基于MILP的轻量级密码算法ACE与SPIX的线性分析

刘 帅[1],任小广[1],王世雄[2],关 杰[3],张啸川[1],谭 捷[1],王 军[1]
(1. 智能博弈与决策实验室,北京 100091;2. 军事科学院,北京 100091;
3. 战略支援部队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与SPIX的线性性质. 给出了环型与门组合结构精确的混合整数线性规划下的线性性质刻画,并将算法ACE与SPIX的非线性操作转化为环型与门组合. 基于此构建了ACE置换与SLISCP置换的混合整数线性规划下的线性模型,求解模型得到了2至4步ACE置换与2至5步SLISCP置换最优的线性迹. 证明了7步、12步ACE置换分别达到了128比特与320比特的安全目标,7步、13步SLISCP置换分别达到了128比特与256比特的安全目标. 对于任意步数的ACE置换与SLISCP置换,认证加密算法ACE-AE-128与SPIX均能够抵抗明文处理阶段的线性区分攻击.

关键词: 混合整数线性规划;约束求解;轻量级密码算法;线性分析
基金项目: 国家自然科学基金(No.62102440)
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112(2024)09-3065-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230673

Linear Analysis of Lightweight Cipher ACE and SPIX Based on Mixed-Integer Linear Programming

LIU Shuai[1], REN Xiao-guang[1], WANG Shi-xiong[2],GUAN Jie[3], ZHANG Xiao-chuan[1], TAN Jie[1], WANG Jun[1]
(1. *Intelligent Game and Decision Laboratory*, *Beijing* 100091, *China*; 2. *Academy of Military Science*, *Beijing* 100091, *China*;
3. *School of Cipher Engineering*, *SSF Information Engineering University*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: The linear property of lightweight cipher ACE and SPIX was researched. The linear property of ring AND-gate combination was described accurately with mixed-integer linear programming. The nonlinear operation of ACE and SPIX was transformed into ring AND-gate combination. Based on this, the linear models of ACE permutation and SLISCP permutation were constructed with mixed-integer linear programming. The models returned the optimal linear characteristics of 2-step to 4-step ACE permutation and 2-step to 5-step SLISCP permutation. It was proved that 7-step and 12-step ACE permutation achieved the 128-bit security and 320-bit security respectively, and 7-step and 13-step SLISCP permutation achieved the 128-bit security and 256-bit security respectively. For the ACE permutation and SLISCP permutation with any number of steps, authenticated encryption algorithm ACE-AE-128 and SPIX can resist the linear distinguish attack of plaintext processing stage.

Key words: mixed-integer linear programming; constraint problem solving; lightweight cipher; linear analysis
Foundation Item(s): National Natural Science Foundation of China (No.62102440)

1 引言

物联网技术日新月异,传统的密码算法已经无法满足资源受限场景的需求,轻量级密码算法[1]的出现有效地解决了这一问题,人们提出了一系列性能优异的轻量级密码算法,如Simeck[2]、GIFT[3]、PRESENT[4]、TWINE[5]等,这引发了学者们对轻量级密码算法安全性的研究[6-8].

2016年National Institute of Standards and Technology(NIST)面向全球密码学者征集同时具有认证与加密功能的轻量级密码算法(LightWeight Cryptography,LWC)[9],这一活动极大地推动了轻量级密码算法与认证加密算法[10]的发展.

收稿日期:2023-07-14;修回日期:2024-04-09;责任编辑:李勇锋

轻量级密码算法的结构复杂多样,其设计可以基于分组密码、流密码、置换等不同密码单元,设计方式灵活多样,这在给轻量级密码算法的设计带来活力的同时,也给轻量级密码的安全性分析带来了极大的挑战. 为了有效应对这一问题,自动化分析工具[11]被应用到轻量级密码算法的分析中. 密码算法的自动化分析起源于1994年Matsui的工作[11],他设计了分支定界的自动搜索算法,有效解决了最优差分链、线性链的搜索问题. 此后,自动化分析工具在密码分析中逐渐代替了传统的分析方法[12~15],其中混合整数线性规划(Mixed Integer Linear Programming,MILP)是应用最为广泛的自动化分析工具之一,该方法由Sun等人[16]于2014年提出,起初用来解决搜索密码算法最优差分链、线性链的问题,后来被应用到密码算法的中间相遇攻击、积分攻击等的自动化分析中[17~21]. 在利用MILP工具进行密码算法安全性分析时,模型的求解效率是制约分析结果的主要因素,如何提高MILP模型求解速度是当前的热点问题之一. 2019年,Zhou等人[22]提出了MILP模型求解的分而治之策略,有效提升了基于MILP的SPN结构分组密码算法的差分链、线性链搜索效果. 2022年,Liu等人[23]基于MILP工具给出了MORUS算法初始化阶段的差分分析,根据MORUS算法初始差分状态的重量和取值对MILP模型进行划分,根据子模型之间的循环等价性证明大部分子模型具有相同的最优解,从而提高了模型求解速度.

轻量级密码算法ACE[24]与SPIX[25]都是LWC活动第二轮的候选算法,他们的设计均采用了双工海绵结构,设计者利用MILP自动化分析工具搜索得到非线性环节SB-64的最小活跃数,粗略估计了ACE与SPIX抵抗线性、差分分析的能力,至此仍没有相关工作给出较为精确的线性分析结果. 值得一提的是,2023年刘帅等人[26]定义了环型与门组合,给出了环型与门组合精确的MILP差分刻画,并基于此对算法ACE的差分性质进行分析.

本文主要研究了轻量级密码算法ACE与SPIX的线性性质. 首先将ACE与SPIX中的非线性操作转化为环型与门组合,基于MILP给出了环型与门组合线性性质的精确刻画,从而建立了ACE置换与SLISCP置换的MILP线性模型. 搜索得到了2至4步ACE置换与2至5步SLISCP置换的最优线性链,证明了7步、12步ACE置换分别实现了128比特与320比特的安全目标,7步、13步SLISCP置换分别实现了128比特与256比特的安全目标. 另外限制ACE置换与SLISCP置换输入、输出状态容量部分的掩码为0,当步数为1至7步时MILP模型无解,证明对于任意步数的ACE置换与SLISCP置换,认证加密算法ACE-AE-128与SPIX均能够抵抗明文处理阶段的线性区分攻击.

2 基础知识

2.1 二次型布尔函数的相关度

本节主要介绍一些基本定义、引理以及二次型布尔函数的相关度计算方法.

定义1 n元布尔函数$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)$的相关度为$\mathrm{cor}(f)=\frac{1}{2^n}\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})}$,相关度的重量记为$-\log_2|\mathrm{cor}(f)|$.

引理1[27] 对于n元布尔函数$f(\boldsymbol{x})$,令$\boldsymbol{M}$是一个n阶可逆矩阵,有:$\mathrm{cor}(f(\boldsymbol{x}))=\mathrm{cor}(f(\boldsymbol{xM}))$.

定义2 一个二次布尔函数$f(\boldsymbol{x})$,如果其常数项为0,则称$f(\boldsymbol{x})$为一个二次型.

令$f(x_1,x_2,\cdots,x_n)$是一个二次布尔函数,对于$i\in\{1,2,\cdots,n\}$,$\sigma(f,x_i)$表示$f(x_1,x_2,\cdots,x_n)$中包含变量x_i的二次项的个数.

定义3 令$f(x_1,x_2,\cdots,x_n)$是一个二次型,f的一个二次项x_ix_j叫做独立二次项当且仅当$\sigma(f,x_i)=\sigma(f,x_j)=1$. 如果$f$中所有的二次项都是独立二次项,则称$f$为不相交二次型.

Shi等人[27]给出了不相交二次型相关度的计算方法(引理2),并给出了将二次型变换为不相交二次型的方法(算法1).

引理2 对于一个不相交二次型布尔函数$f=x_{i_1}x_{i_2}\oplus\cdots\oplus x_{i_{2k-1}}x_{i_{2k}}\oplus x_{j_1}\oplus\cdots\oplus x_{j_s}$,有

$$\mathrm{cor}(f)=\begin{cases}(-1)^{\sigma}\cdot 2^{-k}, & \{j_1,j_2,\cdots,j_s\}\subseteq\{i_1,i_2,\cdots,i_{2k}\}\\ 0, & \{j_1,j_2,\cdots,j_s\}\not\subset\{i_1,i_2,\cdots,i_{2k}\}\end{cases}$$

其中,$\sigma=\sum_{t=1}^{k}\mathrm{Coe}_f(x_{i_{2t-1}})\mathrm{Coe}_f(x_{i_{2t}})$,$\mathrm{Coe}_f(x_{i_{2t-1}})$、$\mathrm{Coe}_f(x_{i_{2t}})$分别表示$f$中一次项$x_{i_{2t-1}}$、$x_{i_{2t}}$的系数.

子算法1(PickIndex)[27] 已知二次布尔函数$f(x_1,x_2,\cdots,x_n)$,PickIndex(f)返回最小的下标$t\in\{1,2,\cdots,n\}$,满足$\sigma(f,x_t)\geqslant\sigma(f,x_{t'})$,$t'\in\{1,2,\cdots,n\}$.

子算法2(Substitute)[27] 已知布尔函数$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)$以及$n$阶可逆矩阵$\boldsymbol{M}$,Substitute($f,\boldsymbol{M}$)返回布尔函数$f(\boldsymbol{xM})$.

定义矩阵$\boldsymbol{I}$为n阶单位矩阵,$\boldsymbol{I}_{u\leftarrow t_1,t_2,\cdots,t_m}$表示一个$n$阶矩阵,其第$u$列中第$t_i(1\leqslant i\leqslant m)$个元素为1,其余元素为0,其余各列均与$\boldsymbol{I}$相同,算法1[27]展示了将二次型变换为不相交二次型的完整过程.

根据算法1以及引理2,可以计算任意二次型的相关度.

2.2 轻量级密码算法ACE与SPIX

2016年,NIST面向全球密码学者征集轻量级密码算法[9],并于2019年公布了第二轮候选算法,包括

算法1　不相交二次型变换

输入:二次型$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)$.

输出:n阶可逆矩阵$\boldsymbol{M}$,不相交二次型$\hat{f}(\boldsymbol{x})=f(\boldsymbol{xM})$.

初始化阶段:$\boldsymbol{M}\leftarrow\boldsymbol{I}$,$\hat{f}(\boldsymbol{x})=f(\boldsymbol{x})$,$v\leftarrow$ PickIndex($\hat{f}$).

变换阶段:

while $\sigma(\hat{f},x_v)\geqslant 2$ do

$m\leftarrow\sigma(\hat{f},x_v)$;

寻找所有$t_1<t_2<\cdots<t_m$满足$x_vx_{t_i}$是$\hat{f}$中的二次项;

$\hat{f}\leftarrow$ Substitute($\hat{f},\boldsymbol{I}_{t_1\leftarrow t_1,t_2,\cdots,t_m}$);

$\boldsymbol{M}\leftarrow\boldsymbol{I}_{t_1\leftarrow t_1,t_2,\cdots,t_m}\cdot\boldsymbol{M}$;

if $\sigma(\hat{f},x_{t_1})\geqslant 2$ then

$k\leftarrow\sigma(\hat{f},x_{t_1})$;

寻找所有$s_1<s_2<\cdots<s_k$,满足$x_{t_1}x_{s_i}$是$\hat{f}$中的二次项;

$\hat{f}\leftarrow$ Substitute($\hat{f},\boldsymbol{I}_{v\leftarrow s_1,s_2,\cdots,s_k}$);

$\boldsymbol{M}\leftarrow\boldsymbol{I}_{v\leftarrow s_1,s_2,\cdots,s_k}\cdot\boldsymbol{M}$;

end

$v\leftarrow$ PickIndex($\hat{f}$);

end

返回$\boldsymbol{M}$、$\hat{f}(\boldsymbol{x})$.

ACE[24]与SPIX[25]. 在介绍这两个算法之前,先来了解其共同的非线性环节SB-64. SB-64采用8轮Feistel结构,分组规模为64,其轮函数与分组密码Simeck[2]相同,图1展示了SB-64的轮函数. 其中$f_{(5,0,1)}(x)=(L^5(x)\odot x)\oplus L^1(x)$,$L^i(x)$为$x$循环左移$i$位,$\odot$为比特与,给定8比特的常数$\mathrm{rc}=(q_7,q_6,\cdots,q_0)$,令$\gamma_r=1^{31}\|q_r$,$r=0,1,\cdots,7$.

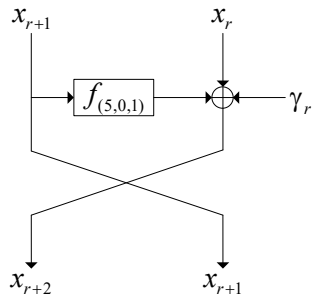


图1　SB-64轮函数

2.2.1　ACE算法

ACE算法包含两个算法,分别为哈希算法ACE-H-256与认证加密算法ACE-AE-128,ACE算法为双工海绵结构,其主体部分为ACE置换,ACE置换迭代了16步ACE-step(如图2所示),分组规模为320,(A^i,B^i,C^i,D^i,E^i),$i=0,1,2,\cdots,16$,表示ACE置换的第i步状态,其中第i步ACE-step中使用了6个8比特的常数$\mathrm{rc}_0^i,\mathrm{rc}_1^i,\mathrm{rc}_2^i,\mathrm{sc}_0^i,\mathrm{sc}_1^i,\mathrm{sc}_2^i$.

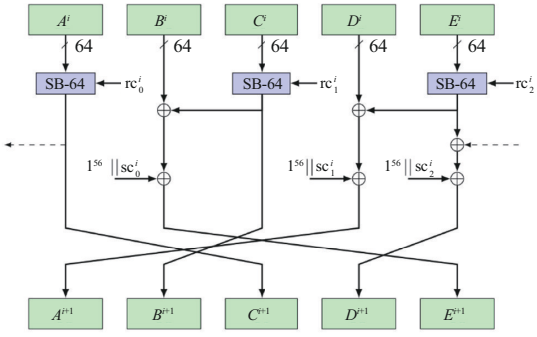


图2　ACE-step

算法ACE-H-256与ACE-AE-128的状态$S=A\|B\|C\|D\|E$的规模为320比特,其中64比特为比率部分(rate part),记为S_r,由$A[7]$、$A[6]$、$A[5]$、$A[4]$、$C[7]$、$C[6]$、$C[5]$、$C[4]$共8个字节组成,其中$A[j]$为A的第j字节,$C[j]$为C的第j字节. 状态中其余256比特为容量部分(capacity part),记为S_c. 图3给出了认证加密算法ACE-AE-128的加密过程,由左至右包含四个阶段:初始化阶段、相关数据处理阶段、明文处理阶段、认证码生成阶段. 图4给出了哈希算法ACE-H-256的示意图,由左至右包含三个阶段:初始化阶段、吸收阶段、挤压阶段.

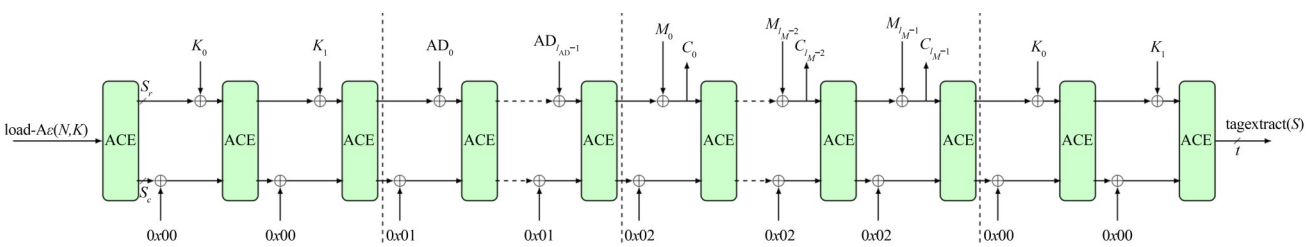


图3　认证加密算法ACE-AE-128

2.2.2　SPIX算法

认证加密算法SPIX的设计采用了双工海绵结构,SPIX算法的主体部分为SLISCP-light-256置换,后面简称SLISCP置换. SLISCP置换规模为256比特,由

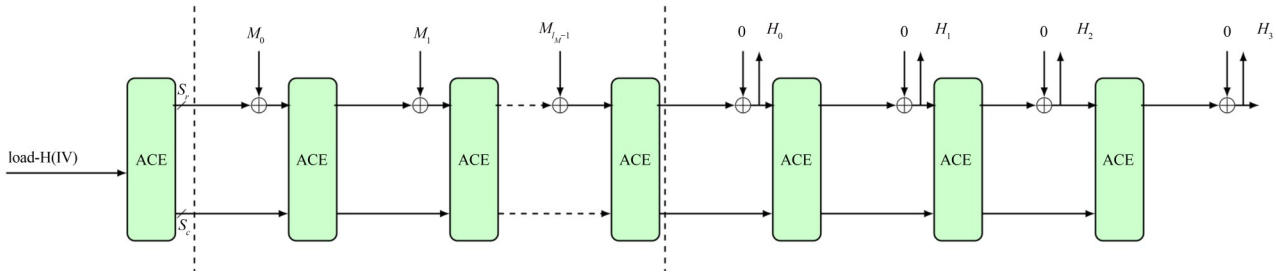


图4 哈希算法ACE-H-256

SLISCP-step迭代$s(s=9,18)$步构成，记作P^s. SLISCP置换第i步状态表示为4个64比特字$(X_0^i,X_1^i,X_2^i,X_3^i)$, $i=0,1,2,\cdots,s$. 图5展示了SLISCP-step，其中，第i步SLISCP-step中使用了4个8比特的常数$\mathrm{rc}_0^i,\mathrm{rc}_1^i,\mathrm{sc}_0^i,\mathrm{sc}_1^i$.

认证加密算法SPIX的状态大小为256比特，状态X中有64比特进行数据的吸收与输出，即比率部分，记为X_r，其余192比特为容量部分，记为X_c. SPIX的比率部分由256比特状态$X=X_0\|X_1\|X_2\|X_3$中8个字节组成：$X_1[7]$、$X_1[6]$、$X_1[5]$、$X_1[4]$、$X_3[7]$、$X_3[6]$、$X_3[5]$、$X_3[4]$，其中$X_1[j]$、$X_3[j]$分别表示X_1、X_3的第j字节. 图6给出了认证加密算法SPIX的加密过程，由左至右包含四个阶段：初始化阶段、相关数据处理阶段、明文处理阶段、认证码生成阶段.

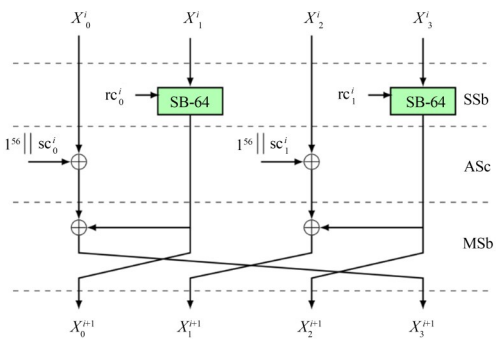


图5 SLISCP-step

本文主要研究了ACE置换与SLISCP置换的线性特征，对于ACE与SPIX的更多细节，请参照设计报告[24,25].

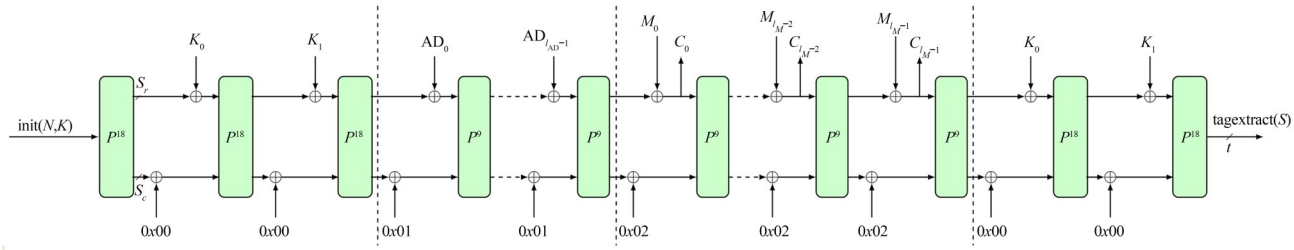


图6 认证加密算法SPIX的加密过程

3 环型与门组合及其MILP线性刻画

本文工作的主要目的是利用MILP自动化搜索技术得到ACE置换与SLISCP置换相关度较大的线性链，需要给出其所有操作的MILP线性刻画，即利用线性（及少量二次）不等式来约束线性掩码，排除零相关的线性链，MILP模型的目标函数为线性链相关度的重量. ACE置换与SLISCP置换中的线性操作（逐比特异或、分支）的MILP线性刻画是直接的[16]，与门是其唯一的非线性操作，若不考虑与门之间的相互关系，对于单个与门，设输入掩码a、b，输出掩码c，可以利用如下线性不等式对其线性特征进行刻画[27]：

$$a\leqslant c, b\leqslant c.$$

其中相关度的重量为c. 然而在ACE置换、SLISCP置换中，与门之间存在很大的关联性，这将大大影响线性链搜索的精确性，本节将ACE置换、SLISCP置换中的非线性操作整合为一类结构——环型与门组合[25]，充分考虑与门之间的相互关系，给出了该结构精确的MILP线性刻画.

3.1 环型与门组合

由2.2节，ACE、SPIX中的非线性环节SB-64轮函数中所有与门可以表示为：

$$y=L^5(x)\odot x$$

将上面式子逐比特展开，得到$y=(x_{31}x_{26},x_{30}x_{25},x_{29}x_{24},\cdots,x_1x_{28},x_0x_{27})$，对$y$的32个比特做一个置换得到$y'=(x_0x_{27},x_{27}x_{22},x_{22}x_{17},x_{17}x_{12},\cdots,x_{10}x_5,x_5x_0)$，这里将这一类函数表示为：

$$g(x_0,x_1,\cdots,x_{n-1})=(x_0x_1,x_1x_2,\cdots,x_{n-2}x_{n-1},x_{n-1}x_0)$$

$g(x_0,x_1,\cdots,x_{n-1})$为$n$维环型与门组合[25]，其中$x_ix_{i+1}$为其第$i$个与门$(i=0,1,\cdots,n-1)$，图7给出了环型与门组合的示意图.

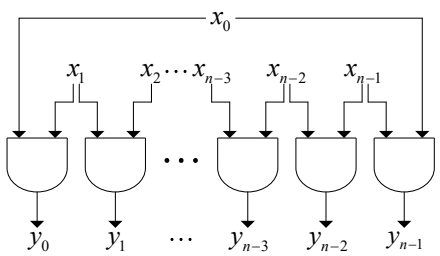


图7　n维环型与门组合

经过上述推导，SB-64轮函数中的与门组合$y=L^5(x)\odot x$实际是一个32维环型与门组合[25]，3.2节将给出n维环型与门组合精确的MILP线性刻画. 2020年，Saha等人[21]基于MILP刻画了函数$f(x_0,x_1,\cdots,x_{n-1})=(x_0x_1,x_1x_2,\cdots,x_{n-2}x_{n-1})$的线性性质(我们称该函数为链型与门组合)，并分析了认证加密算法TinyJUMBU的线性性质. n维环型与门组合在链型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}，这使得n个与门之间的相互关系更加复杂.

在下文关于$g(x_0,x_1,\cdots,x_{n-1})$的相关描述中，总是默认下标的计算模$n$，为了描述简洁不再一一标注.

3.2　环型与门组合精确的MILP线性刻画

对于函数g的MILP线性刻画，往往将其拆解成单个与门的线性刻画，而不考虑与门输入、输出之间的相互关系，这种相互关系会大大影响函数整体的相关度，从而得到不精确的刻画，所以这里将函数g看作一个整体进行精确的线性刻画. 先给出两类函数相关度的计算，对于$m\geqslant 2,n\geqslant 3$，分别定义函数

$$W_1=\bigoplus_{i=0}^{m-2}x_ix_{i+1}\oplus\bigoplus_{i=0}^{m-1}a_ix_i$$

$$W_2=\bigoplus_{i=0}^{n-2}x_ix_{i+1}\oplus x_0x_{n-1}\oplus\bigoplus_{i=0}^{n-1}b_ix_i$$

其中，W_1的第一部分$\bigoplus_{i=0}^{m-2}x_ix_{i+1}$是一个$m$维链型与门组合、$W_2$的第一部分$\bigoplus_{i=0}^{n-2}x_ix_{i+1}\oplus x_0x_{n-1}$是一个$n$维环型与门组合，$a_i,b_i\in\{0,1\}$分别表示$W_1$、$W_2$中一次项的系数，称$W_1$为$m$维I型函数、$W_2$为$n$维II型函数.

定理1给出了W_1、W_2相关度的计算方法，这里借助了Shi等人[27]给出的方法，将二次布尔函数转化为不相交二次型，进而利用引理2计算其相关度. 对于W_1第一部分链型与门组合的相关度，Saha等人[21]在其工作中进行了讨论并给出了其MILP线性刻画，为了进一步的推导，借助Shi等人的方法将其以公理化的形式展现出来.

定理1　对于$m\geqslant 2,n\geqslant 3$，$W_1$为$m$维I型函数、$W_2$为$n$维II型函数，其相关度如下：

(1) 对于W_1，当m是偶数时，

$$|\mathrm{cor}(W_1)|=2^{-\frac{m}{2}}$$

当m是奇数时，

$$|\mathrm{cor}(W_1)|=\begin{cases}2^{-\frac{m-1}{2}}, & \bigoplus_{j=0}^{(m-1)/2}a_{2j}=0\\ 0, & \bigoplus_{j=0}^{(m-1)/2}a_{2j}=1\end{cases}$$

(2) 对于W_2，当n是偶数时，

$$|\mathrm{cor}(W_2)|=\begin{cases}2^{-\frac{n-2}{2}}, & \bigoplus_{i=0}^{n/2-1}b_{2i}=\bigoplus_{i=0}^{n/2-1}b_{2i+1}=0\\ 0, & \bigoplus_{i=0}^{n/2-1}b_{2i}=1\text{或}\bigoplus_{i=0}^{n/2-1}b_{2i+1}=1\end{cases}$$

当n是奇数时，

$$|\mathrm{cor}(W_2)|=\begin{cases}2^{-\frac{n-1}{2}}, & \bigoplus_{i=0}^{n-1}b_i=1\\ 0, & \bigoplus_{i=0}^{n-1}b_i=0\end{cases}$$

证明　根据定义2，显然W_1、W_2是两个二次型，根据2.1节中的算法1，将二次型W_1、W_2分别变换为不相交二次型.

对于$\hat{W}_1$，当$m \bmod 2=0$，有

$$\hat{W}_1=\bigoplus_{i=0}^{m/2-1}x_{2i}x_{2i+1}\oplus\bigoplus_{i=0}^{m/2-1}[(\bigoplus_{j=0}^{i}a_{2j})x_{2i}\oplus a_{2i+1}x_{2i+1}]$$

当$m \bmod 2=1$，有

$$\hat{W}_1=\bigoplus_{i=0}^{(m-3)/2}x_{2i}x_{2i+1}\oplus\bigoplus_{i=0}^{(m-3)/2}[(\bigoplus_{j=0}^{i}a_{2j})x_{2i}\oplus a_{2i+1}x_{2i+1}]\oplus(\bigoplus_{j=0}^{(m-1)/2}a_{2j})x_{m-1}$$

对于$\hat{W}_2$，当$n \bmod 2=0$，有

$$\hat{W}_2=\bigoplus_{i=0}^{n/2-2}x_{2i}x_{2i+1}\oplus\bigoplus_{i=0}^{n/2-2}[(\bigoplus_{j=0}^{i}b_{2j})x_{2i}\oplus b_{2i+1}x_{2i+1}]\oplus(\bigoplus_{i=0}^{n/2-1}b_{2i})x_{n-2}\oplus(\bigoplus_{i=0}^{n/2-1}b_{2i+1})x_{n-1}$$

当$n \bmod 2=1$，有

$$\hat{W}_2=\bigoplus_{i=0}^{(n-3)/2}x_{2i}x_{2i+1}\oplus\bigoplus_{i=0}^{(n-3)/2}[(\bigoplus_{j=0}^{i}b_{2j})x_{2i}\oplus b_{2i+1}x_{2i+1}]\oplus[(\bigoplus_{i=0}^{n-1}b_i)\oplus 1]x_{n-1}$$

根据引理1，$\hat{W}_1$、$\hat{W}_2$为不相交二次型，根据2.1节的引理2，计算$\hat{W}_1$、$\hat{W}_2$的相关度，定理1的结论是显然的.

证毕.

对于n维环型与门组合$g(x_0,x_1,\cdots,x_{n-1})$，令$\mathrm{im}_i\in\{0,1\},i=0,1,2,\cdots,n-1$，表示输入比特$x_i$的线性掩

码，令 $\mathrm{om}_i\in\{0,1\}, i=0,1,2,\cdots,n-1$，表示输出比特 x_ix_{i+1} 的线性掩码，则 g 的线性逼近表达式为

$$L_g(\mathrm{im}_0,\mathrm{im}_1,\cdots,\mathrm{im}_{n-1},\mathrm{om}_0,\mathrm{om}_1,\cdots,\mathrm{om}_{n-1})=\bigoplus_{i=0}^{n-1}\mathrm{im}_i\cdot x_i\oplus\bigoplus_{i=0}^{n-1}\mathrm{om}_i\cdot x_ix_{i+1}.$$

当 om_i 不全为 1 时，将满足 $\mathrm{om}_i=1$ 的下标集合记为 $I=\{i|\mathrm{om}_i=1, i\in\{0,1,\cdots,n-1\}\}$，明显 I 可以表示为 $I=\bigcup_{j=1}^{p}\{i_j,i_j+1,\cdots,i_j+s_j-1\}$，且对于 $j\in\{1,2,\cdots,p\}$，$\mathrm{om}_{i_j-1}=0$、$\mathrm{om}_{i_j+s_j}=0$（下标的计算是模 n 的），这种表示是唯一的，称 $I=\bigcup_{j=1}^{p}\{i_j,i_j+1,\cdots,i_j+s_j-1\}$ 是 L_g 的一个全分割，令 $O=\{i|\mathrm{om}_{i-1}=0,\mathrm{om}_i=0,i\in\{0,1,\cdots,n-1\}\}$.

定理 2 对于环型与门组合 $g(x_0,x_1,\cdots,x_{n-1})$，$L_g(\mathrm{im}_0,\mathrm{im}_1,\cdots,\mathrm{im}_{n-1},\mathrm{om}_0,\mathrm{om}_1,\cdots,\mathrm{om}_{n-1})$ 为其线性逼近表达式，当 om_i 不全为 1 时，令 $I=\bigcup_{j=1}^{p}\{i_j,i_j+1,\cdots,i_j+s_j-1\}$ 是 L_g 的一个全分割，$O=\{i|\mathrm{om}_{i-1}=0,\mathrm{om}_i=0,i\in\{0,1,\cdots,n-1\}\}$，则 L_g 可以表示成如下形式：

$$L_g=\bigoplus_{j=1}^{p}L_j(\boldsymbol{x}_j)\oplus\bigoplus_{i\in O}\mathrm{im}_ix_i$$

其中向量 $\boldsymbol{x}_j=(x_{i_j},x_{i_j+1},\cdots,x_{i_j+s_j})$，$L_j(\boldsymbol{x}_j)=\bigoplus_{t=0}^{s_j-1}x_{i_j+t}x_{i_j+t+1}\oplus\bigoplus_{t=0}^{s_j}\mathrm{im}_{i_j+t}x_{i_j+t}$ 是 s_j+1 维 I 型函数，又有 $\mathrm{cor}(L_g)=[\prod_{j=1}^{p}\mathrm{cor}(L_j(\boldsymbol{x}_j))]\cdot\mathrm{cor}(\bigoplus_{i\in O}\mathrm{im}_ix_i)$.

（1）当 $O\neq\varnothing$ 时，如果存在 $i\in O$：$\mathrm{im}_i=1$，则 $\mathrm{cor}(L_g)=0$；如果对于所有 $i\in O$，均满足 $\mathrm{im}_i=0$，则 $\mathrm{cor}(L_g)=\prod_{j=1}^{p}\mathrm{cor}(L_j(\boldsymbol{x}_j))$；

（2）当 $O=\varnothing$ 时，$\mathrm{cor}(L_g)=\prod_{j=1}^{p}\mathrm{cor}(L_j(\boldsymbol{x}_j))$.

证明 首先，定义一个辅助集合 $I^*=\bigcup_{j=1}^{p}\{i_j,i_j+1,\cdots,i_j+s_j\}$，明显有 $I^*\cap O=\varnothing$ 且 $I^*\cup O=\{0,1,\cdots,n-1\}$，则有

$$\begin{aligned}L_g&=\bigoplus_{i=0}^{n-1}\mathrm{om}_i\cdot x_ix_{i+1}\oplus\bigoplus_{i=0}^{n-1}\mathrm{im}_i\cdot x_i\\&=\bigoplus_{i=0}^{n-1}\mathrm{om}_ix_ix_{i+1}\oplus(\bigoplus_{i\in I^*}\mathrm{im}_i\cdot x_i\oplus\bigoplus_{i\in O}\mathrm{im}_ix_i)\\&=(\bigoplus_{j=1}^{p}\bigoplus_{t=0}^{s_j-1}x_{i_j+t}x_{i_j+t+1})\oplus(\bigoplus_{j=1}^{p}\bigoplus_{t=0}^{s_j}\mathrm{im}_{i_j+t}x_{i_j+t}\oplus\bigoplus_{i\in O}\mathrm{im}_ix_i)\\&=\bigoplus_{j=1}^{p}[\bigoplus_{t=0}^{s_j-1}x_{i_j+t}x_{i_j+t+1}\oplus\bigoplus_{t=0}^{s_j}\mathrm{im}_{i_j+t}x_{i_j+t}]\oplus\bigoplus_{i\in O}\mathrm{im}_ix_i\\&=\bigoplus_{j=1}^{p}L_j(\boldsymbol{x}_j)\oplus\bigoplus_{i\in O}\mathrm{im}_ix_i.\end{aligned}$$

其中 $L_j(\boldsymbol{x}_j)=\bigoplus_{t=0}^{s_j-1}x_{i_j+t}x_{i_j+t+1}\oplus\bigoplus_{t=0}^{s_j}\mathrm{im}_{i_j+t}x_{i_j+t}$ 是 s_j+1 维 I 型函数，其中 $\boldsymbol{x}_j=(x_{i_j},x_{i_j+1},\cdots,x_{i_j+s_j})$，由堆积引理[27]，明显有 $\mathrm{cor}(L_g)=[\prod_{j=1}^{p}\mathrm{cor}(L_j(\boldsymbol{x}_j))]\cdot\mathrm{cor}(\bigoplus_{i\in O}\mathrm{im}_ix_i)$.

证毕.

例 1 已知 8 维环型与门组合 $g(x_0,x_1,\cdots,x_7)$ 以及 g 的一个线性逼近表达式 L_g，如果 $(\mathrm{om}_0,\mathrm{om}_1,\mathrm{om}_2,\mathrm{om}_3,\mathrm{om}_4,\mathrm{om}_5,\mathrm{om}_6,\mathrm{om}_7)=(1,1,0,0,1,1,0,1)$，则 L_g 的全分割为 $I=\{4,5\}\bigcup\{7,0,1\}$，$O=\{3\}$. $L_g=L_1(4,5,6)\oplus L_2(7,0,1,2)\oplus\mathrm{im}_3x_3$，其中：

$$L_0(4,5,6)=x_4x_5\oplus x_5x_6\oplus\mathrm{im}_4x_4\oplus\mathrm{im}_5x_5\oplus\mathrm{im}_6x_6,$$

$$L_1(7,0,1,2)=x_7x_0\oplus x_0x_1\oplus x_1x_2\oplus\mathrm{im}_7x_7\oplus\mathrm{im}_0x_0\oplus\mathrm{im}_1x_1\oplus\mathrm{im}_2x_2.$$

已知 n 维环型与门组合 $g(x_0,x_1,\cdots,x_{n-1})$ 及其一个线性逼近表达式 $L_g(\mathrm{im}_0,\mathrm{im}_1,\cdots,\mathrm{im}_{n-1},\mathrm{om}_0,\mathrm{om}_1,\cdots,\mathrm{om}_{n-1})$，如果 om_i 不全为 1，定理 2 给出了求解 L_g 相关度的方法，如果 om_i 全为 1，L_g 是一个 n 维 II 型函数，可以直接利用定理 1 求解其相关度.

下面根据以上的讨论给出 $g(x_0,x_1,\cdots,x_{n-1})$ 的 MILP 线性刻画，目标是利用限制条件排除使得 $\mathrm{cor}(L_g)=0$ 的线性掩码 $(\mathrm{im}_0,\mathrm{im}_1,\cdots,\mathrm{im}_{n-1},\mathrm{om}_0,\mathrm{om}_1,\cdots,\mathrm{om}_{n-1})$，以及利用线性目标函数表示出相关度的重量 $-\log_2|\mathrm{cor}(L_g)|$，对于每个 im_i，$i=0,1,\cdots,n-1$，添加一对辅助变量 $l_i^{i-1},l_i^i\in\{0,1\}$，满足关系 $\mathrm{im}_i=l_i^{i-1}\oplus l_i^i$，转化为 MILP 限制条件 $i=0,1,\cdots,n-1$：

$$\mathrm{im}_i+l_i^{i-1}+l_i^i=2\mathrm{dummy}_i \tag{1}$$

其中 dummy_i 是一个整数变量，又给出下面限制条件（om_i 不全为 1 时，$\beta=0$，om_i 全为 1 时，$\beta=1$）：

$$\beta=\mathrm{om}_0\mathrm{om}_1\cdots\mathrm{om}_{n-1} \tag{2}$$

如果存在 $i\in O$，使得 $\mathrm{im}_i=1$，根据定理 2，有 $\mathrm{cor}(L_g)=0$，据此给出以下限制条件 $i=0,1,\cdots,n-1$：

$$\begin{aligned}l_i^i&\leqslant\mathrm{om}_i\\l_{i+1}^i&\leqslant\mathrm{om}_i\end{aligned} \tag{3}$$

上述条件使得：对于 $i\in O$，根据集合 O 的定义有 $\mathrm{om}_{i-1}=0,\mathrm{om}_i=0$，则 $l_i^{i-1}=l_i^i=0$，所以 $\mathrm{im}_i=l_i^{i-1}\oplus l_i^i=0$，排除了 $\mathrm{im}_i=1, i\in O$ 的情况.

另外，当 om_i 不全为 1 时，由定理 2，如果 $\mathrm{cor}(L_j(\boldsymbol{x}_j))=0, j=1,\cdots,p$，$\mathrm{cor}(L_g)=0$，$L_j(\boldsymbol{x}_j)=\bigoplus_{t=0}^{s_j-1}x_{i_j+t}x_{i_j+t+1}\oplus\bigoplus_{t=0}^{s_j}\mathrm{im}_{i_j+t}x_{i_j+t}$ 是 s_j+1 维 I 型函数，根据定理 1，当 s_j 是偶数且 $\bigoplus_{t=0}^{s_j/2}\mathrm{im}_{i_j+2t}=1$ 时，$\mathrm{cor}(L_j(\boldsymbol{x}_j))=0$，据此给出以下限制条件 $i=0,1,\cdots,n-1$，令 $\beta_i\in\{0,1\}$：

$$\begin{aligned}&\beta_i=\overline{\beta_{i-1}}\,\mathrm{om}_i\mathrm{om}_{i+1}\overline{\beta}\\&l_i^i-l_{i+2}^{i+1}\leqslant 1-\beta_i\\&l_{i+2}^{i+1}-l_i^i\leqslant 1-\beta_i\end{aligned}\tag{4}$$

当om_i全为1时,$\overline{\beta}=0,\beta_i=0$,式(4)对$l_i^i$、$l_{i+2}^{i+1}$不起任何限制作用,$\mathrm{om}_i$不全为1时,$\overline{\beta}=1$,根据$L_g$的全分割的定义,$\mathrm{om}_{i_j-1}=0$、$\mathrm{om}_{i_j+s_j}=0$、$\mathrm{om}_{i_j+t}=1,\ t=0,1,\cdots,s_j-1$,根据式(4),则有$\beta_{i_j-1}=0$,

$$\beta_{i_j+t}=\begin{cases}1, & t\in\{0,2,4,\cdots,2\left\lfloor\frac{s_j}{2}\right\rfloor-2\}\\0, & t\in\{1,3,5,\cdots,2\left\lfloor\frac{s_j}{2}\right\rfloor-1\}\end{cases}$$

则有$\sum_{t=0}^{s_j-1}\beta_{i_j+t}=\left\lfloor\frac{s_j-1}{2}\right\rfloor$,下面分别就$s_j$为偶数和奇数时的情况进行分析.

(1) 当s_j为偶数时,则有$l_{i_j+2t}^{i_j+2t}=l_{i_j+2t+2}^{i_j+2t+1}$,$t=0,1,\cdots,\frac{s_j}{2}-1$,根据$\mathrm{om}_{i_j-1}=0$、$\mathrm{om}_{i_j+s_j}=0$以及式(3),有$l_{i_j}^{i_j-1}=0$、$l_{i_j+s_j}^{i_j+s_j}=0$,则

$$\begin{aligned}\bigoplus_{t=0}^{s_j/2}\mathrm{im}_{i_j+2t}&=\bigoplus_{t=0}^{s_j/2}(l_{i_j+2t}^{i_j+2t-1}\oplus l_{i_j+2t}^{i_j+2t})\\&=l_{i_j}^{i_j-1}\oplus\bigoplus_{t=0}^{s_j/2-1}(l_{i_j+2t}^{i_j+2t}\oplus l_{i_j+2t+2}^{i_j+2t+1})\oplus l_{i_j+s_j}^{i_j+s_j}=0\end{aligned}$$

则以上限制条件排除了$\mathrm{cor}(L_j(\boldsymbol{x}_j))=0$的情况,此时$|\mathrm{cor}(L_j(\boldsymbol{x}_j))|=2^{-\frac{s_j}{2}}=2^{-(s_j-\sum_{t=0}^{s_j-1}\beta_{i_j+t})}$.

(2) 当s_j为奇数时,根据定理1,有$|\mathrm{cor}(L_j(\boldsymbol{x}_j))|=2^{-\frac{s_j+1}{2}}=2^{-(s_j-\sum_{t=0}^{s_j-1}\beta_{i_j+t})}$.

在上述限制条件下,当om_i不全为1时,令集合$\overline{I}=\{0,1,\cdots,n-1\}-I$,对于$i\in\overline{I}$,由于$\mathrm{om}_i=0$,则$\beta_i=0$,

$$\begin{aligned}|\mathrm{cor}(L_g)|&=\prod_{j=1}^{p}|\mathrm{cor}(L_j(\boldsymbol{x}_j))|=\prod_{j=1}^{p}2^{-(s_j-\sum_{t=0}^{s_j-1}\beta_{i_j+t})}\\&=2^{-\sum_{j=1}^{p}(s_j-\sum_{t=0}^{s_j-1}\beta_{i_j+t})}=2^{-(\sum_{i=0}^{n-1}\mathrm{om}_i-(\sum_{i\in I}\beta_i+\sum_{i\in\overline{I}}\beta_i))}=2^{-(\sum_{i=0}^{n-1}\mathrm{om}_i-\sum_{i=0}^{n-1}\beta_i)}.\end{aligned}$$

从而令MILP模型的目标函数为$\sum_{i=0}^{n-1}\mathrm{om}_i-\sum_{i=0}^{n-1}\beta_i$.

当om_i全为1时,$L_g=\bigoplus_{i=0}^{n-1}x_ix_{i+1}\oplus\bigoplus_{i=0}^{n-1}\mathrm{im}_i\cdot x_i$是一个$n$维II型函数:

(1) n是偶数时,根据定理1,为了排除$\mathrm{cor}(L_g)=0$的情况,给出以下限制条件:

$$\begin{aligned}&\sum_{i=0}^{n/2-1}\mathrm{im}_{2i}+(\beta+1)\mathrm{dummy}_1^*=0\\&\sum_{i=0}^{n/2-1}\mathrm{im}_{2i+1}+(\beta+1)\mathrm{dummy}_2^*=0\end{aligned}\tag{5}$$

其中dummy_1^*、dummy_2^*是整数变量,当om_i全为1时,$\beta=1$,则式(5)使得$\bigoplus_{i=0}^{n/2-1}\mathrm{im}_{2i}=0$且$\bigoplus_{i=0}^{n/2-1}\mathrm{im}_{2i+1}=0$,排除了$\mathrm{cor}(L_g)=0$的情况,且$|\mathrm{cor}(L_g)|=2^{-\frac{n-2}{2}}=2^{-(n-\frac{n+2}{2})}=2^{-(\sum_{i=0}^{n-1}\mathrm{om}_i-\frac{n+2}{2}\beta)}$.

(2) n是奇数时,根据定理1,为了排除$\mathrm{cor}(L_g)=0$的情况,给出以下限制条件:

$$\sum_{i=0}^{n-1}\mathrm{im}_i+(\beta+1)\mathrm{dummy}^*=1\tag{6}$$

其中dummy^*是整数变量,当om_i全为1时,$\beta=1$,则式(6)使得$\bigoplus_{i=0}^{n-1}\mathrm{im}_i=1$,排除了$\mathrm{cor}(L_g)=0$,且$|\mathrm{cor}(L_g)|=2^{-\frac{n-1}{2}}=2^{-(n-\frac{n+1}{2})}=2^{-(\sum_{i=0}^{n-1}\mathrm{om}_i-\frac{n+1}{2}\beta)}$.

当om_i不全为1时,$\beta=0$,式(5)(6)不起任何限制作用. 至此,给出了环型与门组合$g(x_0,x_1,\cdots,x_{n-1})$完整的MILP线性刻画:

(1) n是偶数时,限制条件为式(1)(2)(3)(4)(5),目标函数为

$$\min\sum_{i=0}^{n-1}\mathrm{om}_i-\sum_{i=0}^{n-1}\beta_i-\frac{n+2}{2}\beta.$$

(2) n是奇数时,限制条件为式(1)(2)(3)(4)(6),目标函数为

$$\min\sum_{i=0}^{n-1}\mathrm{om}_i-\sum_{i=0}^{n-1}\beta_i-\frac{n+1}{2}\beta.$$

4　ACE与SPIX算法的线性分析

本节根据第2节的分析与结果,对于ACE置换、SLISCP置换分别建立MILP线性模型,根据对输入掩码、输出掩码的限制分为以下两类场景:

类型1:输入掩码、输出掩码均非0;

类型2:输入掩码、输出掩码比率部分非0,容量部分为0.

ACE的认证加密算法ACE-AE-128与认证加密算法SPIX均包含四个阶段:初始化阶段、相关数据处理阶段、明文处理阶段、认证码生成阶段,图8给出了算法ACE-AE-128与SPIX明文处理阶段的示意图,其中,ACE-AE-128采用了16步的ACE置换,SPIX采用了9步的SLISCP置换P^9.

如图8,假设已知置换类型2的线性对应$(\alpha_1,\beta_1)\to(\alpha_2,\beta_2)$,其相关度的重量为$\omega$,$\alpha_1\neq 0$、$\beta_1=0$分别为输入掩码的比率部分、容量部分,$\alpha_2\neq 0$、$\beta_2=0$分别为输出掩码的比率部分、容量部分,建立线性逼近表达式($\circ$表示向量的点积):

$$\alpha_1\circ C_i\oplus\alpha_2\circ(M_{i+1}\oplus C_{i+1}).$$

在已知明密文的情况下,可以构造明文处理阶段的线性区分攻击,需要的数据量为$2^{2\omega}$.

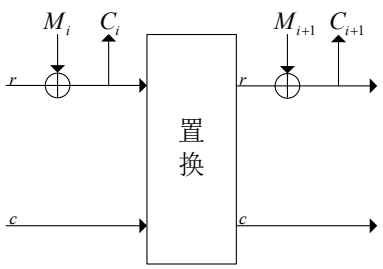


图8 认证加密算法ACE-AE-128与SPIX的明文处理阶段

类型1的线性链包含类型2的线性链，保证算法类型1下的抗线性攻击能力是一类更强的安全目标，需要置换迭代更多的步数. 但随着置换步数的增加，其实现代价也相应地增加，所以如何在更少的步数下实现一定的安全目标是一个意义深远的问题. 算法ACE与SPIX的设计者给出了保证类型1条件下ACE置换与SLISCP置换抗线性攻击能力所需要迭代的最少步数，4.1节展示了他们的分析过程与结果.

4.1 已有的线性分析结果

算法ACE与SPIX的设计者均对算法做出了128比特的安全性声明，他们给出了ACE置换与SLISCP置换粗略的线性分析，利用MILP求解SB-64的最小活跃数，从而给出线性链相关度平方的上界，表1列出了他们的分析结果，目前对算法ACE、SPIX，尚没有进一步的线性分析结果.

表1 算法ACE、SPIX已有的线性分析结果

置换	步数	类型1线性链相关性平方的上界
ACE置换	16	$2^{-327.6}$
SLISIC置换	9	$2^{-140.4}$
	18	$2^{-280.8}$

ACE置换（状态规模为320比特）迭代16步时，类型1线性链相关度平方的上界为$2^{-327.6}$，其安全性超过了状态规模. SLISCP置换（状态规模为256比特）迭代9步时，类型1线性链相关度平方的上界为$2^{-140.4}$，达到了设计者声明的128比特安全边界，SLISCP置换迭代18步时，类型1线性链相关度平方的上界为$2^{-280.8}$，其安全性超过了状态规模.

4.2 本文的线性分析结果

本文的实验主要依赖4台个人电脑完成，Intel® Core™ i7-7700HQ @ 2.80 GHz处理器，16 GB内存（2 400 MHz），利用Gurobi 9.5.1对MILP模型进行求解，对本文所有结果的求解总时间约为1个月. 随着步数的增加，模型的求解将变得十分困难. 相关实验代码已上传至Github，网址为https://github.com/noselfcrown/RAC_cipher_linear_analysis，对ACE、SPIX进行线性攻击的完整MILP约束描述可通过运行代码生成，以.lp文件输出保存.

4.2.1 类型1限制下ACE置换与SLISCP置换的线性分析

在类型1的限制下构建MILP模型，搜索ACE置换与SLISCP置换的线性链，表2给出了置换步数为2至6步时的搜索结果（线性链相关度的平方），其中“*”表示计算能力不足以完成整个搜索过程，不能保证得到的线性链为最优解.

表2 类型1线性链搜索结果

步数	2	3	4	5	6
ACE置换	2^{-18}	2^{-54}	2^{-108}	2^{-162}*	2^{-252}*
SLISCP置换	2^{-18}	2^{-36}	2^{-78}	2^{-116}	2^{-162}*

由表2，当步数为2至4步时，ACE置换类型1线性链相关度平方的上界分别为2^{-18}、2^{-54}、2^{-108}；当步数为2至5步时，SLISCP置换类型1线性链相关度平方的上界分别为2^{-18}、2^{-36}、2^{-78}、2^{-116}. 这是由于这些结果都是MILP模型搜索得到的最优解.

根据Matsui的分支定界理论[11]，假设n_1步置换的类型1线性链相关度平方的上界为ρ_1，n_2步置换的类型1线性链相关度平方的上界为ρ_2，则n_1+n_2步置换的类型1线性链相关度平方的上界为$\rho_1\cdot\rho_2$. 据此，我们可以根据低步数置换的结果推出更高步数置换的类型1线性链相关度平方的上界，并给出算法ACE与SPIX更紧致的安全边界.

算法ACE的安全边界：

（1）由于3步ACE置换的类型1线性链相关度平方的上界为2^{-54}，4步ACE置换的类型1线性链相关度平方的上界为2^{-108}，容易得到7步ACE置换的类型1线性链相关度平方的上界为$2^{-54}\times 2^{-108}=2^{-162}$，所以7步ACE置换可以保证128比特的安全目标.

（2）由于4步ACE置换的类型1线性链相关度平方的上界为2^{-108}，得到12步ACE置换的类型1线性链相关度平方的上界为$2^{-108\times 3}=2^{-324}$，所以12步ACE置换可以保证320比特（状态规模）的安全目标.

算法SPIX的安全边界：

（1）由于2步SLISCP置换的类型1线性链相关度平方的上界为2^{-18}，5步SLISCP置换的类型1线性链相关度平方的上界为2^{-116}，得到7步SLISCP置换的类型1线性链相关度平方的上界为$2^{-18}\times 2^{-116}=2^{-134}$，所以7步SLISCP置换可以保证128比特的安全目标.

（2）由于3步SLISCP置换的类型1线性链相关度平方的上界为2^{-36}，5步SLISCP置换的类型1线性链相关度平方的上界为2^{-116}，得到13步SLISCP置换的类型1线性链相关度平方的上界为$2^{-36}\times 2^{-116}\times 2^{-116}=2^{-268}$，所以13步SLISCP置换可以保证256比特（状态规模）的安

全目标.

4.2.2 类型2限制下ACE置换与SLISCP置换的线性分析

如图8,对于认证加密算法ACE-AE-128与SPIX,如果存在相关度较大的类型2线性链,可以针对明文处理阶段构造线性区分攻击.在类型2的限制下构建MILP模型,搜索ACE置换与SLISCP置换的线性链,考察算法ACE-AE-128、SPIX的明文处理阶段抗线性区分攻击的能力,表3列出了搜索结果,其中"∅"表示模型无解(不存在类型2的线性链),"—"表示模型求解未完成且当前未搜索到有效解.

表3　类型2线性链搜索结果

步数	1	2	3	4	5	6	7	8
ACE置换	∅	∅	∅	∅	∅	∅	∅	—
SLISCP置换	∅	∅	∅	∅	∅	∅	∅	—

由表3,当步数为1至7步时,ACE置换与SLISCP置换均不存在有效的类型2线性链;而当步数大于等于8时,由4.2.1节可知,ACE置换与SLISCP置换均达到了128比特的安全目标.综上,对于任意步数的ACE置换与SLISCP置换,认证加密算法ACE-AE-128与SPIX均具有抵抗明文处理阶段线性区分攻击的能力.

5 总结

本文研究了轻量级密码算法ACE与SPIX的线性性质,ACE置换、SLISCP置换分别为算法ACE、SPIX的主体部分.首先,给出了环型与门组合结构精确的MILP线性刻画,并将算法ACE与SPIX中的非线性操作转化为环型与门组合.基于此构建了ACE置换与SLISCP置换的MILP线性模型,求解模型得到了若干步数置换最优的线性链,细致地分析了算法ACE与SPIX的抗线性攻击能力,给出了算法ACE的128比特与320比特更精确的安全边界,以及算法SPIX的128比特与256比特更精确的安全边界.证明了对于任意步数的ACE置换与SLISCP置换,认证加密算法ACE-AE-128与SPIX均具有抵抗明文处理阶段线性区分攻击的能力.

下一步工作将着手研究更加复杂的与门组合的MILP刻画问题,并应用于密码算法的安全性分析中.

参考文献

[1] POSCHMANN A Y. Lightweight Cryptography: Cryptographic Engineering for a Pervasive World[D]. Bochum: Ruhr-University Bochum, 2009.

[2] YANG G Q, ZHU B, SUDER V, et al. The simeck family of lightweight block ciphers[C]//International Workshop on 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]//International Conference on Cryptographic Hardware and Embedded Systems. Cham: Springer, 2017: 321-345.

[4] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: An ultra-lightweight block cipher[C]//International Workshop on 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]//International Conference on Selected Areas in Cryptography. Berlin: Springer, 2013: 339-354.

[6] 罗芳, 欧庆于, 周学广, 等. 轻量级分组密码MIBS-80算法的Biclique分析[J]. 软件学报, 2015, 26(Suppl.(1)): 8-16.
LUO F, OU Q Y, ZHOU X G, et al. A biclique cryptanalysis on lightweight block cipher MIBS-80[J]. Journal of Software, 2015, 26(Suppl.(1)): 8-16. (in Chinese)

[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] 李浪, 李肯立, 贺位位, 等. Magpie:一种高安全的轻量级分组密码算法[J]. 电子学报, 2017, 45(10): 2521-2527.
LI L, LI K L, HE W W, et al. Magpie: A high-security lightweight block cipher[J]. Acta Electronica Sinica, 2017, 45(10): 2521-2527. (in Chinese)

[9] Lawrence B. Submission requirements and evaluation criteria for the lightweight cryptography standardization process [EB/OL]. (2018). https://csrc.nist.gov/projects/lightweight-cryptography.

[10] 吴文玲. 认证加密算法研究进展[J]. 密码学报, 2018, 5(1): 68-82.
WU W L. Research advances on authenticated encryption algorithms[J]. Journal of Cryptologic Research, 2018, 5(1): 68-82. (in Chinese)

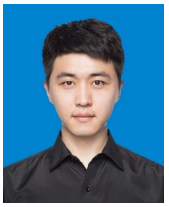
[11] MITSURU M. On correlation between the order of S-boxes and the strength of DES[C]//Advances in Cryptology — EUROCRYPT' 94. Berlin: Springer, 1995: 366-375.

[12] WANG S P, HU B, GUAN J, et al. MILP-aided method of searching division property using three subsets and applications[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2019: 398-427.

[13] KÖLBL S, LEANDER G, TIESSEN T. Observations on the SIMON block cipher family[C]//Annual Cryptology

Conference. 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]//Australasian Conference on Information Security and Privacy. Cham: 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: 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]//International Conference on the Theory and Application of Cryptology and Information Security. 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]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2018: 3-34.
[18] HU K, SUN S W, TODO Y, et al. Massive superpoly recovery with nested monomial predictions[M]//Lecture Notes in Computer Science. Cham: Springer, 2021: 392-421.
[19] SASAKI Y, TODO Y. New algorithm for modeling S-box in MILP based differential and division trail search [C]//International Conference for Information Technology and Communications. Cham: 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]//International Conference on 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: 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, 2020: 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, 2023, 45(7): 2537-2545.
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, 2023, 45(7): 2537-2545. (in Chinese)
[24] AAGAARD M, ALTAWY R, GONG G, et al. ACE: An authenticated encryption and hash algorithm[EB/OL]. (2018). https://csrc. nist. gov/projects/lightweight-cryptography.
[25] RIHAM A, GONG G, MORGAN H, et al. SPIX: An authenticated cipher submission to the NIST LWC competition [EB/OL]. (2019). https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/spix-spec-round2.pdf.
[26] 刘帅, 关杰, 胡斌, 等. 基于MILP的轻量级密码算法ACE的差分分析[J]. 通信学报, 2023, 44(1): 39-48.
LIU S, GUAN J, HU B, et al. Differential analysis of lightweight cipher algorithm ACE based on MILP[J]. Journal on Communications, 2023, 44(1): 39-48. (in Chinese)
[27] SHI DP, SUN SW, YU S, et al. Correlation of quadratic boolean functions: Cryptanalysis of all versions of full MORUS[C]//CRYPTO 2019. Santa Barbara: Springer, 2019: 180-209.

作者简介



刘 帅 男, 1993年12月出生于山东省泰安市. 现为智能博弈与决策实验室助理研究员. 主要研究方向为认证加密算法的分析与应用、深度学习等.
E-mail: sssshuai1993@163.com

关 杰 女, 1974年9月出生于河南省郑州市. 现为信息工程大学密码工程学院教授、博士生导师. 主要研究方向为密码理论和密码算法分析等.