一种变体BISON分组密码算法及分析

赵海霞[①②③] 韦永壮*[②] 刘争红[①]

[①](桂林电子科技大学认知无线电与信息处理省部共建教育部重点实验室 桂林 541004)

[②](桂林电子科技大学广西密码学与信息安全重点实验室 桂林 541004)

[③](桂林电子科技大学数学与计算科学学院 桂林 541004)

摘 要：该文基于Whitened Swap-or-Not(WSN)的结构特点，分析了Canteaut 等人提出的Bent whItened Swap Or Not –like (BISON-like) 算法的最大期望差分概率值(MEDP)及其(使用平衡函数时)抵御线性密码分析的能力；针对BISON算法迭代轮数异常高(一般为3n轮，n为数据分组长度)且密钥信息的异或操作由不平衡Bent函数决定的情况，该文采用了一类较小绝对值指标、高非线性度、较高代数次数的平衡布尔函数替换BISON算法中的Bent函数，评估了新变体BISON算法抵御差分密码分析和线性密码分析的能力。研究结果表明：新的变体BISON算法仅需迭代n轮；当n较大时(如n=128或256)，其抵御差分攻击和线性攻击的能力均接近理想值。且其密钥信息的异或操作由平衡函数来决定，故具有更好的算法局部平衡性。

关键词：差分密码分析；线性密码分析；WSN结构；BISON-like分组密码算法；变体BISON分组密码算法

中图分类号：TN918.2; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)07-1796-07

DOI: 10.11999/JEIT190517

A Variant BISON Block Cipher Algorithm and Its Analysis

ZHAO Haixia[①②③] WEI Yongzhuang[②] LIU Zhenghong[①]

[①](*Key Laboratory of Cognitive Radio and Information Processing*, *Ministry of Education*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

[②](*Guangxi Key Laboratory of Cryptography and Information Security*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

[③](*School of Mathematics and Computational Science*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: Based on the characteristics of Whitened Swap-or-Not (WSN) construction, the maximum expected differential probability (MEDP) of Bent whItened Swap Or Not -like (BISON-like) algorithm proposed by Canteaut et al. is analyzed in this paper. In particular, the ability of BISON-like algorithm with balanced nonlinear components against linear cryptanalysis is also investigated. Notice that the number of iteration rounds of BISON algorithm is rather high (It needs usually to iterate 3n rounds, n is the block length of data) and Bent function (unbalanced) is directly used to XOR with the secret key bits. In order to overcome these shortcomings, a kind of balanced Boolean functions that has small absolute value indicator, high nonlinearity and high algebraic degree is selected to replace the Bent functions used in BISON algorithm. Moreover, the abilities of this new variant BISON algorithm against both the differential cryptanalysis and the linear cryptanalysis are estimated. It is shown that the new variant BISON algorithm only needs to iterate n-round function operations; If n is relative large (e.g. n=128 or n=256), Its abilities against both the differential

收稿日期：2019-07-10；改回日期：2020-03-08；网络出版：2020-03-20

*通信作者： 韦永壮 walker_wyz@guet.edu.cn

基金项目：国家自然科学基金(61572148, 61872103)，广西科技计划项目基金(桂科AB18281019)，广西自然科学基金(2017GXNSFBA198056)，认知无线电与信息处理省部共建教育部重点实验室主任基金(CRKL180107)，广西密码学与信息安全重点实验室基金(GCIS201706)

Foundation Items: The National Natural Science Foundation of China (61572148, 61872103), The Foundation of Guangxi Science and Technology Program (Guike AB18281019). The Natural Science Foundation of Guangxi (2017GXNSFBA198056), The Foundation of Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) (CRKL180107), The Foundation of Guangxi Key Laboratory of Cryptography and Information Security (GCIS201706)

cryptanalysis and the linear cryptanalysis almost achieve ideal value. Furthermore, due to the balanced function is directly XORed with the secret key bits of the variant algorithm, it attains a better local balance indeed.

Key words: Differential cryptanalysis; Linear cryptanalysis; Whitened Swap-Or-Not construction; Bent whItened Swap Or Not -like block cipher algorithm; Variant BISON block cipher algorithm

1　引言

分组密码具有速度快、易于标准化和便于软硬件实现等优点，所以在网络空间安全领域有着广泛的应用。分组密码的设计要兼顾安全性和实现性，其基本设计思想是通过多轮迭代将一个弱密码部件堆积成一个强密码部件，例如AES算法就是建立在多轮置换之上设计的[1]，置换之间插入轮密钥加，这样的密码称为密钥交替密码[2,3]。最著名的交替密码算法采用的是迭代的Even-Mantour结构[4,5]。文献[6]给出了r轮迭代Even - Mantour结构的严格安全界,即攻破r轮迭代Even-Mantour结构，攻击者大概需进行$2^{rn/(r+1)}$次oracle查询，其中n为分组长度。这说明迭代Even-Mantour结构的安全性不但依赖于分组长度n，而且与轮数r也息息相关。注意到，Even-Mantour密码结构算法的差分界和线性界较难分析，即使是采用宽轨迹设计策略的AES算法，也要通过分析其扩散层的分支数及超级S盒的性能才能确定其差分界和线性界[7,8]。为了获得更紧致的安全界以降低对随机置换及轮数r的依赖，文献[9]在Swap-Or-Not结构基础之上提出了Whitened Swap-Or-Not(WSN)结构。该结构不依赖于随机置换，仅需要2个公共的随机(布尔)函数。遗憾的是文献[9]并未讨论WSN结构实例化的问题。随后，文献[10]给出了一个WSN结构的算法，但是由于其加密函数的某些部分是线性的，故该算法很快就被攻破了[11]。在2019欧洲密码年会上，Canteaut等人[12]基于WSN结构新提出Bent whItened Swap Or Not –like(BISON-like)算法，并重点研究了其中的BISON算法实例抵御差分攻击、线性攻击及代数攻击的能力。与传统的宽轨迹设计策略(如基于SPN算法)不同的是：BISON算法的最大期望差分概率(MEDP)和最大期望线性概率(MELP)的计算方法简单，且与部件的确切细节无关。然而，BISON算法采用2次Bent函数，这导致了该算法设计中存在一些不足：该算法所需的迭代轮数异常高(一般为3n轮，n为数据分组长度)，且密钥信息的异或操作由不平衡Bent函数来决定。此外该算法的数据分组长度n严格为奇数，不利于针对字节的计算机指令级运算。

鉴于BISON算法的上述缺点，本文基于WSN的结构特点，分析了BISON-like算法的最大期望差分概率值及其(使用平衡函数时)抵御线性密码分析的能力；使用一类绝对值指标小、非线性度高、代数次数高的平衡布尔函数代替Bent函数做非线性部件，我们称之为变体BISON算法。研究结果证实：新的变体算法仅需迭代n轮；当n较大时(如n=128或256)，该变体BISON算法抵御差分攻击和线性攻击的能力与BISON算法的相当，均接近理想的情况。另一方面，该变体BISON算法的密钥信息的异或操作由平衡函数来决定，具有更好的算法局部平衡性。此外，该算法的数据分组长度n可为奇数也可为偶数，便于数据的读取和算法的实现。

本文余下结构如下：第2节介绍基础知识。第3节，介绍BISON-like算法；讨论了BISON-like算法的最大期望差分概率；对非线性部件$f_{b(i)}$为平衡函数的BISON-like算法进行线性密码分析。第4节，提出变体BISON算法，并对其进行了差分密码分析与线性密码分析。第5节总结全文。

2　基础知识

定义 1[13]　f为n元布尔函数，$\boldsymbol{a}\in F_2^n$, f在$\boldsymbol{a}$处的Walsh谱值为$W_f(\boldsymbol{a})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{f(\boldsymbol{x})+\boldsymbol{a}\cdot\boldsymbol{x}}$，其中$\boldsymbol{a}\cdot\boldsymbol{x}$为$\boldsymbol{a}$与$\boldsymbol{x}$的内积。

定义 2[13]　f为n元布尔函数，f的非线性度$N_f:=\min\limits_{l(\boldsymbol{x})\in L_n[\boldsymbol{x}]}\{d(f(\boldsymbol{x}),l(\boldsymbol{x}))\}$。$N_f$与$W_f(\boldsymbol{a})$的关系为

$$N_f=2^{n-1}-2^{-1}\max_{\boldsymbol{a}}|W_f(\boldsymbol{a})| \tag{1}$$

定义 3[14]　设f为n元布尔函数，则f的平方和指标$\sigma_f=\sum_{\boldsymbol{s}\in F_2^n}{\Delta_f}^2(\boldsymbol{s})$, f的绝对值指标$\Delta_f=\max\limits_{\boldsymbol{s}\in F_2^n,\boldsymbol{s}\neq 0}|\Delta_f(\boldsymbol{s})|$，其中$\Delta_f(\boldsymbol{s})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{s})}$为$f$的自相关函数。

σ_f与N_f的关系、$\Delta_f(\boldsymbol{s})$与$W_f(\boldsymbol{a})$的关系[15]为

$$N_f\le 2^{n-1}-2^{-n/2-1}\sqrt{\sigma_f} \tag{2}$$

$$W_f{}^2(\boldsymbol{a})=\sum_{\boldsymbol{s}\in F_2^n}\Delta_f(\boldsymbol{s})(-1)^{\boldsymbol{a}\cdot\boldsymbol{s}} \tag{3}$$

定义 4[16]　迭代分组密码的一条r轮差分特征$\Omega=(\boldsymbol{\delta_0},\boldsymbol{\delta_1},\cdots,\boldsymbol{\delta_r})$所对应的概率DP$(\Omega)$是指在轮密钥$\boldsymbol{k_1},\boldsymbol{k_2},\cdots,\boldsymbol{k_r}$取值独立且均匀分布的情形下，当输入对的差分值为$\boldsymbol{\delta_0}$时，中间状态$(\boldsymbol{y_i},\boldsymbol{y_i}^*)$的差分值

满足 $\boldsymbol{y_i}+\boldsymbol{y_i}^*=\boldsymbol{\delta_i}, 1\le i\le r$ 的概率，$\mathrm{DP}(\Omega)=\prod_{i=1}^{r}\mathrm{DP}(\boldsymbol{\delta_{i-1}},\boldsymbol{\delta_i})$。

定义5[16] 迭代分组密码的一条r轮线性特征$\boldsymbol{\theta}=(\boldsymbol{\theta_0},\boldsymbol{\theta_1},\cdots,\boldsymbol{\theta_r})$所对应的线性概率$\mathrm{LP}(\boldsymbol{\theta})$是指在轮密钥$\boldsymbol{k_1},\boldsymbol{k_2},\cdots,\boldsymbol{k_r}$取值独立且均匀分布的情形下，当输入掩码为$\boldsymbol{\theta_0}$时，中间状态$\boldsymbol{y_i}$的掩码为$\boldsymbol{\theta_i}$, $1\le i\le r$ 的概率，$\mathrm{LP}(\boldsymbol{\theta})=\prod_{i=1}^{r}LP(\boldsymbol{\theta_{i-1}},\boldsymbol{\theta_i})$。

MEDP和MELP的理想值分别为2^{-n}和0，因此算法设计者希望迭代分组密码的MEDP与MELP均尽量接近理想值。

3 BISON-like算法介绍

WSN结构的轮函数$R_{\boldsymbol{k_i},\boldsymbol{w_i}}(\boldsymbol{x}):F_2^n\to F_2^n$，其定义[9]为$R_{\boldsymbol{k_i},\boldsymbol{w_i}}(\boldsymbol{x})=\boldsymbol{x}+f_{b(i)}(\boldsymbol{w_i}+\max\{\boldsymbol{x},\boldsymbol{x}+\boldsymbol{k_i}\})\boldsymbol{k_i}$。其中$\boldsymbol{k_i},\boldsymbol{w_i}$为轮密钥，$\boldsymbol{w_i}$为白化密钥；$f_{b(i)}\in\{f_0,f_1\}$, f_0和f_1为两个随机函数，若整个算法是m轮的，则前$m/2$轮采用f_0，后$m/2$轮采用f_1；$\max\{\boldsymbol{x},\boldsymbol{x}+\boldsymbol{k_i}\}$按字典序取$\boldsymbol{x}$与$\boldsymbol{x}+\boldsymbol{k_i}$的最大值。可用其他函数$\Phi_{\boldsymbol{k_i}}(\boldsymbol{x})$替换其中的最大值函数，但要求$\Phi_{\boldsymbol{k_i}}$满足条件：$\Phi_{\boldsymbol{k_i}}(\boldsymbol{x})=\Phi_{\boldsymbol{k_i}}(\boldsymbol{y})$当且仅当$\boldsymbol{y}\in\{\boldsymbol{x},\boldsymbol{x}+\boldsymbol{k_i}\}$，值得注意的是$\mathrm{Ker}\Phi_{\boldsymbol{k_i}}=\{\boldsymbol{0},\boldsymbol{k_i}\}$的线性函数$\Phi_{\boldsymbol{k_i}}(\boldsymbol{x})$满足该条件。

为抵御已知明文攻击，WSN结构的算法必须至少迭代n轮；为抵御差分攻击和回旋攻击(Boomerang attack)，轮函数中的随机函数$f_{b(i)}$必须依赖所有输入比特。考虑到上述限制条件，文献[12]将采用WSN结构且满足下述条件的算法称为BISON-like算法。

定义6[12] BISON-like算法的轮函数$R_{\boldsymbol{k_i},\boldsymbol{w_i}}(\boldsymbol{x}):F_2^n\to F_2^n$的定义为

$$R_{\boldsymbol{k_i},\boldsymbol{w_i}}(\boldsymbol{x})=\boldsymbol{x}+f_{b(i)}(\boldsymbol{w_i}+\Phi_{\boldsymbol{k_i}}(\boldsymbol{x}))\boldsymbol{k_i}\tag{4}$$

其中$\boldsymbol{k_i}$,$\boldsymbol{w_i}$为轮密钥，$\boldsymbol{w_i}$为白化密钥，$\boldsymbol{k_i}$线性独立[17]。$f_{b(i)}$为$n-1$元布尔函数；$\Phi_{\boldsymbol{k_i}}(\boldsymbol{x}):F_2^n\to F_2^{n-1}$为线性函数，且$\mathrm{Ker}\Phi_{\boldsymbol{k_i}}=\{\boldsymbol{0},\boldsymbol{k_i}\}$；算法至少迭代$n$轮。特别地，当$f_{b(i)}$为Bent函数时，称之为BISON算法。

注1 本文分析遵循对称密码分析的两个基本假设：各轮白化密钥线性独立；轮密钥满足随机等价假设。

3.1 BISON-like算法的差分密码分析

文献[12]关于BISON-like算法的差分密码分析的主要结论如下所述。

引理1[12] BISON-like算法中的轮函数$R_{\boldsymbol{k_i},\boldsymbol{w_i}}(\boldsymbol{x})$的DDT为：

当$\boldsymbol{\beta}=\boldsymbol{\alpha}$时，$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}+\Delta_f(\Phi_{\boldsymbol{k_i}}(\boldsymbol{\alpha}))$；当$\boldsymbol{\beta}=\boldsymbol{\alpha}+\boldsymbol{k_i}$时，$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}-\Delta_f(\Phi_{\boldsymbol{k_i}}(\boldsymbol{\alpha}))$；在其余差分对处$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=0$。特别地，若$f_{b(i)}$为Bent函数，则轮函数的DDT为：当$\boldsymbol{\beta}=\boldsymbol{\alpha}=\boldsymbol{k_i}$或$\boldsymbol{\beta}=\boldsymbol{\alpha}=\boldsymbol{0}$时，$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^n$；当$\boldsymbol{\beta}\in\{\boldsymbol{\alpha},\boldsymbol{\alpha}+\boldsymbol{k_i}\}$且$\boldsymbol{\alpha}\notin\{\boldsymbol{0},\boldsymbol{k_i}\}$时，$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}$；在其余差分对处$\mathrm{DDT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=0$。

引理2[12] 对n轮BISON-like算法，设轮密钥$\boldsymbol{k_1},\boldsymbol{k_2},\cdots,\boldsymbol{k_n}$线性独立，则对任意输入差分$\boldsymbol{\alpha}$, $\boldsymbol{\alpha}\ne\boldsymbol{0}$及任意输出差分$\boldsymbol{\beta}$有$\mathrm{EDP}^n(\boldsymbol{\alpha},\boldsymbol{\beta})\le\left(2^{-1}+2^{-n}\max\limits_{1\le i\le n}\Delta_{f_{b(i)}}\right)^{n-1}$。特别地，若$f_{b(i)}$为Bent函数，则有：当$\boldsymbol{\beta}=\sum_{j=l+1}^{n}\lambda_j\boldsymbol{k_j}$时，$\mathrm{EDP}^n(\boldsymbol{\alpha},\boldsymbol{\beta})=0$；当$\boldsymbol{\beta}=\boldsymbol{k_l}+\sum_{j=l+1}^{n}\lambda_j\boldsymbol{k_j}$时，$\mathrm{EDP}^n(\boldsymbol{\alpha},\boldsymbol{\beta})=2^{-n+1}$；在其余差分对处，$\mathrm{EDP}^n(\boldsymbol{\alpha},\boldsymbol{\beta})=2^{-n}$。其中$\boldsymbol{k_l}$为$\boldsymbol{\alpha}$在基$(\boldsymbol{k_1},\boldsymbol{k_2},\ldots,\boldsymbol{k_n})$下的分解式$\boldsymbol{\alpha}=\boldsymbol{k_l}+\sum_{j=1}^{l-1}\lambda_j{}^{\alpha}\boldsymbol{k_j}$中的最后一个轮密钥。

命题1[12] 设轮数$r\ge n$，轮密钥$\boldsymbol{k_1},\boldsymbol{k_2},\cdots,\boldsymbol{k_n}$线性独立，则BISON算法的$\mathrm{MEDP}=2^{-(n-1)}$。

文献[12]仅讨论了r轮($r\ge n$)BISON算法的MEDP。下面讨论r轮($r\ge n$)BISON-like算法的MEDP。

定理 1 设轮密钥$\boldsymbol{k_1},\boldsymbol{k_2},\cdots,\boldsymbol{k_n}$线性独立，则$r\,(r\ge n)$轮BISON-like算法的最大期望差分概率为

$$\mathrm{MEDP}=\left(2^{-1}+2^{-n}\max_{1\le i\le n}\Delta_{f_{b(i)}}\right)^{n-1}。$$

证明 由引理2知，对于n轮的BISON-like算法，其$\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}]\le\left(2^{-1}+2^{-n}\max\limits_{1\le i\le n}\Delta_{f_{b(i)}}\right)^{n-1}$。记$n+1$轮的差分特征为$(\boldsymbol{\delta_0},\boldsymbol{\delta_1},\cdots,\boldsymbol{\delta_n},\boldsymbol{\delta_{n+1}})$, $\boldsymbol{\delta_0}=\boldsymbol{\alpha}$, $\boldsymbol{\delta_i}=\boldsymbol{\alpha}+\sum_{j=1}^{i}\lambda_j\boldsymbol{k_j}$, $\boldsymbol{\delta_{n+1}}=\boldsymbol{\beta}$。由BISON-like算法轮函数可知$\boldsymbol{\delta_{n+1}}=\boldsymbol{\delta_n}+\lambda_{n+1}\boldsymbol{k_{n+1}}$, $\lambda_{n+1}\in\{0,1\}$。故$\boldsymbol{\beta}$能被达到当且仅当$\boldsymbol{\delta_n}=\boldsymbol{\beta}$或$\boldsymbol{\delta_n}=\boldsymbol{\beta}+\boldsymbol{k_{n+1}}$，从而

$$\begin{aligned}\mathrm{EDP}^{n+1}[\boldsymbol{\alpha},\boldsymbol{\beta}]=&\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\delta_n}]\Pr_{\boldsymbol{w_{n+1}}}[R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}(\boldsymbol{x})\\&+R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}(\boldsymbol{x}+\boldsymbol{\delta_n})=\boldsymbol{\beta}]\\=&\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}]\Pr_{\boldsymbol{w_{n+1}}}[R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}(\boldsymbol{x})\\&+R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}(\boldsymbol{x}+\boldsymbol{\beta})=\boldsymbol{\beta}]\\&+\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}+\boldsymbol{k_{n+1}}]\Pr_{\boldsymbol{w_{n+1}}}\\&[R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}(\boldsymbol{x})+R_{\boldsymbol{k_{n+1}},\boldsymbol{w_{n+1}}}\\&(\boldsymbol{x}+\boldsymbol{\beta}+\boldsymbol{k_{n+1}})=\boldsymbol{\beta}]。\end{aligned}$$

当$\boldsymbol{\beta}\ne\boldsymbol{k_{n+1}}$时，$\mathrm{EDP}^{n+1}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{-1}\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}]+2^{-1}\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}+\boldsymbol{k_{n+1}}]\le\left(2^{-1}+2^{-n}\max\limits_{1\le i\le n}\Delta_{f_{b(i)}}\right)^{n-1}$。

当$\boldsymbol{\beta}=\boldsymbol{k_{n+1}}$时，$\mathrm{EDP}^{n+1}[\boldsymbol{\alpha},\boldsymbol{\beta}]=1\times\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}]+0\times\mathrm{EDP}^n[\boldsymbol{\alpha},\boldsymbol{\beta}+\boldsymbol{k_{n+1}}]\le\left(2^{-1}+2^{-n}\max\limits_{1\le i\le n}\Delta_{f_{b(i)}}\right)^{n-1}$。

综上可得，$r\,(r\geq n)$轮BISON-like算法的$\mathrm{MEDP}=\left(2^{-1}+2^{-n}\max\limits_{1\leq i\leq n}\Delta_{f_{b(i)}}\right)^{n-1}$。

证毕

3.2 f为平衡函数的BISON-like算法的线性密码分析

本节将讨论当式(4)中的非线性部件$f_{b(i)}$为平衡函数时，BISON-like算法的1轮及多轮的线性密码分析。式(4)中的$\Phi_{\boldsymbol{k}_i}$的定义与文献[12]相同，其表达式为

$$\Phi_{\boldsymbol{k}_i}(\boldsymbol{x})=\left(x_{j(\boldsymbol{k}_i)}\boldsymbol{k}_i+\boldsymbol{x}\right)\cdot[1,2,\cdots,j(\boldsymbol{k}_i)-1,j(\boldsymbol{k}_i)+1,\cdots,n]\quad(5)$$

其中$j(\boldsymbol{k}_i)$为密钥$\boldsymbol{k}_i$的比特1的最小下标，易证明$\Phi_{\boldsymbol{k}_i}$为线性函数且$\mathrm{Ker}\Phi_{\boldsymbol{k}_i}=\{\boldsymbol{0},\boldsymbol{k}_i\}$。

定理2　设BISON-like算法的轮函数$R_{\boldsymbol{k}_i,\boldsymbol{w}_i}$的表达式如式(4)、式(5)所示，$f_{b(i)}$为$n-1$元平衡布尔函数，则$R_{\boldsymbol{k}_i,\boldsymbol{w}_i}$的线性逼近表为：当$\boldsymbol{\alpha}=\boldsymbol{\beta}$且$\boldsymbol{\beta}\cdot\boldsymbol{k}_i=0$时，$\mathrm{LAT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^n$；当$\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i=1$且存在$j_0\neq j(\boldsymbol{k}_i)$使得$\alpha_{j_0}\neq\beta_{j_0}$时，$\mathrm{LAT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}\pm W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')$；当$(\boldsymbol{\alpha},\boldsymbol{\beta})$为其他掩码对时，$\mathrm{LAT}_R[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}$。其中$\boldsymbol{\alpha}''$, $\boldsymbol{\beta}''$是$\boldsymbol{\alpha}$, $\boldsymbol{\beta}$去掉第$j(\boldsymbol{k}_i)$位比特之后得到的$n-1$维向量。

证明　由定义可得$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=\sum\limits_{\boldsymbol{x}\in F_2^n}(-1)^{\boldsymbol{\alpha}\cdot\boldsymbol{x}+\boldsymbol{\beta}R_{\boldsymbol{k}_i,\boldsymbol{w}_i}(\boldsymbol{x})}=\sum\limits_{\boldsymbol{x}\in F_2^n}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{x}+\boldsymbol{\beta}\cdot f_{b(i)}\left(\boldsymbol{w}_i+\Phi_{\boldsymbol{k}_i}(\boldsymbol{x})\right)\boldsymbol{k}_i}$。

令$\Phi_{\boldsymbol{k}_i}(\boldsymbol{x})=\boldsymbol{y}$，由$\Phi_{\boldsymbol{k}_i}$为线性函数且$\mathrm{Ker}\Phi_{\boldsymbol{k}_i}=\{\boldsymbol{0},\boldsymbol{k}_i\}$得$\Phi_{\boldsymbol{k}_i}(\boldsymbol{x}+\boldsymbol{k}_i)=\boldsymbol{y}$，故上式可化为

$$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=\left[1+(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{k}_i}\right]\cdot\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'+f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})\boldsymbol{\beta}\cdot\boldsymbol{k}_i},$$

其中$\boldsymbol{y}'$是$\boldsymbol{y}$的第$j(\boldsymbol{k}_i)$位注入比特0后而得的n维向量。

情形1，当$\boldsymbol{\alpha}=\boldsymbol{\beta}$时，$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2\sum\limits_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})\boldsymbol{\beta}\cdot\boldsymbol{k}_i}=\begin{cases}2^n,\boldsymbol{\beta}\cdot\boldsymbol{k}_i=0;\\0,\boldsymbol{\beta}\cdot\boldsymbol{k}_i=1\end{cases}$

情形2，当$\boldsymbol{\alpha}\neq\boldsymbol{\beta}$时，$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=\begin{cases}0,\boldsymbol{\alpha}\cdot\boldsymbol{k}_i\neq\boldsymbol{\beta}\cdot\boldsymbol{k}_i;\\2\sum\limits_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'+f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})\boldsymbol{\beta}\cdot\boldsymbol{k}_i},\\\quad\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i。\end{cases}$

(1) 当$\boldsymbol{\alpha}\neq\boldsymbol{\beta}$且$\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i=0$时，有

$$\begin{aligned}&2\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'+f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})\boldsymbol{\beta}\cdot\boldsymbol{k}_i}\\&=2\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'}\\&=2\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')\cdot\boldsymbol{y}}=0;\end{aligned}$$

(2) 当$\boldsymbol{\alpha}\neq\boldsymbol{\beta}$且$\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i=1$时，令$\boldsymbol{w}_i+\boldsymbol{y}=\boldsymbol{x}$可得

$$\begin{aligned}&2\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'+f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})\boldsymbol{\beta}\cdot\boldsymbol{k}_i}\\&=2\sum_{\boldsymbol{y}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{y}'+f_{b(i)}(\boldsymbol{w}_i+\boldsymbol{y})}\\&=2\sum_{\boldsymbol{x}\in F_2^{n-1}}(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\left(\boldsymbol{w}'_i+\boldsymbol{x}'\right)+f_{b(i)}(\boldsymbol{x})}\\&=2(-1)^{(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{w}'_i}\sum_{\boldsymbol{x}\in F_2^{n-1}}(-1)^{\left(\boldsymbol{\alpha}''+\boldsymbol{\beta}''\right)\cdot\boldsymbol{x}+f_{b(i)}(\boldsymbol{x})}\\&=\pm2W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')\,,\end{aligned}$$

其中$\boldsymbol{w}'_i$和$\boldsymbol{x}'$分别是是$\boldsymbol{w}_i$和$\boldsymbol{x}$的第$j(\boldsymbol{k}_i)$位注入比特0后而得的n维向量。

注意到当$\boldsymbol{\alpha}[1,2,\cdots,j(\boldsymbol{k}_i)-1,j(\boldsymbol{k}_i)+1,\cdots,n]=\boldsymbol{\beta}[1,2,\cdots,j(\boldsymbol{k}_i)-1,j(\boldsymbol{k}_i)+1,\cdots,n]$，且$\alpha_{j(\boldsymbol{k}_i)}\neq\beta_{j(\boldsymbol{k}_i)}$时有$\boldsymbol{\alpha}''+\boldsymbol{\beta}''=\boldsymbol{0}$，结合$f_{b(i)}$的平衡性可得$W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')=0$，故有：当$\boldsymbol{\alpha}=\boldsymbol{\beta}$且$\boldsymbol{\beta}\cdot\boldsymbol{k}_i=0$时，$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^n$；当$\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i=1$且存在$j_0\neq j(\boldsymbol{k}_i)$使得$\alpha_{j_0}\neq\beta_{j_0}$时，$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=\pm2W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')$；当$(\boldsymbol{\alpha},\boldsymbol{\beta})$为其他掩码对时，$W_{R_{\boldsymbol{k}_i,\boldsymbol{w}_i}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=0$。　证毕

文献[12]讨论的是BISON算法的线性密码分析，其轮函数的定义与式(4)、式(5)相同，非线性部件$f_{b(i)}$为$n-1$元布尔函数，其轮函数线性逼近表为：当$\boldsymbol{\alpha}=\boldsymbol{\beta}$且$\boldsymbol{\beta}\cdot\boldsymbol{k}_i=0$时，$\mathrm{LAT}_{\mathrm{BISON}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^n$；当$\boldsymbol{\alpha}\cdot\boldsymbol{k}_i=\boldsymbol{\beta}\cdot\boldsymbol{k}_i=1$时，$\mathrm{LAT}_{\mathrm{BISON}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}\pm2^{(n-1)/2}$；当$(\boldsymbol{\alpha},\boldsymbol{\beta})$为其他掩码对时，$\mathrm{LAT}_{\mathrm{BISON}}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}$。对比后，发现$f_{b(i)}$的平衡性对BISON-like算法的线性密码分析的结果有较显著的影响，当取$f_{b(i)}$为平衡函数时，轮函数的线性逼近表中将有更多的元素为2^{n-1}。

下面讨论r轮$(r\geq n)$线性特征的线性概率上界。

定理 3　设BISON-like算法的轮函数$R_{\boldsymbol{k}_i,\boldsymbol{w}_i}$如式(4)、式(5)所定义，$f_{b(i)}$为$n-1$元平衡布尔函数，$1\leq i\leq n$。$\boldsymbol{\theta}=(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1,\cdots,\boldsymbol{\theta}_r)$是$r$轮的非平凡线性特征，$r\geq n$，则$\mathrm{LP}(\theta)\leq2^{-(2n-2)}\max\limits_{1\leq i\leq r}\max\limits_{\boldsymbol{a}\in F_2^n,\boldsymbol{a}\neq0}{W_{f_{b(i)}}}^2(\boldsymbol{a})$。

证明　下面仅证$r=n$的情形，同理可证明$r>n$的情形。反证法，假设存在n轮的线性概率$\mathrm{LP}(\theta)=1$的非平凡的线性特征$\boldsymbol{\theta}=(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1,\cdots,\boldsymbol{\theta}_n)$，则由堆积引理可得$\mathrm{LP}(\theta_{i-1},\theta_i)=1$, $i=1,2,\cdots,n$，即$\left|\{\boldsymbol{x}\in F_2^n|\,\boldsymbol{\theta}_{i-1}\cdot\boldsymbol{x}+\boldsymbol{\theta}_i\cdot R_{\boldsymbol{k}_i,\boldsymbol{w}_i}(\boldsymbol{x})=0\}\right|/2^n=1$，$i=1,2,\cdots,n$，由定理2可知，该式成立当且仅当$\boldsymbol{\theta}_{i-1}=\boldsymbol{\theta}_i$且$\boldsymbol{\theta}_i\cdot\boldsymbol{k}_i=0$, $i=1,2,\cdots,n$，结合$\boldsymbol{k}_1,\boldsymbol{k}_2,\cdots,\boldsymbol{k}_n$线性独立得：$\boldsymbol{\theta}_i=\boldsymbol{0}$, $i=1,2,\cdots,n$。这与$\boldsymbol{\theta}$是非平凡线性特征相矛盾，故至少存在1个i^*, $1\leq i^*\leq n$，使得$\Pr[\boldsymbol{\theta}_{i^*-1}\cdot\boldsymbol{x}=\boldsymbol{\theta}_{i^*}\cdot R_{\boldsymbol{k}_{i^*},\boldsymbol{w}_{i^*}}(\boldsymbol{x})]=2^{-1}\pm2^{-n}$

$W_{f_{b(i^*)}}(\boldsymbol{\theta}''_{\boldsymbol{i^*-1}}+\boldsymbol{\theta}''_{\boldsymbol{i^*}})$或$2^{-1}$，其中$\boldsymbol{\theta}''_{\boldsymbol{i^*-1}}+\boldsymbol{\theta}''_{\boldsymbol{i^*}}\neq\boldsymbol{0}$。故 $\mathrm{LP}(\theta_{\boldsymbol{i^*-1}},\theta_{\boldsymbol{i^*}})=2^{-(2n-2)}{W_{f_{b(i^*)}}}^2(\theta''_{\boldsymbol{i^*-1}}+\theta''_{\boldsymbol{i^*}})$或0，从而

$$\mathrm{LP}(\boldsymbol{\theta})\le 2^{-(2n-2)}\max_{\boldsymbol{a}\in F_2^n,\boldsymbol{a}\neq\boldsymbol{0}}{W_{f_{b(i^*)}}}^2(\boldsymbol{a})\le 2^{-(2n-2)}\max_{1\le i\le n}\max_{\boldsymbol{a}\in F_2^n,\boldsymbol{a}\neq 0}{W_{f_{b(i)}}}^2(\boldsymbol{a})。$$

证毕

注2：BISON算法的$\mathrm{MELP}=2^{-(n-1)}$。

4 变体BISON算法

本节从一类绝对值指标小的平衡布尔函数中选取非线性度高、代数次数高的函数做式(4)中的非线性部件$f_{b(i)}$，线性部件$\Phi_{\boldsymbol{k_i}}$与式(5)相同，将由此而得的BISON-like算法称为变体BISON算法。

4.1 一类绝对值指标为8的平衡布尔函数

由引理1、引理2及定理1可知，轮函数中$f_{b(i)}$的绝对值指标越小， BISON-like算法抵御差分攻击的能力就越强，因此本文以拥有较小的绝对值指标的平衡布尔函数为切入点，从中寻找高非线性度、高代数次数的函数用做BISON-like算法中的$f_{b(i)}$。

众所周知，绝对值指标的下界为0，在全体布尔函数中，有且仅有Bent函数的绝对值指标为0，因此Bent函数拥有最佳的绝对值指标。当$n\ge 3$时，偶重量的布尔函数的绝对值指标是8的倍数，故3元及3元以上的平衡布尔函数的绝对值指标最小为8。文献[15]给出了如下一类绝对值指标为8的平衡布尔函数。

定理 4[15] 设$f(\boldsymbol{x})\in B_n$, $wt(f)=2^{n-1}$, $f(\boldsymbol{x})$在A上满足扩散准则，$A\subset F_2^n$, $|A|=t$。当$0\le t\le 7\times 2^{n-3}-1$且$t$为奇数时，$\sigma_f=2^{2n}+2^6(2^n-t-1)$当且仅当对任意的$\boldsymbol{s}\in F_2^n$有$\Delta_f(\boldsymbol{s})=2^n$，1次；$\Delta_f(\boldsymbol{s})=8$，$(7\times 2^{n-3}-t-1)/2$次；$\Delta_f(\boldsymbol{s})=-8$，$(9\times 2^{n-3}-t-1)/2$次；$\Delta_f(\boldsymbol{s})=0$，$t$次。

显然，定理4中的函数的绝对值指标为8，是具有最佳绝对值指标的平衡布尔函数。该类函数的平方和指标$\sigma_f=2^{2n}+2^6(2^n-t-1)$，由$v2^{n-3}-1$及式(2)可得，当$n$较大时，有

$$N_f\le 2^{n-1}-2^{n/2-1}\sqrt{1+2^{-(n-6)}-(t+1)/2^{2n-6}}\approx 2^{n-1}-2^{n/2-1}。$$

由此可见该类函数有可能具有极高的非线性度。文献[15]用计算机搜索找到了满足定理4条件的4元平衡函数，其中一些函数的代数次数可达到3，非线性度可达4.84(近似值)。且随着变元个数n的增大，满足定理4条件的n元平衡布尔函数的数目就会增多，因此本文能在该类函数中找到具有高非线性度、高代数次数的平衡布尔函数，用这样的函数做$f_{b(i)}$可使得相应的BISON-like算法具有较好的安全性能。本文将使用满足定理4条件的平衡布尔函数做$f_{b(i)}$而得的BISON-like算法称为变体BISON算法。

4.2 变体BISON算法的差分密码分析

设$f_{b(i)}$是满足定理4条件的$n-1$元平衡布尔函数，则$f_{b(i)}$的自相关值分别为2^{n-1}，8，-8，0，$\Delta_{f_{b(i)}}(\boldsymbol{s})=2^n$当且仅当$\boldsymbol{s}=\boldsymbol{0}$。根据引理1可求得变体BISON算法的轮函数的DDT：当$\boldsymbol{\beta}=\boldsymbol{\alpha}=\boldsymbol{0}$或$\boldsymbol{\beta}=\boldsymbol{\alpha}=\boldsymbol{k_i}$时，$\mathrm{DDT}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^n$；当$\boldsymbol{\beta}\in\{\boldsymbol{\alpha},\boldsymbol{\alpha}+\boldsymbol{k_i}\}$且$\boldsymbol{\alpha}\notin\{\boldsymbol{0},\boldsymbol{k_i}\}$时，$\mathrm{DDT}[\boldsymbol{\alpha},\boldsymbol{\beta}]=2^{n-1}$或$2^{n-1}\pm 8$；当$(\boldsymbol{\alpha},\boldsymbol{\beta})$为其他差分对时，$\mathrm{DDT}[\boldsymbol{\alpha},\boldsymbol{\beta}]=0$。

对于r轮($r\ge n$)的变体BISON算法，由引理2与定理1可得其最大期望差分概率$\mathrm{MEDP}_{\text{变体BISON}}=2^{-(n-1)}\left(1+2^{-(n-4)}\right)^{n-1}$。当$n\ge 8$时，有$\mathrm{MEDP}_{\mathrm{BISON}}<\mathrm{MEDP}_{\text{变体BISON}}<2\mathrm{MEDP}_{\mathrm{BISON}}$。依次取数据分组长度$n$为17, 33, 65及129，计算出了相应的$\mathrm{MEDP}_{\mathrm{BISON}}$与$\mathrm{MEDP}_{\text{变体BISON}}$，见表1。发现当$n\ge 17$时，$\mathrm{MEDP}_{\text{变体BISON}}\approx\mathrm{MEDP}_{\mathrm{BISON}}$；随着$n$的增大，$\mathrm{MEDP}_{\text{变体BISON}}$与理想值$(2^n-1)^{-1}$相当。

4.3 变体BISON算法的线性密码分析

结合定理2，由线性逼近表对BISON-like算法进行线性密码分析，发现$W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')$的绝对值越小，BISON-like算法抵御线性攻击的能力就越强。由式(3)可得，对于$\boldsymbol{a}\in F_2^{n-1}$有

$$\begin{aligned}{W_{f_{b(i)}}}^2(\boldsymbol{a})&=\sum\nolimits_{\boldsymbol{s}\in F_2^{n-1}}\Delta_{f_{b(i)}}(\boldsymbol{s})(-1)^{\boldsymbol{a}\cdot\boldsymbol{s}}\\&=2^{n-1}+8\sum\nolimits_{\Delta_{f_{b(i)}}(\boldsymbol{s})=8}(-1)^{\boldsymbol{a}\cdot\boldsymbol{s}}\\&\quad-8\sum\nolimits_{\Delta_{f_{b(i)}}(\boldsymbol{s})=-8}(-1)^{\boldsymbol{a}\cdot\boldsymbol{s}}\end{aligned}\tag{6}$$

由定理4可得${W_{f_{b(i)}}}^2(\boldsymbol{a})\le 2^{n-1}+2^{n+2}-8(t+1)$。显然$t$越大，${W_{f_{b(i)}}}^2(\boldsymbol{a})$越小。由定理4知$0\le t\le 7\times 2^{n-4}-1$，故可在定理4的函数类中选取对应$t$值为$7\times 2^{n-4}-1$的函数做$f_{b(i)}$，相应地

$${W_{f_{b(i)}}}^2(\boldsymbol{a})\le 2^n,\left|W_{f_{b(i)}}(\boldsymbol{a})\right|\le 2^{n/2}\tag{7}$$

表 1 $\mathrm{MEDP}_{\text{变体BISON}}$, $\mathrm{MEDP}_{\mathrm{BISON}}$与$\mathrm{MEDP}_{\text{理想值}}$的对比

n	17	33	65	129
$\mathrm{MEDP}_{\mathrm{BISON}}=2^{-(n-1)}$	$=2^{-16}$	$=2^{-32}$	$=2^{-64}$	$=2^{-128}$
$\mathrm{MEDP}_{\text{变体BISON}}=\left(1/2+2^{-(n-3)}\right)^{n-1}$	$\approx 2^{-15.9972}$	$\approx 2^{-32}$	$\approx 2^{-64}$	$\approx 2^{-128}$
$\mathrm{MEDP}_{\text{理想值}}=(2^n-1)^{-1}$	$\approx 2^{-17}$	$\approx 2^{-33}$	$\approx 2^{-65}$	$\approx 2^{-129}$

变体BISON算法的轮函数中的$f_{b(i)}$为平衡函数，故由定理2可求得$\mathrm{LAT}_{\text{变体BISON}}$，对比$\mathrm{LAT}_{\text{变体BISON}}$与$\mathrm{LAT}_{\text{BISON}}$，发现：

(1) $\mathrm{LAT}_{\text{变体BISON}}$有更多的元素为0；

(2) 当$\boldsymbol{\alpha}\cdot\boldsymbol{k_i}=\boldsymbol{\beta}\cdot\boldsymbol{k_i}=1$且存在$j_0\neq j\,(\boldsymbol{k_i})$,使得$\alpha_{j_0}\neq\beta_{j_0}$时，变体BISON算法对应位置的偏差$\varepsilon_{\text{变体BISON}}=\pm 2^{-n}W_{f_{b(i)}}(\boldsymbol{\alpha}''+\boldsymbol{\beta}'')$，故$|\varepsilon_{\text{变体BISON}}|\leq 2^{-n/2}$；BISON算法对应位置的偏差$\varepsilon_{\text{BISON}}=\pm 2^{-(n+1)/2}$, $|\varepsilon_{\text{BISON}}|=2^{-(n+1)/2}$。简而言之，在这些位置上$\max|\varepsilon_{\text{变体BISON}}|$至多为$\max|\varepsilon_{\text{BISON}}|$的2倍。

由定理3知，若$\boldsymbol{\theta}=(\boldsymbol{\theta_0},\boldsymbol{\theta_1},\cdots,\boldsymbol{\theta_r})$是BISON-like算法的$r$轮$(r\geq n)$非平凡线性特征，则有$\mathrm{LP}(\theta)\leq 2^{-(2n-2)}\max\limits_{1\leq i\leq r}\max\limits_{\boldsymbol{a}\in F_2^n,\boldsymbol{a}\neq 0}{W_{f_{b(i)}}}^2(\boldsymbol{a})$。由式(7)知，若在定理4的函数类中选取对应$t$值为$7\times 2^{n-4}-1$的函数做$f_{b(i)}$，则有$\max\limits_{\boldsymbol{a}\in F_2^n,\boldsymbol{a}\neq 0}{W_{f_{b(i)}}}^2(\boldsymbol{a})=2^n, 1\leq i\leq r$，从而可使得$\mathrm{LP}_{\text{变体BISON}}(\theta)\leq 2^{-(n-2)}$即$\mathrm{MELP}_{\text{变体BISON}}=2^{-(n-2)}$。由注2知$\mathrm{MELP}_{\text{变体BISON}}=2\mathrm{MELP}_{\text{BISON}}$。显然随着$n$的增大，$\mathrm{MELP}_{\text{变体BISON}}$越接近理想值0。

综合上所述，对比后发现：变体BISON算法的迭代轮数远低于BISON算法的迭代轮数；当n较大时，$\mathrm{MEDP}_{\text{变体BISON}}\approx\mathrm{MEDP}_{\text{BISON}}$; $\mathrm{MELP}_{\text{变体BISON}}=2\mathrm{MELP}_{\text{BISON}}$；在1轮之后，变体BISON算法的代数次数就有可能达到最大值$n-1$，而BISON算法则在$n-2$轮之后，其代数次数才有可能达到最大值$n-1$；变体BISON算法的非线性部件是平衡的，而BISON算法的非线性部件则不平衡。具体情况见表2，其中n是数据分组长度，n为奇数。

5　结束语

本文讨论了基于WSN结构的BISON-like算法的最大期望差分概率,并分析了该算法使用平衡函数作为核心部件时抵御线性密码分析的能力。由此，本文使用一类拥有低绝对值指标、高非线性度、高代数次数的函数直接作为BISON-like算法中的非线性部件，即给出了一种变体BISON算法。研究结果表明:变体BISON算法的迭代轮数远低于原有BISON算法的迭代轮数；特别是其密钥信息的异或操作由平衡函数来决定，从而新变体算法具有更好的算法局部平衡性。此外，本文对变体BISON算法还进行了差分密码分析与线性密码分析:发现当输入变元个数n较大时，变体BISON算法抵御差分攻击和线性攻击的能力与BISON算法的较接近，同时其差分界与线性界均接近理想值。

表 2　r轮$(r\geq n)$变体BISON算法与BISON算法综合安全性能对比

算 法	迭代轮数	MEDP	MELP	局部平衡性
BISON算法	$3n$	$2^{-(n-1)}$	$2^{-(n-1)}$	否
变体BISON算法	n	$2^{-(n-1)}\left(1+\frac{1}{2^{n-4}}\right)^n$	$2^{-(n-2)}$	是

参 考 文 献

[1] National Institute of Standards and Technology (NIST). FIPS PUB 197 Advanced encryption standard (AES)[S]. U.S. Department of Commerce, 2001.

[2] DAEMEN J and RIJMEN V. The wide trail design strategy[C]. The 8th IMA International Conference on Cryptography and Coding, Cirencester, UK, 2001: 222–238. doi: 10.1007/3-540-45325-3_20.

[3] DAEMEN J and RIJMEN V. The Design of Rijndael: AES-The Advanced Encryption Standard. Information Security and Cryptography[M]. Berlin Heidelberg: Springer, 2002: 35–79. doi: 10.1007/978-3-662-04722-4.

[4] EVEN S and MANSOUR Y. A construction of a cipher from a single pseudorandom permutation[J]. *Journal of Cryptology*, 1997, 10(3): 151–161. doi: 10.1007/s001459900025.

[5] CHEN Shan, LAMPE R, LEE J, *et al*. Minimizing the two-round EVEN-MANSOUR cipher[J]. *Journal of Cryptology*, 2018, 31(4): 1064–1119. doi: 10.1007/s00145-018-9295-y.

[6] CHEN Shan and STEINBERGER J. Tight security bounds for key-alternating ciphers[C]. The 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 2014: 327–350. doi: 10.1007/978-3-642-55220-5_19.

[7] GRASSI L, RECHBERGER C, and RØNJOM S. Subspace trail cryptanalysis and its applications to AES[J]. *IACR Transactions on Symmetric Cryptology*, 2016, 2016(2): 192–225. doi: 10.13154/tosc.v2016.i2.192-225.

[8] GRASSI L, RECHBERGER C, and RØNJOM S. A new structural-differential property of 5-Round AES[C]. The 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 2017: 289–317. doi: 10.1007/978-3-319-56614-6_10.

[9] TESSARO S. Optimally secure block ciphers from ideal primitives[C]. The 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 2015: 437–462. doi: 10.1007/978-3-662-48800-3_18.

[10] HOANG V T, MORRIS B, and ROGAWAY P. An enciphering scheme based on a card shuffle[C]. The 32nd Annual Cryptology Conference, Santa Barbara, US, 2012: 1–13. doi: 10.1007/978-3-642-32009-5_1.

[11] VAUDENAY S. The end of encryption based on card shuffling[EB/OL]. https://crypto.2012.rump.cr.yp.to/9f3046f7f835f99aabca5d4ad7946b2.pdf, 2012.

[12] CANTEAUT A, LALLEMAND V, LEANDER G, *et al*. BISON instantiating the Whitened Swap-Or-Not construction[C]. The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 2019: 585–616. doi: 10.1007/978-3-030-17659-4_20.

[13] CUSICK T W and STĂNICĂ P. Cryptographic Boolean Functions and Applications[M]. Amsterdam: Elsevier, 2009: 7–16.

[14] ZHANG Xianmo and ZHENG Yuliang. GAC — the Criterion for Global Avalanche Characteristics of Cryptographic Functions[M]. MAURER H, CALUDE C, and SALOMAA A. J.UCS the Journal of Universal Computer Science. Berlin, Heidelberg: Springer, 1996: 320–337. doi: 10.1007/978-3-642-80350-5_30.

[15] ZHOU Yu, ZHANG Weiguo, LI Juan, *et al*. The autocorrelation distribution of balanced Boolean function[J]. *Frontiers of Computer Science*, 2013, 7(2): 272–278. doi: 10.1007/s11704-013-2013-x.

[16] 李超, 孙兵, 李瑞林. 分组密码的攻击方法与实例分析[M]. 北京: 科学出版社, 2010: 64–116.
LI Chao, SUN Bing, and LI Ruilin. Attack Methods and Case Analysis of Block Cipher[M]. Beijing: Science Press, 2010: 64–116.

[17] KRANZ T, LEANDER G, and WIEMER F. Linear cryptanalysis: Key schedules and tweakable block ciphers[J]. *IACR Transactions on Symmetric Cryptology*, 2017(1): 474–505.

赵海霞：女，1981年生，博士生，研究方向为密码函数、分组密码分析.

韦永壮：男，1976年生，教授，博士生导师，研究方向为密码函数、分组密码分析.

刘争红：男，1979年生，高级实验师，硕士生导师，研究方向为通信信息安全.

责任编辑：阮 望