,1)$（所有比特全为 1）时，假设输出差为 $(a_0,a_1,\cdots,a_{n-1})\in\{0,1\}^n$，令 N_1 表示输出差中 1 的数量，则有：1) 若 $n-N_1\equiv 0\bmod 2$，差分转移概率为 $2^{-(n-1)}$；2) 若 $n-N_1\equiv 1\bmod 2$，差分转移概率为 0。

证明　对于 n 维环形与门组合 $g(x_0,x_1,\cdots,x_{n-1})$，当其输入差分为 $(1,1,1,\cdots,1)$ 时，假设其输出差分为 $(a_0,a_1,\cdots,a_{n-1})\in\{0,1\}^n$，根据表 1，第 i 个与门 x_ix_{i+1} 的输出差分 $\Delta x_ix_{i+1}=x_i\oplus x_{i+1}\oplus 1$，差分转移概率为

$$\begin{aligned}&\mathrm{Pr}_g[(1,1,\cdots,1)\to(a_0,a_1,\cdots,a_{n-1})]=\\&\mathrm{Pr}[\bigcap_{i=0}^{n-1}(x_i\oplus x_{i+1}\oplus 1=a_i)]=\\&\mathrm{Pr}[\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)]\cdot\\&\mathrm{Pr}[x_{n-1}\oplus x_0\oplus 1=a_{n-1}\mid\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)]\end{aligned}$$

易得 $\mathrm{Pr}\left[\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)\right]=2^{-(n-1)}$，对于上式中条件概率 $\mathrm{Pr}\left[x_{n-1}\oplus x_0\oplus 1=a_{n-1}\mid\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)\right]$，当 $\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)$ 成立时，有

$$\begin{aligned}&x_{n-1}\oplus x_0\oplus 1=\\&\bigoplus_{i=0}^{n-2}(x_i\oplus x_{i+1})\oplus 1=\\&\bigoplus_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1)\oplus\bigoplus_{i=0}^{n-1}1=\\&\bigoplus_{i=0}^{n-2}a_i\oplus\bigoplus_{i=0}^{n-1}1=\\&\bigoplus_{i=0}^{n-1}a_i\oplus a_{n-1}\oplus\bigoplus_{i=0}^{n-1}1=\\&\bigoplus_{i=0}^{N_1-1}1\oplus\bigoplus_{i=0}^{n-1}1\oplus a_{n-1}=\\&[(n-N_1)\bmod 2]\oplus a_{n-1}\end{aligned}$$

由此，当 $n-N_1\equiv 0\bmod 2$ 时，$\mathrm{Pr}\left[x_{n-1}\oplus x_0\oplus 1=a_{n-1}\mid\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)\right]=1$，$\mathrm{Pr}_g[(1,1,\cdots,1)\to(a_0,a_1,\cdots,a_{n-1})]=2^{-(n-1)}$；当 $n-N_1\equiv 1\bmod 2$ 时，$\mathrm{Pr}\left[x_{n-1}\oplus x_0\oplus 1=a_{n-1}\mid\bigcap_{i=0}^{n-2}(x_i\oplus x_{i+1}\oplus 1=a_i)\right]=0$，$\mathrm{Pr}_g[(1,1,\cdots,1)\to(a_0,a_1,\cdots,a_{n-1})]=0$。

对于 n 维环形与门组合 $g(x_0,x_1,\cdots,x_{n-1})$，当输入差为全 1 时，输出差中 1 的个数与 n 具有相同的奇偶性，为此加入如下限制条件

$$\begin{aligned}&\lambda=\mathrm{id}_0\mathrm{id}_1\cdots\mathrm{id}_{n-1}\\&\sum_{i=0}^{n-1}\mathrm{od}_i+(\lambda+1)\mathrm{dummy}=n\end{aligned}\tag{4}$$

其中，dummy 是一个辅助变量。当且仅当所有 $i\in\{0,1,\cdots,n-1\}$，满足 $\mathrm{id}_i=1$ 时，$\lambda=1$（即输入差为全 1），此时，第二个等式使输出差中 1 的个数与 n 具有相同的奇偶性；其他情况下，第二个等式不起任何作用。在输入差为全 1 的情况下，最后一个与门与前 $n-1$ 个与门具有相关性，因此目标函数应该减去 λ。$\lambda=\mathrm{id}_0\mathrm{id}_1\cdots\mathrm{id}_{n-1}$ 与 $\begin{cases}\sum_{i=0}^{n-1}\mathrm{id}_i-n\lambda\geqslant 0\\ \sum_{i=0}^{n-1}\mathrm{id}_i-n\lambda\leqslant n-1\end{cases}$ 线性表达式等价。

综上，式(1)、式(3)和式(4)给出了 n 维环形与门组合 $g(x_0,x_1,\cdots,x_{n-1})$ 完全精确的 MILP 差分刻画，目标函数为 $\min\sum_{i=0}^{n-1}\lambda_{i,i+1}-\sum_{i=0}^{n-1}\lambda_{i,i+1,i+2}-\lambda$。

式(1)、式(3)和式(4)共包含 $5n+2$ 个线性表达式、一个二次表达式以及 n 个逻辑或表达式。如果单纯把 n 维环形与门组合 g 当作一个大规模的 S 盒

处理，由于规模过大，利用之前关于 S 盒的 MILP 刻画技术[30]很难对函数 g 进行有效刻画，本文仅利用 $O(n)$ 个表达式精确刻画了 n 维环形与门组合 g 的差分特性，并验证了以上刻画是完全精确的。

2.2 MILP 差分模型的快速求解

为了提高搜索差分/线性链的速度，Zhou 等[22]针对 SPN 结构与 Feistel 结构的分组密码给出了 MILP 模型的分而治之求解策略，其基本思想是缩减 MILP 模型的可行域，这部分可行域由于活跃 S 盒的数量较多，不包含较好的差分/线性链。Zhou 等[22]的方法并不适用于 ACE 算法，由于 ACE 算法的非线性环节（环形与门组合）规模较大，把环形与门组合当作 S 盒处理仅考虑其活跃性，会忽略很多细节。由于 ACE 的状态规模较大，且轮函数较为复杂，其 MILP 差分模型很难求解，本节结合 Gurobi 求解器及 ACE 的特点，给出了提高 MILP 差分模型求解速度的方法。

对于一条差分链，假设其差分转移概率为 $P\neq 0$，称 $-\mathrm{lb}P$ 为差分转移概率的重量。求解差分链的最大差分转移概率即求解差分转移概率重量的最小值，这与 2.1 节中给出的目标函数一致。按照 2.1 节的刻画方法给出 R 步 ACE-step 的 MILP 差分模型，记该模型为 $\mathcal{M}_1$，并利用 Gurobi 求解器求解该 MILP 差分模型，Gurobi 求解器实时返回当前的最优解 CB 以及最优解的下界 LB，当 CB=LB 时，Gurobi 确定 CB 为该模型最优解 B 并返回该解，据此可以将 Gurobi 求解过程分为 2 个主要部分：1) 求解当前最优解 CB，直到得到全局最优解 B；2) 计算更紧致的下界 LB，直到 LB=B。

根据经验，在 Gurobi 的求解过程中，往往能够较快地给出全局最优解 B，而绝大部分时间都被用来收紧下界 LB，使 LB 的数值逐渐增加，逼近数值 B。根据 Gurobi 求解过程的特点，给出 2 种方式来提高 MILP 差分模型 $\mathcal{M}_1$ 的求解速度：1) 建立一个粗略的 MILP 差分模型 $\mathcal{M}_2$，给出模型 $\mathcal{M}_1$ 目标函数的紧致下界，以提高求解过程第二部分的速度；2) 通过分析环形与门组合的差分转移概率与输入差之间的关系，加入一些限制条件缩减 MILP 差分模型 $\mathcal{M}_1$ 的可行域或者缩小变量的取值范围，从而提高求解过程第一部分的速度。

2.2.1 MILP 差分模型下界的确定

本节建立了一个 MILP 差分模型 $\mathcal{M}_2$，对于 R 步 ACE-step，$\mathrm{AC}_{i,j}\in\{0,1\}$ 表示第 $i(i=0,1,\cdots,R-1)$ 步 ACE-step 中第 $j(j=0,1,2)$ 个 SB-64 的活跃性，当且仅当该 SB-64 的输入差不为 0 时，$\mathrm{AC}_{i,j}=1$，否则 $\mathrm{AC}_{i,j}=0$，目标函数为 $\min\sum_{i=0}^{R-1}\sum_{j=0}^{2}\mathrm{AC}_{i,j}$。

2 种模型的区别仅在于模型 $\mathcal{M}_1$ 的目标函数是使差分链的差分转移概率重量达到最小，而模型 $\mathcal{M}_2$ 的目标函数是使差分链中活跃 SB-64 的数量达到最小。由于目标函数更加简单，后者的求解变得非常容易。对于一个活跃的 SB-64，其差分转移概率的重量最小值为 18[31]，由此容易得到定理 2。

定理 2 对于 R 步 ACE-step，假设其活跃 SB-64 的最小数量为 v，则其差分转移概率的重量下界为 $18v$。

证明 对于 R 步 ACE-step 的任意一条概率为 $P=2^{-p}\neq 0$ 的差分链，其活跃 SB-64 的数量为 w，设第 $i(i=0,1,\cdots,w-1)$ 个活跃 SB-64 的差分转移概率重量为 p_i，则 $p=\sum_{i=0}^{w-1}p_i\geqslant\sum_{i=0}^{w-1}18=18w\geqslant 18v$，所以差分转移概率的重量下界为 $18v$。证毕。

定理 2 给出了一种确定 MILP 差分模型 $\mathcal{M}_1$ 目标函数下界的方法，由于 Gurobi 求解过程第二步花费的时间远大于第一步，这种方法大大提升了模型 $\mathcal{M}_1$ 的求解速度。表 3 给出了不同步数 ACE 置换活跃 SB-64 的最小数量及其搜索时间。

表 3 不同步数 ACE 置换活跃 SB-64 的最小数量及其搜索时间

步数	活跃 SB-64 最小数量	搜索时间/s
3	4	0.13
4	6	1.82
5	6	0.41
6	8	0.92

2.2.2 增加 MILP 差分模型的限制条件

ACE 中唯一的非线性操作是环形与门组合，根据 2.1 节的分析直观地得出一个结论：环形与门组合的输入差分重量越小，差分转移概率越大。定理 3 具体分析了环形与门组合的差分转移概率与输入差分重量之间的关系。

定理 3 假设 n 维环形与门组合的输入差分为 $\mathrm{id}=(\mathrm{id}_0,\mathrm{id}_1,\cdots,\mathrm{id}_{n-1})$，id 的重量为 $W_{\mathrm{id}}=\sum_{i=0}^{n-1}\mathrm{id}_i$，对于任意输出差分，满足差分转移概率 $P\neq 0$，则概率 P 具有 $P=2^{-p}$ 的形式，其中 p 为非负整数，且有

$\frac{1}{2}W_{\mathrm{id}} \leqslant p \leqslant 2W_{\mathrm{id}}$。

证明　根据 2.1 节的分析，容易得到差分转移概率为 $P=2^{-p}$，其中 $p=\sum_{i=0}^{n-1}\lambda_{i,i+1}-\sum_{i=0}^{n-1}\lambda_{i,i+1,i+2}-\lambda$ 且 $\lambda_{i,i+1}=\mathrm{id}_i \mid \mathrm{id}_{i+1}, \lambda_{i,i+1,i+2}=\mathrm{id}_i\overline{\mathrm{id}_{i+1}}\mathrm{id}_{i+2}, \lambda=\mathrm{id}_0\mathrm{id}_1\cdots\mathrm{id}_{n-1}$。

1) 当 $W_{\mathrm{id}}<n$ 时，$\lambda=0$，对于任意 $i=0,1,2,\cdots,n-1$，$\lambda_{i-1,i,i+1}$ 与 $\lambda_{i,i+1,i+2}$ 的取值不可能同时为 1，则有 $\lambda_{i-1,i,i+1}+\lambda_{i,i+1,i+2}\leqslant 1$，若 $\mathrm{id}_i=\mathrm{id}_{i+1}=0$，$\lambda_{i,i+1}=\lambda_{i-1,i,i+1}+\lambda_{i,i+1,i+2}=0$，否则，$\lambda_{i,i+1}=1\geqslant \lambda_{i-1,i,i+1}+\lambda_{i,i+1,i+2}$，所以 $\lambda_{i,i+1}\geqslant\lambda_{i-1,i,i+1}+\lambda_{i,i+1,i+2}$ 恒成立，则有

$$p=\sum_{i=0}^{n-1}\lambda_{i,i+1}-\sum_{i=0}^{n-1}\lambda_{i,i+1,i+2}=$$
$$\frac{1}{2}\sum_{i=0}^{n-1}\lambda_{i,i+1}+\frac{1}{2}\sum_{i=0}^{n-1}(\lambda_{i,i+1}-2\lambda_{i,i+1,i+2})=$$
$$\frac{1}{2}\sum_{i=0}^{n-1}\lambda_{i,i+1}+\frac{1}{2}\sum_{i=0}^{n-1}(\lambda_{i,i+1}-(\lambda_{i-1,i,i+1}+\lambda_{i,i+1,i+2}))\geqslant$$
$$\frac{1}{2}\sum_{i=0}^{n-1}\lambda_{i,i+1}\geqslant\frac{1}{2}\sum_{i=0}^{n-1}\mathrm{id}_i=\frac{1}{2}W_{\mathrm{id}}$$

2) 当 $W_{\mathrm{id}}=n$ 时，根据定理 1 明显有

$$p=n-1=W_{\mathrm{id}}-1\geqslant\frac{1}{2}W_{\mathrm{id}}$$

综上，$p\geqslant\frac{1}{2}W_{\mathrm{id}}$ 成立，显然 p 为非负整数，且

$$p\leqslant\sum_{i=0}^{n-1}\lambda_{i,i+1}=\sum_{i=0}^{n-1}(\mathrm{id}_i \mid \mathrm{id}_{i+1})\leqslant\sum_{i=0}^{n-1}(\mathrm{id}_i+\mathrm{id}_{i+1})=$$
$$\sum_{i=0}^{n-1}\mathrm{id}_i+\sum_{i=0}^{n-1}\mathrm{id}_{i+1}=2W_{\mathrm{id}}$$

证毕。

定理 3 中的不等式 $\frac{1}{2}W_{\mathrm{id}}\leqslant p\leqslant 2W_{\mathrm{id}}$ 中等号均可能成立，例如输入差分为全 0 时。这说明，定理 3 可以由输入差分重量给出差分转移概率“紧凑”的取值范围。

本文的 MILP 差分模型刻画了 R 步 ACE-step（R 是一个正整数），每一步 ACE-step 包含 24 个环形与门组合，则 R 步共包含 $24R$ 个环形与门组合，假设这些环形与门组合之间是相互独立的，对于 R 步 ACE-step 的一条差分链，根据定理 3 容易得到差分链的差分转移概率与环形与门组合的输入差分重量之间的关系，即推论 1。

推论 1　对于 R 步 ACE-step 的一条概率非 0 的差分链，其第 $i(i=0,1,2,\cdots,24R-1)$ 个环形与门组合的输入差分为 $(d_{i,0},d_{i,1},\cdots,d_{i,31})$，令 $W_L=\sum_{i=0}^{24R-1}\sum_{j=0}^{31}d_{i,j}$，则这条差分链的差分转移概率具有形式 $P_L=2^{-p'}$，p' 为非负整数且满足 $\frac{1}{2}W_L\leqslant p'\leqslant 2W_L$。

证明　假设该差分链第 i 个环形与门组合的差分转移概率为 P_i，则有 $P_L=\prod_{i=0}^{24R-1}P_i$，根据定理 1，易得 $P_L=2^{-\sum_{i=0}^{24R-1}p_i}$，且 $\frac{1}{2}W_L\leqslant\sum_{i=0}^{24R-1}p_i\leqslant 2W_L$。证毕。

根据前面的分析，Gurobi 求解器会实时返回当前最优解 CB，且利用 2.2.1 节中的方法可以确定最优解的下界 LB，令 SUM 表示 MILP 模型中所有 $24R$ 个环形与门组合的输入差分变量的和，设定当 Gurobi 求解器长时间没有返回更优的解时，根据当前的最优解 CB 以及最优解的下界 LB 加入以下限制条件。

条件 1　SUM<2CB。

条件 2　$\mathrm{SUM}>\frac{1}{2}(\mathrm{LB}-1)$。

根据推论 1，条件 1 删除了 MILP 模型的部分解，这部分解对应的目标函数不小于 CB，所以必然不包括更优的解；条件 2 删除了 MILP 模型中变量的部分取值，这部分取值必然不构成一个有效解，假设其构成一个有效解，那么该解对应的目标函数小于 LB，产生了矛盾。条件 1 缩减了 MILP 模型的可行域，条件 2 缩减了 MILP 模型中变量的取值范围，这些限制条件使 MILP 模型的求解速度大幅提升。

通过以上加速方法，经过实验验证，3 步 ACE 置换 MILP 差分模型求解时间由 3 700 s 降低到 1 900 s，4 步 ACE 置换 MILP 差分模型求解时间由 24 200 s 降低到 10 600 s，而对于 5 步 ACE 置换，加速前的模型无法在有限时间内完成求解过程，而加速后的模型求解大约花费了 2 天时间。

3　ACE 的差分分析

ACE 算法中的 ACE 置换包含 16 步 ACE-step，本文主要分析了 R 步 ACE-step 的 ACE 置换的差分特征，在本文的分析中，限制 ACE 置换输入差与输出差中 64 bit 比率部分非 0，其余比特为 0。本节

首先给出了文献[24]的差分分析结果，然后给出了本文的分析结果。

3.1 文献[24]的差分分析结果

文献[24]中给出了 ACE 的差分分析结果，目前，对于 ACE 算法，尚没有进一步的差分分析结果，文献[24]利用 MILP 自动搜索技术，求解出 16 步 ACE-step 中活跃 SB-64 数量的最小值为 21，其中 SB-64 的差分转移概率上界为 $2^{-15.8}$，由此得到了 16 步 ACE-step 的最大差分转移概率的上界 $2^{-15.8\times 21}=2^{-331.8}<2^{-320}$，这样 16 步 ACE-step 保证了 ACE 置换达到差分安全边界 2^{-320}，使 ACE 状态与随机 320 bit 状态不可区分。

3.2 本文的差分分析结果

本文对 ACE 置换建立 MILP 差分模型，从而搜索其高概率差分链，ACE 置换中的线性操作包括异或、移位，其中，移位操作只需要改变差分值的位置，不需要进行额外的刻画。

对于比特异或 $a\oplus b=c$，可以用等式 $\Delta a+\Delta b+\Delta c=2\text{dummy}$ 刻画其差分性质，这里需要引入一个整数变量 dummy。

2.1 节将 ACE 置换中的非线性操作转化为 32 维环形与门组合，并给出了其差分性质精确的 MILP 刻画，综上，可对 ACE 置换的差分性质利用 MILP 进行全面的刻画，并通过 Gurobi 求解器进行求解。

本文搜索了 ACE 置换的步数为 1~6 时的差分链，表 4 给出了最优搜索结果，当步数为 1、2 时，没有满足条件的差分链。

表 4 ACE 置换差分链最优搜索结果

步数	差分转移概率
3	2^{-98}
4	2^{-142}
5	2^{-142}
6	2^{-198}

对于表 4 给出的差分链，搜索具有相同输入差、输出差的多条差分链，从而得到更大、更精确的差分传递概率。例如，当步数为 3 时，找到一条概率为 2^{-98} 的差分链，表 5 给出了这条差分链，固定其输入差 ΔS^0 以及输出差 ΔS^3，搜索得到多条大概率的差分链，计算其概率之和为 $2^{-98}\times 6+2^{-99}\times 13+2^{-100}\times 183+2^{-101}\times 627+2^{-102}\times 671\approx 2^{-90.52}$。

对表 4 中 3~6 步的差分链均做此处理，表 6 给出了多条差分链的概率之和。

表 5 3 步 ACE 置换概率为 2^{-98} 的差分链

状态	ΔS^0	ΔS^1	ΔS^2	ΔS^3
A	00000000	00000000	00000001	00000010
	00000000	00000000	00000000	00000000
B	00000000	00000011	00000000	00000000
	00000000	00000000	00000000	00000000
C	00000001	00000000	00000000	00000011
	00000000	00000000	00000000	00000000
D	00000000	00000000	00000001	00000000
	00000000	00000000	00000000	00000000
E	00000000	00000011	00000011	00000000
	00000000	00000000	00000000	00000000

表 6 多条差分链的概率之和

步数	差分转移概率
3	$2^{-90.52}$
4	$2^{-134.14}$
5	$2^{-137.21}$
6	$2^{-190.17}$

根据以上搜索结果，本文给出了减轮认证加密算法 ACE-$\mathcal{AE}$-128 的差分伪造攻击和减轮哈希函数 ACE-$\mathcal{H}$-256 的差分碰撞攻击，当 ACE 置换的步数为 3 时，差分伪造攻击的成功概率为 $2^{-90.52}$，差分碰撞攻击的成功概率为 $2^{-90.52}$。文献[24]指出，ACE-$\mathcal{AE}$-128 的认证安全目标为 128 bit，ACE-$\mathcal{H}$-256 的碰撞安全目标为 128 bit。从表 6 可以看出，4 步 ACE 置换可以保证认证加密算法 ACE-$\mathcal{AE}$-128 抗差分伪造攻击，哈希算法 ACE-$\mathcal{H}$-256 抗差分碰撞攻击。

4 结束语

轻量级密码算法 ACE 是 LWCA 征集活动中第二轮的候选算法，文献[24]给出了较粗略的差分分析结果，为了给出进一步的结果，本文利用自动化分析工具 MILP 对 ACE 算法的差分性质进行研究，首先给出了 ACE 算法非线性操作差分性质精确的 MILP 刻画，实际上，该部分工作可以直接应用到 SIMON、Simeck 等密码算法的分析中；然后给出了 ACE 置换的高概率差分链，并利用多差分技术提高差分链的概率，分别给出了 ACE-$\mathcal{AE}$-128 的差分伪造攻击与哈希函数 ACE-$\mathcal{H}$-256 的差分碰撞攻击。

本文的工作为利用自动化分析工具研究基于与门设计的密码算法的差分性质提供了理论参考

与技术基础，下一步考虑将环形与门组合的 MILP 差分刻画进行扩展并应用到更多相关算法的差分分析中，尝试给出改进的差分分析结果。

参考文献：

[1] POSCHMANN A Y. Lightweight cryptography: cryptographic engineering for a pervasive world[M]. Bochum: Ruhr-University Bochum, 2009.

[2] YANG G Q, ZHU B, SUDER V, et al. The simeck family of lightweight block ciphers[C]//2015 Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015: 307-329.

[3] BANIK S, PANDEY S K, PEYRIN T, et al. GIFT: a small present[C]//2017 Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2017: 321-345.

[4] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]//2007 Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2007: 450-466.

[5] SUZAKI T, MINEMATSU K, MORIOKA S, et al. TWINE: a lightweight block cipher for multiple platforms[C]//2012 Selected Areas in Cryptograph. Berlin: Springer, 2012: 339-354.

[6] 李玮, 汪梦林, 谷大武, 等. 轻量级密码算法TWINE的唯密文故障分析[J]. 通信学报, 2021, 42(3): 135-149.
LI W, WANG M L, GU D W, et al. Ciphertext-only fault analysis of the TWINE lightweight cryptogram algorithm[J]. Journal on Communications, 2021, 42(3): 135-149.

[7] LIU S, GUAN J, HU B. Fault attacks on authenticated encryption modes for GIFT[J]. IET Information Security, 2022, 16(1): 51-63.

[8] 陈平, 廖福成, 卫宏儒. 对轻量级密码算法 MIBS 的相关密钥不可能差分攻击[J]. 通信学报, 2014, 35(2): 190-193, 201.
CHEN P, LIAO F C, WEI H R. Related-key impossible differential attack on a lightweight block cipher MIBS[J]. Journal on Communications, 2014, 35(2): 190-193, 201.

[9] LAWRENCE B. Submission requirements and evaluation criteria for the lightweight cryptography standardization process[M]. Gaithersburg: Submission to NIST-LWC, 2019.

[10] 吴文玲. 认证加密算法研究进展[J]. 密码学报, 2018, 5(1): 70-82.
WU W L. Research advances on authenticated encryption algorithms[J]. Journal of Cryptologic Research, 2018, 5(1): 70-82.

[11] MATSUI M. On correlation between the order of S-boxes and the strength of DES[C]//Advances in Cryptology — EUROCRYPT'94. Berlin: Springer, 1994: 366-375.

[12] WANG S P, HU B, GUAN J, et al. MILP-aided method of searching division property using three subsets and applications[C]//Advances in Cryptology — ASIACRYPT 2019. Berlin: Springer, 2019: 398-427.

[13] KÖLBL S, LEANDER G, TIESSEN T. Observations on the SIMON block cipher family[C]//Advances in Cryptology — CRYPTO 2015. Berlin: Springer, 2015: 161-185.

[14] SONG L, HUANG Z J, YANG Q Q. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA[C]//2016 Information Security and Privacy — 21st Australasian Conference. Berlin: Springer, 2016: 379-394.

[15] SUN S W, GERAULT D, LAFOURCADE P, et al. Analysis of AES, SKINNY, and others with constraint programming[J]. IACR Transactions on Symmetric Cryptology, 2017(1): 281-306.

[16] SUN S W, HU L, WANG P, et al. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers[C]//Advances in Cryptology — ASIACRYPT 2014. Berlin: Springer, 2014: 158-178.

[17] SHI D P, SUN S W, DERBEZ P, et al. Programming the Demirci-Selcuk meet-in-the-middle attack with constraints[C]//Advances in Cryptology — ASIACRYPT 2018. Berlin: Springer, 2018: 3-34.

[18] HU K, SUN S W, TODO Y, et al. Massive superpoly recovery with nested monomial predictions[C]//Advances in Cryptology — ASIACRYPT 2021. Berlin: Springer, 2021: 392-421.

[19] SASAKI Y, TODO Y. New algorithm for modeling S-box in MILP based differential and division trail search[C]//Innovative Security Solutions for Information Technology and Communications. Berlin: Springer, 2017: 150-165.

[20] FU K, WANG M Q, GUO Y H, et al. MILP-based automatic search algorithms for differential and linear trails for speck[C]//Fast Software Encryption. Berlin: Springer, 2016: 268-288.

[21] SAHA D, SASAKI Y, SHI D P, et al. On the security margin of TinyJAMBU with refined differential and linear cryptanalysis[J]. IACR Transactions on Symmetric Cryptology, 2020, 2020(3): 152-174.

[22] ZHOU C N, ZHANG W T, DING T Y, et al. Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach[J]. IACR Transactions on Symmetric Cryptology, 2019(4): 438-469.

[23] 刘帅, 关杰, 胡斌, 等. 基于混合整数线性规划的 MORUS 初始化阶段的差分分析[J]. 电子与信息学报, 2022: doi. 10.11999/JEIT220735.
LIU S, GUAN J, HU B, et al. Differential analysis of the initialization of MORUS based on mixed-integer linear programming[J]. Journal of Electronics & Information Technology, 2022: doi. 10.11999/JEIT220735.

[24] AAGAARD M, ALTAWY R, GONG G, et al. ACE: an authenticated encryption and hash algorithm[M]. Gaithersburg: Submission to NIST-LWC, 2019.

[25] LIU J Y, LIU G Q, QU L J. A new automatic tool searching for impossible differential of NIST candidate ACE[J]. Mathematics, 2020, 8(9): 1576-1587.

[26] 叶涛, 韦永壮, 李灵琛. ACE密码算法的积分分析[J]. 电子与信息学报, 2021, 43(4): 908-914.
YE T, WEI Y Z, LI L C. Integral cryptanalysis of ACE encryption algorithm[J]. Journal of Electronics & Information Technology, 2021, 43(4): 908-914.

[27] CHANG L P, WEI Y C, HE S Y, et al. Research on forgery attack on authentication encryption algorithm ACE[C]//Proceedings of 2022 IEEE 10th Joint International Information Technology and Artificial

Intelligence Conference. Piscataway: IEEE Press, 2022: 1952-1958.

[28] 蒋梓龙, 金晨辉. Saturnin 算法的不可能差分分析[J]. 通信学报, 2022, 43(3): 53-62.
JIANG Z L, JIN C H. Impossible differential cryptanalysis of Saturnin algorithm[J]. Journal on Communications, 2022, 43(3): 53-62.

[29] DUNKELMAN O, LAMBOOIJ E, GHOSH S. Practical related-key forgery attacks on the full TinyJUMBU-192/256[M]. London: Eprint, 2022.

[30] ABDELKHALEK A, SASAKI Y, TODO Y, et al. MILP modeling for (large) S-boxes to optimize probability of differential characteristics[J]. IACR Transactions on Symmetric Cryptology, 2017(4): 99-129.

[31] ALTAWY R, ROHIT R, HE M, et al. Sliscp-light: towards hardware optimized sponge-specific cryptographic permutations[J]. ACM Transactions on Embedded Computing Systems, 2018, 17(4): 1-26.

[作者简介]

刘帅（1993− ），男，山东泰安人，信息工程大学博士生，主要研究方向为认证加密算法的分析与应用等。

关杰（1974− ），女，河南郑州人，博士，信息工程大学教授，主要研究方向为密码理论和密码算法分析等。

胡斌（1971− ），男，河南信阳人，博士，信息工程大学教授，主要研究方向为对称密码算法分析等。

马宿东（1996− ），男，安徽宿州人，信息工程大学博士生，主要研究方向为序列密码算法的分析等。