模 2^n 加法最佳线性逼近关系研究

薛 帅* 戚文峰
(郑州信息工程大学信息工程学院应用数学系 郑州 450002)

摘 要：该文研究了模 2^n 加法运算的最佳线性逼近问题。利用权位分量函数的线性逼近关系，该文首先给出了模 2^n 加法最佳线性逼近相关值的计算公式。其次通过递归构造得到了模 2^n 加法最佳线性逼近集的生成方法。该文的研究从理论上更清楚地刻画了二元模 2^n 加法最佳线性逼近的内在规律，有助于更好地利用该线性逼近关系实现对实际密码算法的有效分析。

关键词：密码学；相关值；最佳线性逼近；模 2^n 加法
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2012)09-2156-05
DOI: 10.3724/SP.J.1146.2012.00096

Research on the Best Linear Approximation of Addition Modulo 2^n

Xue Shuai Qi Wen-feng
(*Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou* 450002, *China*)

Abstract: In this paper, the best linear approximation of addition modulo 2^n is studied. Firstly, the formula for maximum correlations of addition modulo 2^n is proposed by using the linear approximation of the coordinate functions of addition modulo 2^n. Moreover, a method to construct the best linear approximation set of addition modulo 2^n is given in a recursive way. The paper characterizes the inner principle of best linear approximation of addition modulo 2^n theoretically, which will help to use the linear approximation relation to realize an effective analysis of cryptographic algorithms.

Key words: Cryptography; Correlation; Best linear approximation; Addition modulo 2^n

1 引言

线性分析是常用的重要密码分析方法之一，它的核心在于寻找目标函数输入输出间的线性逼近关系。当输入输出状态集较大时，直接遍历输入输出空间全体来寻找密码体制总体的最佳线性逼近往往是不实用的。常用的方法是先研究密码体制组件的最佳线性逼近，进而优化组合得到一条总体线性逼近路径。因此，研究密码体制中各种常用基本函数的最佳线性逼近显得至关重要。

模 2^n 加法运算是目前应用最为广泛的一类密码基本函数，从上世纪 90 年代起，各国密码学者开始研究整数模 2^n 加法的线性逼近问题。早期的研究更多关注模 2^n 加法运算整体与异或运算的线性逼近问题，Staffelbach 和 Meier 给出了初步的研究结果[1]，近来文献[2–4]作了进一步分析。随着研究的发展，人们发现在对状态变量为多比特整数的算法进行分析时，利用比特间的线性逼近关系可能会得到优势更明显的线性关系[5,6]。从 2003 年开始，Wallén 等人[7–9]对模 2^n 加法比特间任意组合的线性逼近问题进行了系统研究。文献[7,8]对两个整数模 2^n 加减法的进位函数进行了研究，给出了进位函数线性逼近相关值的计算方法，同时也得到了求取任意给定的相关值绝对值对应的全部线性逼近的算法。文献[9]给出了多个整数模 2^n 加法线性逼近时，计算任意指定线性逼近关系对应相关值的方法。

在实际分析过程时，为了寻找目标函数的最佳线性逼近，通常需要对全体线性逼近关系对应的相关值进行计算，并对比找出相关值最大的那些线性逼近。然而，当输入输出变量所含比特数 n 较大时，需要遍历的线性逼近关系集合太大，往往无法通过直接遍历全体线性逼近关系得到目标函数的最佳线性逼近。本文从二元模 2^n 加法运算的内在结构特点入手，对输出分量间按任意指定方式进行比特组合时线性逼近关系的最大相关值以及对应的线性关系进行了研究。

本文余下部分安排如下：第 2 节介绍文中需要的符号以及线性逼近的基本概念。第 3 节研究了二元模 2^n 加法单个分量的线性逼近关系，以及相邻分

2012-02-06 收到，2012-04-26 改回
国家自然科学基金(61070178)资助课题
*通信作者：薛帅 xue.shuai@163.com

量线性逼近时相关值的变化规律。第 4 节分析了多个分量按任意给定方式异或时的最大相关值，并给出了产生最大相关值对应所有线性逼近关系的方法。最后一节对全文进行了总结。

2　符号及基本概念

设 n 是正整数，对任意的整数 $x\in \boldsymbol{Z}_{2^n}$，它与 $\boldsymbol{F}_2^n$ 上向量 $(x_{n-1}, x_{n-2}, \cdots, x_0)$ 一一对应，其中 $x=2^{n-1}x_{n-1}+2^{n-2}x_{n-2}+\cdots+x_0$, $x_i\in\{0,1\}$称为 x 的第 i 权位比特。以下将二者不加区分。对任意两个整数 $x, y\in \boldsymbol{Z}_{2^n}$，定义 x 与 y 的内积为 $x\cdot y=x_{n-1}y_{n-1}\oplus\cdots\oplus x_0y_0$，定义 x 与 y 的对位乘法为 $xy=(x_{n-1}y_{n-1}, \cdots, x_0y_0)$。

设 m 是正整数，f 是 $\boldsymbol{Z}_{2^n}$ 到 $\boldsymbol{Z}_{2^n}$ 的函数。对任给的 $u\in \boldsymbol{Z}_{2^n}$, $v\in \boldsymbol{Z}_{2^n}$，由 u, v 决定的函数 f 的线性逼近关系形式如下：

$$u\cdot f(x)=v\cdot x \tag{1}$$

其中 u 称为输出线性掩码(linear masking)，v 称为输入线性掩码。线性逼近关系式(1)对 f 函数的逼近效果可以用相关值来衡量 $\mathrm{cor}_f(u,v)=2\cdot\Pr(u\cdot f(x)=v\cdot x)-1$，其中 x 是 $\boldsymbol{Z}_{2^n}$ 上服从均匀分布的随机变量。显然，$\mathrm{cor}_f(u,v)\in[-1,1]$，并且$|\mathrm{cor}_f(u, v)|$越大，式(1)的逼近效果越好。

本文主要考虑二元模 2^n 加法函数的线性逼近问题。以下均设 $f:\boldsymbol{Z}_{2^n}\times\boldsymbol{Z}_{2^n}\to\boldsymbol{Z}_{2^n}$ 是二元模 2^n 加法函数，$f(x,y)=x+y(\mathrm{mod}\ 2^n)=(f_{(n-1)}(x,y), f_{(n-2)}(x,y), \cdots, f_{(0)}(x,y))$，其中 $x=(x_{n-1}, x_{n-2},\cdots, x_0)$, $y=(y_{n-1}, y_{n-2},\cdots, y_0)\in\boldsymbol{Z}_{2^n}$, $f_{(i)}:\boldsymbol{Z}_{2^n}\times\boldsymbol{Z}_{2^n}\to\boldsymbol{Z}_{2^n}$ 是 f 的第 i 权位分量函数。

任给 $u,v,w\in\boldsymbol{Z}_{2^n}$，简记 $c(u;v,w)=\mathrm{cor}_f(u,(v,w))$, $c_{(i)}(v,w)=\mathrm{cor}_f(2^i;\ v,\ w)$。并记 $MC(u)=\max\limits_{v,w\in\boldsymbol{Z}_{2^n}}|c(u;v,w)|$为输入掩码为 u 时 f 的最大相关值，$LM(u)=\{(v,w):|c(u;\ v,\ w)|=MC(u), v,w\in\boldsymbol{Z}_{2^n}\}$为相应的最佳线性逼近集。

3　二元模 2^n 加法相邻分量函数的线性逼近关系

不妨记 $z=(z_{n-1}, z_{n-2},\cdots, z_0)=x+y(\mathrm{mod}\ 2^n)$，第 i 比特的进位为 σ_i, $0\le i\le n-1$, 并令 $\sigma_0=0$，则

$$z_i=x_i\oplus y_i\oplus\sigma_i,\ \ \sigma_{i+1}=x_iy_i\oplus x_i\sigma_i\oplus y_i\sigma_i \tag{2}$$

显然 z_i 和 σ_{i+1} 是只与 $x_0, x_1,\cdots, x_i, y_0, y_1,\cdots, y_i$ 有关的函数。因此，对任给的 $v,\ w\in\boldsymbol{Z}_{2^n}$，若 $v, w<2^i$ 或者 $v, w\ge 2^{i+1}$，则 $\Pr(z_i=v\cdot x\oplus v\cdot x)=1/2$，从而 $c_{(i)}(v,w)=0$。即若 $c_{(i)}(v,w)\ne 0$, 则 $2^i\le v, w<2^{i+1}$。更一般的，容易验证下面的结论成立。

引理 1　设 $u, v, w\in\boldsymbol{Z}_{2^n}$, $u\ne 0$, k 是使得 $u_k=1$ 成立的最大正整数，$0\le k\le n-1$。若 $c(u;\ v, w)\ne 0$，则 $2^k\le v, w<2^{k+1}$。

进而，可以证明相邻分量函数 $f_{(i)}$ 和 $f_{(i+1)}$ 的相关值满足下面的关系：

引理 2　对任意 $0\le i\le n-2$，有

$$c_{(i+1)}(2^{i+1}\oplus 2^i, 2^{i+1})=c_{(i+1)}(2^{i+1}, 2^{i+1}\oplus 2^i)=1/2 \tag{3}$$

$$c_{(i+1)}(2^{i+1}\oplus v', 2^{i+1}\oplus w')=(1/2)\,c_{(i)}(2^i\oplus v', 2^i\oplus w') \tag{4}$$

$$c_{(i+1)}(2^{i+1}\oplus 2^i\oplus v', 2^{i+1}\oplus 2^i\oplus w')=-(1/2)\,c_{(i)}(2^i\oplus v', 2^i\oplus w') \tag{5}$$

其中 $0\le v',\ w'<2^i$。而当 v, w 取其它值时，相关值 $c_{(i+1)}(v,\ w)$均为 0。

证明　由式(2)可知

$$\sigma_{i-1}=\begin{cases}0, & x_i=y_i=0\\ 1, & x_i=y_i=1\\ \sigma_i, & x_i\oplus y_i=1\end{cases} \tag{6}$$

若 $c_{(i+1)}(v,\ w)\ne 0$，则由引理 1 知，$2^{i+1}\le v, w<2^{i+2}$，故可设 $v=2^{i+1}\oplus v_i2^i\oplus v'$, $w=2^{i+1}\oplus w_i2^i\oplus w'$，其中 $v_i, w_i\in\{0, 1\}$, $0\le v',\ w'<2^i$。此时由定义知

$$\begin{aligned}c_{(i+1)}(v,\ w)&=2\cdot\Pr(z_{i+1}=x_{i+1}\oplus y_{i+1}\oplus v_ix_i\oplus w_iy_i\\&\quad\oplus v'\cdot x\oplus w'\cdot y)-1\\&=2\cdot\Pr(\sigma_{i-1}\oplus v_ix_i\oplus w_iy_i\oplus v'\cdot x\\&\quad\oplus w'\cdot y=0)-1\end{aligned}$$

利用式(6)，由全概率公式可以得到

$$\begin{aligned}&\Pr(\sigma_{i-1}\oplus v_ix_i\oplus w_iy_i\oplus v'\cdot x\oplus w'\cdot y=0)\\&=(1/4)(\Pr(v'\cdot x\oplus w'\cdot y=0)+\Pr(v'\cdot x\\&\quad\oplus w'\cdot y=v_i\oplus w_i\oplus 1)+\Pr(\sigma_i\oplus v'\cdot x\\&\quad\oplus w'\cdot y=v_i)+\Pr(\sigma_I\oplus v'\cdot x\oplus w'\cdot y=w_i)\end{aligned} \tag{7}$$

当 $v_i\oplus w_i=1$ 时，式(7)即为

$$\begin{aligned}&\Pr(\sigma_{i-1}\oplus v_ix_i\oplus w_iy_i\oplus v'\cdot x\oplus w'\cdot y=0)\\&=(1/2)\Pr(v'\cdot x\oplus w'\cdot y=0)+1/4\end{aligned} \tag{8}$$

由于

$$\Pr(v'\cdot x\oplus w'\cdot y=0)=\begin{cases}1, & v'=w'=0\\ 1/2, & \text{其它}\end{cases} \tag{9}$$

故当且仅当 $v'=w'=0$，即$(v,\ w)=(2^{i+1}\oplus 2^i, 2^{i+1})$或者$(2^{i+1}, 2^{i+1}\oplus 2^i)$时，相关值 $c_{(i+1)}(v,\ w)=1/2\ne 0$，从而式(3)成立。同理可证：当 $v_i=w_i=0$ 时，$c_{(i+1)}(v,\ w)=(1/2)\,c_{(i)}(2^i\oplus v', 2^i\oplus w')$，从而式(4)成立。当 $v_i=w_i=1$ 时，$c_{(i+1)}(v,\ w)=-(1/2)\,c_{(i)}(2^i\oplus v', 2^i\oplus w')$，从而式(5)成立。因此，引理 2 的结论成立。　　证毕

注 1　引理 2 刻画了模 2^n 加法相邻分量函数相关值的变化规律。由于 $\Pr(z_0=x_0\oplus y_0)=1$，即 $c_{(0)}(v,\ w)=1$，而对其它 $i\ge 1$, $|c_{(i)}(v,\ w)|<1$，故由引理 2 知，$|c_{(i)}(v,\ w)|$的最大值为 1/2，且仅当$(v,\ w)=(2^i\oplus 2^{i-1},\ 2^i)$或者$(2^i,\ 2^i\oplus 2^{i-1})$时 $c_{(i)}(v,w)$取到最大值，即有

$$MC(2^i)=\begin{cases}1, & i=0\\ 1/2, & 1\le i\le n-1\end{cases}$$

$$LM(2^i)=\begin{cases}\{(1,1)\}, & i=0\\ \{(2,2),(2,3),(3,2),(3,3)\}, & i=1\\ \{(2^i,2^i\oplus 2^{i-1}),(2^i\oplus 2^{i-1},2^i)\}, & 1\le i\le n-1\end{cases}$$

此外，当 $u=2^{i+1}\oplus 2^i(1\le i\le n-1)$时， 利用类似引理 2 的证明方法可以证明函数 $u\cdot f$的相关值 $c(2^{i+1}\oplus 2^i;\ v,\ w)$满足下面的关系。

引理 3 对任意的 $1\le i\le n-2$，有

$$\left.\begin{aligned}&c(2^{i+1}\oplus 2^i;2^{i+1}\oplus 2^i,2^{i+1}\oplus 2^i)=(1/2)\\ &c(2^{i+1}\oplus 2^i;2^{i+1},2^{i+1})=-(1/2)\\ &c(2^{i+1}\oplus 2^i;2^{i+1}\oplus 2^i\oplus v',2^{i+1}\oplus w')\\ &\quad=(1/2)c_{(i)}(2^i\oplus v',2^i\oplus w')\\ &c(2^{i+1}\oplus 2^i;2^{i+1}\oplus v',2^{i+1}\oplus 2^i\oplus w')\\ &\quad=(1/2)c_{(i)}(2^i\oplus v',2^i\oplus w')\end{aligned}\right\}\quad(10)$$

其中 $0\le v',\ w'<2^i$。而当 $v,\ w$ 取其它值时，相关值 $c(2^{i+1}\oplus 2^i;\ v,\ w)$均为 0。

注 2 由引理 3 知，$|c(2^{i+1}\oplus 2^i;\ v,\ w)|$的最大值为 1/2，且

$MC(2^{i+1}\oplus 2^i)=1/2$

$LM(2^{i+1}\oplus 2^i)=\{(2^{i+1}\oplus 2^i,2^{i+1}\oplus 2^i),\ (2^{i+1},\ 2^{i+1})\}$

4 二元模 2^n 加法函数的最佳线性逼近

任给整数 $u\in \boldsymbol{Z}_{2^n}$，本节考虑 $u\cdot f$ 的最佳线性逼近问题。对任意 $u,\ u'\in \boldsymbol{Z}_{2^n}$，简记

$$LM(u)\oplus LM(u')=\{(v\oplus v',\ w\oplus w'):(v,\ w)\in LM(u),\ (v',\ w')\in LM(u')\}$$

由于 $\Pr(f_{(0)}(x,\ y)=x_0\oplus y_0)=1$，故 $c(u;\ v,\ w)=c(u\oplus 1;\ v\oplus 1,\ w\oplus 1)$，从而当 $u_0=1$ 时，有

$$\left.\begin{aligned}&MC(u)=MC(u\oplus 1)\\ &LM(u)=\{(v\oplus 1,w\oplus 1):(v,w)\in LM(u\oplus 1)\}\\ &\quad=LM(1)\oplus LM(u\oplus 1)\end{aligned}\right\}\quad(11)$$

因此下面仅需计算当 u 为偶数时的最大相关值及其对应的线性关系。

引理 4[8] 设 $u\in \boldsymbol{Z}_{2^n}$，$u\notin\{0,1\}$，$k$ 是使得 $u_k=1$ 成立的最大正整数，$1\le k\le n-1$。则对任意的 $i\ge k$，有

$$c(u\oplus 2^{i-1};\ v,w)=\frac{1}{2}\begin{cases}c(u;u_i2^i\oplus v\bar{e}_i\oplus 2^{i+1},u_i2^i\oplus w\bar{e}_i\oplus 2^{i+1}), & v_i\ne w_i\\ (-1)^{u_i\oplus v_i}c(u\oplus 2^i;u_i2^i\oplus v\bar{e}_i\oplus 2^{i+1}\oplus 2^i, & \\ \quad u_i2^i\oplus w\bar{e}_i\oplus 2^{i+1}\oplus 2^i), & v_i=w_i\end{cases}$$

其中 $\bar{e}_i=(\underbrace{1,\cdots,1}_{n-1-i\text{项}},0,\underbrace{1,\cdots,1}_{i\text{项}})$。

引理 5 设 $u\in \boldsymbol{Z}_{2^n}$，$u\notin\{0,1\}$，$k$ 是使得 $u_k=1$ 成立的最大正整数，$1\le k\le n-1$。则对任意的 $i\ge k$，有

$$c(u\oplus 2^{i+1};\ 2^{i+1}\oplus 2^i\oplus a,\ 2^{i+1}\oplus b)=\frac{1}{2}c(u;a,b)\quad(12)$$

$$c(u\oplus 2^{i+1};\ 2^{i+1}\oplus a,2^{i+1}\oplus 2^i\oplus b=\frac{1}{2}c(u;a,b)\quad(13)$$

$$c(u\oplus 2^{i+1};2^{i+1}\oplus 2^i\oplus a',\ 2^{i+1}\oplus 2^i\oplus b')=\frac{1}{2}c(u\oplus 2^i;a',b')\quad(14)$$

$$c(u\oplus 2^{i+1};\ 2^{i+1}\oplus a',2^{i+1}\oplus b')=-\frac{1}{2}c(u\oplus 2^i;a',b')\quad(15)$$

其中 $a,b,a',b'\in \boldsymbol{Z}_{2^n}$ 并且使得 $c(u;a,b)\ne 0$，$c(u\oplus 2^i;a',b')\ne 0$。在其它情况下 $c(u\oplus 2^{i+1};v,w)$均为 0。

证明 由引理 1 知，若 $c(u\oplus 2^{i+1};v,w)\ne 0$，则 $2^{i+1}\le v,w<2^{i+2}$，不妨设 $v=2^{i+1}\oplus v_i2^i\oplus v'$，$w=2^{i+1}\oplus w_i2^i\oplus w'$，其中 $v_i,w_i\in\{0,1\}$，$0\le v',\ w'<2^i$。下面分 $i=k$ 和 $i>k$ 两种情况讨论。

(1)当 $i=k$ 时，$u_i=u_k=1$。 若 $v_i=w_i$，则由引理 4 知

$$c(u\oplus 2^{i-1};\ v,w=(1/2)(-1)^{1\oplus v_i}c(u\oplus 2^i;\ v\bar{e}_i\oplus 2^{i+1},\ w\bar{e}_i\oplus 2^{i+1})$$

由于 $v\bar{e}_i=v\oplus v_i2^i$，$w\bar{e}_i=w\oplus w_i2^i$，故有

$$c(u\oplus 2^{i-1};\ v,w)=\begin{cases}\frac{1}{2}c(u\oplus 2^i;\ v\oplus 2^{i+1}\oplus 2^i,w\oplus 2^{i+1}\oplus 2^i), & v_i=w_i=1\\ -\frac{1}{2}c(u\oplus 2^i;\ v\oplus 2^{i+1},w\oplus 2^{i+1}), & v_i=w_i=0\end{cases}\quad(16)$$

注意到当 $v_i=w_i=1$ 时，$v=2^{i+1}\oplus 2^i\oplus v'$，$w=2^{i+1}\oplus 2^i\oplus w'$，而当 $v_i=w_i=0$ 时，$v=2^{i+1}\oplus v'$，$w=2^{i+1}\oplus w'$，故

$$c(u\oplus 2^{i+1};2^{i+1}\oplus 2^i\oplus v',2^{i+1}\oplus 2^i\oplus w')=(1/2)c(u\oplus 2^i;\ v',\ w')\quad(17)$$

$$c(u\oplus 2^{i+1};2^{i+1}\oplus v',2^{i+1}\oplus w')=-(1/2)c(u\oplus 2^i;v',w')\quad(18)$$

令 $a'=v'$，$b'=w'$，可知式(14)，式(15)在此情况下成立。

若 $v_i\ne w_i$时，同理可证式(12)，式(13)成立。

(2)当 $i>k$ 时，$u_i=0$。 若 $v_i=w_i$，则由引理 4 知

$$
\begin{aligned}
&c(u\oplus 2^{i-1};\ v,w)\\
&\quad=(1/2)(-1)^{v_i}c(u\oplus 2^i;\ v\overline{e}_i\oplus 2^{i+1}\oplus 2^i,\\
&\qquad w\overline{e}_i\oplus 2^{i+1}\oplus 2^i)\\
&\quad=\begin{cases}-(1/2)c(u\oplus 2^i;\ v\oplus 2^{i+1},w\oplus 2^{i+1}),\\ \qquad v_i=w_i=1\\ (1/2)c(u\oplus 2^i;\ v\oplus 2^{i+1}\oplus 2^i,w\oplus 2^{i+1}\oplus 2^i),\\ \qquad v_i=w_i=0\end{cases}
\end{aligned}\tag{19}
$$

注意到当 $v_i=w_i=1$ 时，$v=2^{i+1}\oplus 2^i\oplus v'$, $w=2^{i+1}\oplus 2^i\oplus w'$，而当 $v_i=w_i=0$ 时，$v=2^{i+1}\oplus v'$,$w=2^{i+1}\oplus w'$，故式(19)即为

$$
\left.\begin{aligned}
&c(u\oplus 2^{i+1};2^{i+1}\oplus 2^i\oplus v',2^{i+1}\oplus 2^i\oplus w')\\
&\quad=-\frac{1}{2}c(u\oplus 2^i;v'\oplus 2^i,w'\oplus 2^i)\\
&c(u\oplus 2^{i+1};2^{i+1}\oplus v',2^{i+1}\oplus w')\\
&\quad=\frac{1}{2}c(u\oplus 2^i;v'\oplus 2^i,w'\oplus 2^i)
\end{aligned}\right\}\tag{20}
$$

令 $a'=v'\oplus 2^i$, $b'=w'\oplus 2^i$ 可知式(14)，式(15)在此情况下成立。

若 $v_i\neq w_i$，同理可证式(12)，式(13)成立。

证毕

引理 5 给出了 $c(u\oplus 2^{i+1};\ v,\ w)$所有可能的非零相关值的产生方式。由引理 5 知当 $i\geq k$时，$c(u\oplus 2^{i+1};\ v,\ w)$取最大值当且仅当 $c(u;a,b)$或者 $c(u\oplus 2^i;\ a',b')$取最大值，并且 $MC(u\oplus 2^{i+1})=(1/2)\cdot\max(MC(u),MC(u\oplus 2^i))$。注意到 $LM(2^{i+1})=\{(2^{i+1}\oplus 2^i,\ 2^{i+1}),(2^{i+1},\ 2^{i+1}\oplus 2^i)\}$,$LM(2^{i+1}\oplus 2^i)=\{(2^{i+1}\oplus 2^i,2^{i+1}\oplus 2^i),(2^{i+1},\ 2^{i+1})\}$，故下面的结论成立。

定理 1　设 $u\in \boldsymbol{Z}_{2^n}$, $u\notin\{0,1\}$, k 是使得 $u_k=1$ 成立的最大正整数，$1\leq k\leq n-1$。则对任意的 $i\geq k$，有

$$
MC(u\oplus 2^{i+1})=(1/2)\max(MC(u),MC(u\oplus 2^i))\tag{21}
$$

并且

$$
\begin{aligned}
&LM(u\oplus 2^{i+1})\\
&\quad=\begin{cases}LM(u)\oplus LM(2^{i+1}),\\ \qquad MC(u)>MC(u\oplus 2^i)\\ \{LM(u)\oplus LM(2^{i+1})\}\cup\{LM(2^{i+1}\oplus 2^i)\\ \quad\oplus LM(u\oplus 2^i)\},\quad MC(u)=MC(u\oplus 2^i)\\ LM(2^{i+1}\oplus 2^i)\oplus LM(u\oplus 2^i),\\ \qquad 其它\end{cases}
\end{aligned}\tag{22}
$$

当 $u=2^{i+j-1}\oplus 2^{i+j-2}\oplus\cdots\oplus 2^i$时，利用数学归纳法与定理 1 可以证明下面的结论成立。

定理 2　设 $u\in \boldsymbol{Z}_{2^n}$，若 $u=2^{i+j-1}\oplus 2^{i+j-2}\oplus\cdots\oplus 2^i$, $i\geq 1$, $j\geq 1$，则

$$
MC(u)=2^{-\lfloor j/2\rfloor}\tag{23}
$$

$$
LM(u)=\begin{cases}\oplus_{l=0}^{j/2-1}LM(2^{2l+i+1}\oplus 2^{2l+i}),\\ \qquad j是偶数\\ \cup_{l=0}^{(j-1)/2}\{LM(2^{i+j-1}\oplus 2^{i+j-2})\oplus\cdots\oplus\\ LM(2^{i+2l+2}\oplus 2^{i+2l+1})\oplus LM(2^{i+2l})\\ \quad\oplus LM(2^{i+2l-1}\oplus 2^{i+2l-2})\oplus\cdots\\ \quad\oplus LM(2^{i+1}\oplus 2^i)\},\ j是奇数\end{cases}\tag{24}
$$

由定理 1 和定理 2 还可以得到：

推论 1　设 $u\in \boldsymbol{Z}_{2^n}$，若 $u=2^k\oplus 2^{k-1}\oplus\cdots\oplus 2^i$, $1\leq i\leq k\leq n-1$，则对任意正整数 $l\geq 2$，都有 $MC(u\oplus 2^{k+l})=(1/2)MC(u)$。

类似于定理 2 的证明，由定理 1 和推论 1 知，若 $u=2^k\oplus 2^{k-1}\oplus\cdots\oplus 2^i$,$u'=2^{k+l+t-1}\oplus 2^{k+l+t-2}\oplus\cdots\oplus 2^{k+l}$, $l\geq 2$, $t\geq 1$，则

$$
MC(u\oplus u')=2^{-\lfloor (k-i+1)/2\rfloor}\cdot 2^{-\lfloor t/2\rfloor}\tag{25}
$$

更一般的，可以得到定理 3。

定理 3　设 $u\in \boldsymbol{Z}_{2^n}$, $u\notin\{0,1\}$，若在$(u_1,u_2,\cdots,u_{n-1})$中恰有 s 个$(0,1,\cdots,1,0)$串(也称为 1 游程)，并且每段中 1 的个数分别为 d_i, $1\leq i\leq s$，则

$$
MC(u)=2^{-\sum_{i=1}^{s}\lfloor\frac{d_i}{2}\rfloor}\tag{26}
$$

由定理 1，定理 2 和推论 1，还可以给出 $u\cdot f$ 对应的最佳线性逼近关系定理 4。

定理 4　设 $u\in \boldsymbol{Z}_{2^n}$, $u\notin\{0,1\}$，若在$(u_1,u_2,\cdots,u_{n-1})$中最后 1 个 1 游程起点为 t_1，长度为 d_1。则对任意整数 $u'=2^{t_2+d_2-1}\oplus 2^{t_2+d_2-2}\oplus\cdots\oplus 2^{t_2}$, $t_2>t_1+d_1, d_2\geq 1$，有

$$
LM(u'\oplus u)\begin{cases}(LM(u')\oplus LM(u))\cup S(u',u),\\ \qquad t_2=t_1+d_1+1且d_1,d_2是奇数\\ LM(u')\oplus LM(u),\\ \qquad 其它\end{cases}\tag{27}
$$

其中

$$
\begin{aligned}
S(u',u)=&LM(u'\oplus 2^{t_2})\oplus LM(2^{t_2}\oplus 2^{t_1+d_1})\\
&\oplus LM(2^{t_1+d_1}\oplus 2^{t_1+d_1-1})\oplus LM(2^{t_1+d_1-1}\oplus u)。
\end{aligned}
$$

对任给的 $u\in \boldsymbol{Z}_{2^n}$，由定理 2 与定理 4 可以递归给出完整的最佳线性逼近关系集合，可以用下面方法来生成 $LM(u)$。

(1)统计$(u_1,u_2,\cdots,u_{n-1})$中 1 游程的个数 s，并计算各游程对应整数 $u^{(i)}$, $1\leq i\leq s$, 由定理 2 计算出 $LM(u^{(i)})$, $1\leq i\leq s$。

(2)令 $T_0(u)=\varnothing, T_1(u)=LM(u^{(1)})$。对 $1\leq i\leq s-1$，按下面的方式递归计算 $T_{i+1}(u)$：

若 $u^{(i)}$, $u^{(i+1)}$对应的 1 游程长度为奇数且间隔为 1，令

$T_{i+1}(u)=(T_i(u)\oplus LM(u^{(i+1)}))\cup(T_{i-1}(u)\oplus S(u^{(i)},u^{(i+1)}))$

否则令

$$T_{i+1}(u)=(T_i(u)\oplus LM(u^{(i+1)}))$$

由定理 4 知 $LM(u\oplus u_0)=T_s(u)$，因此

$$LM(u)=\begin{cases}T_s(u), & u_0=0\\ T_s(u)\oplus\{(1,1)\}, & \text{其它}\end{cases} \tag{28}$$

由定理 2，定理 3 和定理 4 可知，随着 u 重量的增加，$MC(u)$会逐渐减小，而$|LM(u)|$会逐渐增大。表 1 给出了几例不同重量 u 的最大相关值与最佳线性逼近关系集合。

表 1 不同 $u\cdot f$的最大相关值与最佳线性逼近关系集合

u	$MC(u)$	$LM(u)$	$\lvert LM(u)\rvert$
2^{16}	2^{-1}	$(2^{16}\oplus 2^{15}, 2^{16})$, $(2^{16}, 2^{16}\oplus 2^{15})$	2
$2^{16}\oplus 1$	2^{-1}	$(2^{16}\oplus 2^{15}\oplus 1, 2^{16}\oplus 1)$, $(2^{16}\oplus 1, 2^{16}\oplus 2^{15}\oplus 1)$	2
$2^{16}\oplus 2^{15}$	2^{-1}	$(2^{16}\oplus 2^{15}, 2^{16}\oplus 2^{15})$, $(2^{16}, 2^{16})$	2
$2^{16}\oplus 2^{12}$	2^{-2}	$(2^{16}\oplus 2^{15}\oplus 2^{12}\oplus 2^{11}, 2^{16}\oplus 2^{12})$, $(2^{16}\oplus 2^{12}, 2^{16}\oplus 2^{15}\oplus 2^{12}\oplus 2^{11})$, $(2^{16}\oplus 2^{15}\oplus 2^{12}, 2^{16}\oplus 2^{12}\oplus 2^{11})$, $(2^{16}\oplus 2^{12}\oplus 2^{11}, 2^{16}\oplus 2^{15}\oplus 2^{12})$	4
$2^{16}\oplus 2^{14}$	2^{-2}	$(2^{16}\oplus 2^{15}\oplus 2^{14}\oplus 2^{13}, 2^{16}\oplus 2^{14})$, $(2^{16}\oplus 2^{14}, 2^{16}\oplus 2^{15}\oplus 2^{14}\oplus 2^{13})$, $(2^{16}\oplus 2^{15}\oplus 2^{14}, 2^{16}\oplus 2^{14}\oplus 2^{13})$, $(2^{16}\oplus 2^{14}\oplus 2^{13}, 2^{16}\oplus 2^{15}\oplus 2^{14})$, $(2^{16}\oplus 2^{14}, 2^{16}\oplus 2^{14})$, $(2^{16}\oplus 2^{15}, 2^{16}\oplus 2^{15})$, $(2^{16}, 2^{16})$, $(2^{16}\oplus 2^{15}\oplus 2^{14}, 2^{16}\oplus 2^{15}\oplus 2^{14})$	8

5 结束语

本文研究了二元模 2^n 加法运算的线性逼近关系， 通过分析二元模 2^n 加法运算的内在结构，首先给出了单个输出分量的线性逼近关系，接着分析了输出分量间按任意指定方式进行比特组合时线性逼近关系的最大相关值，并给出了相应的最佳线性逼近集的构造方法。目前大多数有关模 2^n 加法最佳线性逼近关系主要依靠搜索获得，本文的研究从理论上更清楚地刻画了二元模 2^n 加法最佳线性逼近集合的内在规律，有助于更好地利用该线性逼近关系实现对实际密码算法的有效分析。

参 考 文 献

[1] Staffelbach O and Meier W. Cryptographic significance of the carry for ciphers based on integer addition[C]. Crypto 1990, Santa Barbara, CA, USA, 1990, LNCS 537: 601–614.

[2] Sarkar P. On approximating addition by exclusive OR [OL]. http://eprint.iacr.org/2009/047.pdf. 2009.

[3] Alquié D. Approximating addition by XOR: how to go all the way[OL]. http://eprint.iacr.org/2010/072.pdf. 2010.

[4] Zhou C, Feng X, and Wu C. Linear approximations of addition modulo 2^n–1[C]. Fast Software Encryption 2011, Lyngby, Denmark, 2011, LNCS 6733: 359–377.

[5] Ekdahl P and Johansson T. Distinguishing attacks on SOBER-t16 and t32[C]. Fast Software Encryption 2002, Leuven, Belgium, 2002, LNCS 2365: 210–224.

[6] Coppersmith D, Halevi S, and Jutla C. Cryptanalysis of stream ciphers with linear masking[C]. Crypto 2002, Santa Barbara, CA, USA, 2002, LNCS 2442: 515–532.

[7] Wallén J. Linear approximations of addition modulo 2^n[C]. Fast Software Encryption 2003, LUND, Sweden, 2003, LNCS 2887: 261–273.

[8] Wallén J. On the differential and linear properties of addition[R]. Research Report A84, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, 2003.

[9] Nyberg K and Wallén J. Improved linear distinguishers for SNOW 2.0[C]. Fast Software Encryption 2006, Graz, Austria, 2006, LNCS 4047: 144–162.

薛 帅： 男，1982 年生，博士生，研究方向为密码学.

戚文峰： 男，1963 年生，教授，博士生导师，研究方向为有限域、密码学.