第20卷 第3期
2003年08月

工 程 数 学 学 报
JOURNAL OF ENGINEERING MATHEMATICS

Vol. 20 No. 3
Aug. 2003

文章编号：1005-3085(2003)03-0063-07

带多比特记忆组合生成器的“广义能量守恒猜想”及部分证明*

张卫明， 李世取
（郑州信息工程大学应用数学系，郑州 450002）

摘 要：对带多比特记忆的组合生成器提出了“广义能量守恒猜想”，即 j 时刻的输出与 j 时刻以前的输入的所有线性函数的相关系数平方和收敛于1（当 $j \to \infty$），并给出了部分证明。

关键词：带记忆组合生成器；能量守恒定理；相关性；相关免疫
分类号：AMS(2000) 62M02；62M05 中图分类号：O211.62 文献标识码：A

1 引 言

流密码系统使用的一类重要的密钥流生成器是由一组线性移位寄存器（LFSR）和一个无记忆非线性组合函数组成。这种系统中，输出序列总与一条或一组不同的LFSRs序列存在相关性，因此会受到分别征服攻击[1,2]。要抵抗“分别征服攻击”，就要求非线性组合函数有高的相关免疫阶数[1]。而为抵抗基于B-M算法的攻击，还要求非线性组合函数有高的非线性次数。但是非线性组合函数的非线性次数和相关免疫阶数之间存在制约关系。为克服这种制约关系，Rueppel在[3,4]中提出了带记忆的非线性组合生成器，而且证明了只需带1比特记忆就可同时获得最高相关免疫阶数和最高非线性次数。

无记忆组合生成器有著名的“能量守恒定理”，即输出与输入的所有线性函数的相关系数平方和等于1[5]。此结果已成为无记忆组合生成器相关性分析的理论基础。Meier证明了带1比特记忆的组合生成器有相应的结果：j 时刻的输出与 j 时刻以前的输入的所有线性函数的相关系数平方和极限小于等于1（$j \to \infty$），且除特殊情况外其极限为1[6]。本文称之为“带1比特记忆组合生成器的广义能量守恒定理”，此结果在带1比特记忆组合生成器的分析和设计中有多方面的应用。

但对于带多比特记忆的组合生成器考虑类似问题变得非常复杂，本文提出猜想：对于带多比特记忆组合生成器“广义能量守恒定理”仍然成立。证明此猜想并找出使极限小于1甚至等于0的条件对于带多比特记忆组合生成器的分析和设计都是非常有意义的，本文给

* 收稿日期：2001-08-02。 作者简介：张卫明（1976年11月生），男，硕士，研究方向：概率统计在密码学中的应用。

出了部分证明。

2 带多比特记忆组合生成器的概率模型

具有 r 比特记忆和 n 个输入的非线性组合生成器定义为：

$$y^{(j)} = V(x^{(j)}, y^{(j-1)}), j \geq 1$$
$$z_j = f(x^{(j)}, y^{(j-1)}), j \geq 1$$

其中，V: $GF^n(2)\times GF^r(2)\to GF^r(2)$ 为状态向量函数，f: $GF^n(2)\times GF^r(2)\to GF(2)$ 为输出函数。

$y^{(j)} = (y_{1j}, y_{2j}, \cdots, y_{rj})$ 是时刻 j 的状态向量，$y^{(0)}$ 为初始状态，$x^{(j)} = (x_{1j}, x_{2j}, \cdots, x_{nj})$ 为时刻 j 的输入向量。

设 $f(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+r})$ 是平衡的 $n+r$ 元布尔函数，而

$$V(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+r})$$
$$= (g_1(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+r}), \cdots, g_r(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+r}))$$

是平衡的 $n+r$ 元 r 维布尔向量函数。又设

$$X^{(1)} = (X_{11}, X_{21}, \cdots, X_{n1}), X^{(2)} = (X_{12}, X_{22}, \cdots, X_{n2}), \cdots, X^{(m)} = (X_{1m}, X_{2m}, \cdots, X_{nm}), \cdots$$

是定义在同一概率空间上的相互独立的 n 维布尔随机向量序列，且对任一 $k \geq 1$，$(X_{1k}, X_{2k}, \cdots, X_{nk})$ 中的 $X_{1k}, X_{2k}, \cdots, X_{nk}$ 是相互独立且都具有均匀分布的布尔随机变量；

还设 $Y_{10}, \cdots, Y_{r0}$ 是定义在同一概率空间上的相互独立、都具有均匀分布的布尔随机变量，且 $Y^{(0)} = (Y_{10}, \cdots, Y_{r0}), X^{(1)}, X^{(2)}, \cdots, X^{(m)}, \cdots$ 也是相互独立的。

最后记

$$Y^{(j)} = (g_1(X^{(j)}, Y^{(j-1)}, \cdots, g_r(X^{(j)}, Y^{(j-1)}))$$
$$Z_j = f(X^{(j)}, Y^{(j-1)}), \quad j = 1, 2, \cdots$$

由 $Y^{(0)}$ 和 $X^{(1)}$ 相互独立且分布都是均匀的以及 $V(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+r})$ 的平衡性可递归得到对每个 $j \geq 1$，$Y^{(j)}$ 都与 $Y^{(0)}$ 一样，是分量之间相互独立且每个分量都具有均匀分布的 r 维布尔随机向量；同理可知对每个 $j \geq 1$ Z_j 都是具有均匀分布的布尔随机变量。本文要讨论的是 Z_j 和 $(X^{(1)}, X^{(2)}, \cdots, X^{(j)})$ 的整体相关性的极限性质。

3 记号和引理

本文用大写表示布尔随机变量，小写表示其取值或一般的布尔变量，它们之间的运算都是 $GF(2)$ 上的加法或乘法运算。为了简便，以带 2 比特记忆组合生成器为例来进行讨论。带 2 比特记忆组合生成器定义为：

$$y_j = V(g_1(x^{(j)}, y^{(j-1)}), g_2(x^{(j)}, y^{(j-1)})), j \geq 1$$
$$z_j = f(x^{(j)}, y^{(j-1)}), j \geq 1$$

定义复合函数

$$G_1^1(x^{(1)}, y^{(0)}) = g_1(x^{(1)}, y^{(0)})$$
$$G_1^2(x^{(2)}, x^{(1)}, y^{(0)}) = g_1(x^{(2)}, g_1(x^{(1)}, y^{(0)}), g_2(x^{(1)}, y^{(0)})) \cdots$$

一般的，可定义

$$G_1^j(x^{(j)}, x^{(j-1)}, \cdots, x^{(1)}, y^{(0)}), \quad j \geq 1$$

类似的定义

$$G_2^1(x^{(1)}, y^{(0)}) = g_2(x^{(1)}, y^{(0)})$$
$$G_2^2(x^{(2)}, x^{(1)}, y^{(0)}) = g_2(x^{(2)}, g_1(x^{(1)}, y^{(0)}), g_2(x^{(1)}, y^{(0)})), \cdots$$
$$G_2^j(x^{(j)}, x^{(j-1)}, \cdots, x^{(1)}, y^{(0)}), \quad j \geq 1$$

和

$$F^1(x^{(1)}, y^{(0)}) = f(x^{(1)}, y^{(0)})$$
$$F^2(x^{(2)}, x^{(1)}, y^{(0)}) = f(x^{(2)}, g_1(x^{(1)}, y^{(0)}), g_2(x^{(1)}, y^{(0)})), \cdots$$
$$F^j(x^{(j)}, x^{(j-1)}, \cdots, x^{(1)}, y^{(0)}), \quad j \geq 1$$

实际上 $y_{1j} = G_1^j$, $y_{2j} = G_2^j$, $z_j = F^j$, 这里 G_1^j, G_2^j, F^j 都是 $nj+2$ 元布尔函数。

定义 1　设 $X = (X_1, X_2, \cdots, X_n)$ 是布尔随机向量, 其中 $X_1, X_2, \cdots, X_n$ 独立均匀分布, $h_1(x_1, x_2, \cdots, x_n)$ 和 $h_2(x_1, x_2, \cdots, x_n)$ 是 n 元布尔函数, 则 h_1 和 h_2 的相关系数定义为

$$c(h_1, h_2) = 2P\{h_1(X_1, X_2, \cdots, X_n) = h_2(X_1, X_2, \cdots, X_n)\} - 1$$

若 $h_2 = \omega \cdot X$, $\omega \in GF^n(2)$, 则利用 Walsh 谱有: $c(h_1, h_2) = S_{(h_1)}(\omega)$

由循环谱的性质和布尔随机变量联合分布的分解式[7] 可得下面两个引理, 它们可看文献[8] 中的引理的推论:

引理 1　任给 $w_1, w_2, \cdots, w_j \in GF^n(2)$, $w_1 \neq 0$, Z_j 与 $w_j \cdot X^{(j)} + \cdots + w_1 \cdot X^{(1)}$ 的相关系数

$$C(Z_j, w_j \cdot X^{(j)} + \cdots + w_j \cdot X^{(1)})$$
$$= S_{(f)}(w_j, 1, 0)S_{(G_1^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0) + S_{(f)}(w_j, 0, 1)S_{(G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$+ S_{(f)}(w_j, 1, 1)S_{(G_1^{j-1}+G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$

引理 2　对任给的 $w_1, w_2, \cdots, w_j \in GF^n(2)$, $w_1 \neq 0$,

$$S_{(G_1^j)}(w_j, w_{j-1}, \cdots, w_1, 0, 0)$$
$$= S_{(g_1)}(w_j, 1, 0)S_{(G_1^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0) + S_{(g_1)}(w_j, 0, 1)S_{(G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$+ S_{(g_1)}(w_j, 1, 1)S_{(G_1^{j-1}+G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$S_{(G_2^j)}(w_j, w_{j-1}, \cdots, w_1, 0, 0)$$
$$= S_{(g_2)}(w_j, 1, 0)S_{(G_1^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0) + S_{(g_2)}(w_j, 0, 1)S_{(G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$+ S_{(g_2)}(w_j, 1, 1)S_{(G_1^{j-1}+G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$S_{(G_1^j+G_2^j)}(w_j, w_{j-1}, \cdots, w_1, 0, 0)$$
$$= S_{(g_1+g_2)}(w_j, 1, 0)S_{(G_1^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0) + S_{(g_1+g_2)}(w_j, 0, 1)S_{(G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$
$$+ S_{(g_1+g_2)}(w_j, 1, 1)S_{(G_1^{j-1}+G_2^{j-1})}(w_{j-1}, \cdots, w_1, 0, 0)$$

为考察输出与输入的的相关系数平方和, 引入如下记号

$$a_0 = \sum_{w \in GF^n(2)} S^2_{(g_1)}(w, 0, 0), \quad a_1 = \sum_{w \in GF^n(2)} S^2_{(g_1)}(w, 1, 0)$$
$$a_2 = \sum_{w \in GF^n(2)} S^2_{(g_1)}(w, 0, 1), \quad a_3 = \sum_{w \in GF^n(2)} S^2_{(g_1)}(w, 1, 1)$$
$$b_0 = \sum_{w \in GF^n(2)} S^2_{(g_2)}(w, 0, 0), \quad b_1 = \sum_{w \in GF^n(2)} S^2_{(g_2)}(w, 1, 0)$$

$$b_2=\sum_{w\in GF^n(2)}S^2_{(g_1)}(w,0,1),\quad b_3=\sum_{w\in GF^n(2)}S^2_{(g_2)}(w,1,1)$$

$$c_0=\sum_{w\in GF^n(2)}S^2_{(g_1+g_2)}(w,0,0),\quad c_1=\sum_{w\in GF^n(2)}S^2_{(g_1+g_2)}(w,1,0)$$

$$c_2=\sum_{w\in GF^n(2)}S^2_{(g_1+g_2)}(w,0,1),\quad c_3=\sum_{w\in GF^n(2)}S^2_{(g_1+g_2)}(w,1,1)$$

$$d_0=\sum_{w\in GF^n(2)}S^2_{(f)}(w,0,0),\quad d_1=\sum_{w\in GF^n(2)}S^2_{(f)}(w,1,0)$$

$$d_2=\sum_{w\in GF^n(2)}S^2_{(f)}(w,0,1),\quad d_3=\sum_{w\in GF^n(2)}S^2_{(f)}(w,1,1)$$

$$A_j=\sum_{\substack{w_j,\cdots,w_1\in GF^n(2)\\ w_1\neq 0}}S^2_{(G^j_1)}(w_j,\cdots,w_1,0,0)$$

$$B_j=\sum_{\substack{w_j,\cdots,w_1\in GF^n(2)\\ w_1\neq 0}}S^2_{(G^j_2)}(w_j,\cdots,w_1,0,0)$$

$$C_j=\sum_{\substack{w_j,\cdots,w_1\in GF^n(2)\\ w_1\neq 0}}S^2_{(G^j_1+G^j_2)}(w_j,\cdots,w_1,0,0)$$

$$D_j=\sum_{\substack{w_j,\cdots,w_1\in GF^n(2)\\ w_1\neq 0}}S^2_{(F^j)}(w_j,\cdots,w_1,0,0)$$

由无记忆组合函数的“能量守恒定理”可得

$$a_0+a_1+a_2+a_3=1,\quad b_0+b_1+b_2+b_3=1$$

$$c_0+c_1+c_2+c_3=1,\quad d_0+d_1+d_2+d_3=1$$

4 猜想与部分证明

命题 1 （带多比特记忆组合生成器的“广义能量守恒定理”）对 $1\leq i\leq j$, Z_j 与 $X^{(j)}, X^{(j-1)}, \cdots, X^{(j-i+1)}$ 的所有线性函数

$$w_0\circ X^{(j)}+w_1\circ X^{(j-1)}+\cdots+w_i\circ X^{(j-i+1)},\quad w_0,w_1,\cdots,w_i\in GF^n(2)$$

的相关系数平方和的极限小于等于 $1(i,j\to\infty)$, 且除特殊情况外其极限为 1。

由第 2 节的概率模型易知, 某一时刻 j 的输出与它以前的一段时间 i 内的输入的相关性与时刻 j 无关, 只与时间长度 i 有关。所以上述命题等价于命题 2。

命题 2 对 $j\geq 1$, Z_j 与 $X^{(j)}, X^{(j-1)}, \cdots, X^{(1)}$ 的所有线性函数

$$w_j\circ X^{(j)}+w_{j-1}\circ X^{(j-1)}+\cdots+w_i\circ X^{(1)},\quad w_1,w_2,\cdots,w_j\in GF^n(2)$$

的相关系数平方和的极限小于等于 $1(j\to\infty)$, 且除特殊情况外其极限为 1。

事实上对每个 $j\geq 1$, $Z_j=F^j(X^{(j)},X^{(j-1)},\cdots,X^{(1)},Y^{(0)})$, 由无记忆组合函数的“能量守恒定理”可知 Z_j 与 $X^{(j)}, X^{(j-1)}, \cdots, X^{(1)}$ 的所有线性函数的相关系数平方和小于等于 1, 所以其极限也小于等于 1。故关键是证明命题的后半部分。

下面就一种特殊情况: 即当把

$$S_{(F^j)}(w_j,w_{j-1},\cdots,w_1,0,0),\ w_j,w_{j-1},\cdots,w_1\in GF^n(2),\ w_1\neq 0$$

用引理 1 和引理 2 分解再平方后, 只有平方项而所有交叉相乘的项都为 0 时, 来证明猜想成

立。

引理 3　若 $n+2$ 元布尔函数 $h=f, g_1, g_2$ 或 g_1+g_2 时都有

$$\sum_{w\in GF^n(2)} S_{(h)}(w,1,0)S_{(h)}(w,0,1)=0 \tag{1}$$

$$\sum_{w\in GF^n(2)} S_{(h)}(w,1,0)S_{(h)}(w,1,1)=0 \tag{2}$$

$$\sum_{w\in GF^n(2)} S_{(h)}(w,0,1)S_{(h)}(w,1,1)=0 \tag{3}$$

则, 对 $j\geq 2$

$$D_j=d_1A_{j-1}+d_2B_{j-1}+d_3C_{j-1},\quad A_j=a_1A_{j-1}+a_2B_{j-1}+a_3C_{j-1}$$

$$B_j=b_1A_{j-1}+b_2B_{j-1}+b_3C_{j-1},\quad C_j=c_1A_{j-1}+c_2B_{j-1}+c_3C_{j-1}$$

证明　由引理 2 易证。

引理 4　条件同引理 3, 并且行列式

$$\begin{vmatrix} 1-a_1 & -a_2 & -a_3 \\ -b_1 & 1-b_2 & -b_3 \\ -c_1 & -c_2 & 1-c_3 \end{vmatrix}\neq 0$$

则$\sum_{j=1}^{\infty}A_j=1, \sum_{j=1}^{\infty}B_j=1, \sum_{j=1}^{\infty}C_j=1$

证明　由引理 3 A_j, B_j, C_j 满足线性递归方程组

$$A_j=a_1A_{j-1}+a_2B_{j-1}+a_3C_{j-1}$$

$$B_j=b_1A_{j-1}+b_2B_{j-1}+b_3C_{j-1}$$

$$C_j=c_1A_{j-1}+c_2B_{j-1}+c_3C_{j-1},\qquad j\geq 2$$

因为 g_1, g_2, g_1+g_2 都是平衡的布尔函数, 所以在零点的 Walsh 谱值为 0, 所以

$$A_1=a_0, B_1=b_0, C_1=c_0$$

为解上面的线性递归方程组, 引入生成函数

$$A(x)=\sum_{j=1}^{\infty}A_jx^j,\ B(x)=\sum_{j=1}^{\infty}B_jx^j,\ C(x)=\sum_{j=1}^{\infty}C_jx^j$$

由线性递归方程组可得方程组

$$(1-a_1x)A(x)-a_2xB(x)-a_3xC(x)=a_0x$$

$$-b_1xA(x)+(1-b_1x)B(x)-b_3xC(x)=b_0x$$

$$-c_1xA(x)-c_2xB(x)+(1-c_3x)C(x)=c_0x$$

令

$$T(x)=\begin{vmatrix} 1-a_1x & -a_2x & -a_3x \\ -b_1x & 1-b_2x & -b_3x \\ -c_1x & -c_2x & 1-c_3x \end{vmatrix}$$

当 $T(x)\neq 0$ 时, 方程组有唯一解

$$A(x)=\frac{1}{T(x)}\begin{vmatrix} a_0x & -a_2x & -a_3x \\ b_0x & 1-b_2x & -b_3x \\ c_0x & -c_2x & 1-c_3x \end{vmatrix},\quad B(x)=\frac{1}{T(x)}\begin{vmatrix} 1-a_1x & a_0x & -a_3x \\ -b_1x & b_0x & -b_3x \\ -c_1x & c_0x & 1-c_3x \end{vmatrix}$$

$$C(x)=\frac{1}{T(x)}\begin{vmatrix}1-a_1x & -a_2x & a_0x\\ -b_1x & 1-b_2x & b_0x\\ -c_1x & -c_2x & c_0x\end{vmatrix}$$

特别地, 若

$$T(1)=\begin{vmatrix}1-a_1 & -a_2 & -a_3\\ -b_1 & 1-b_2 & -b_3\\ -c_1 & -c_2 & 1-c_3\end{vmatrix}\neq 0$$

注意到 $a_0+a_1+a_2+a_3=1$, $b_0+b_1+b_2+b_3=1$, $c_0+c_1+c_2+c_1=1$, 可得

$$A(1)=\frac{\begin{vmatrix}a_0 & -a_2 & -a_3\\ b_0 & 1-b_2 & -b_3\\ c_0 & -c_2 & 1-c_3\end{vmatrix}}{\begin{vmatrix}1-a_1 & -a_2 & -a_3\\ -b_1 & 1-b_2 & -b_3\\ -c_1 & -c_2 & 1-c_3\end{vmatrix}}=1$$

所以$\sum_{j=1}^{\infty}A_j=A(1)=1$。同理可得: $\sum_{j=1}^{\infty}B_j=1$。$\sum_{j=1}^{\infty}C_j=1$。

定理 1　条件同引理4, 则对 $j\geq 1$, Z_j 与$X^{(j)}, X^{(j-1)}, \cdots, X^{(1)}$ 的所有线性函数的相关系数平方和 M_j 的极限等于 1($j\to\infty$)。

证明　把 $X^{(j)}, X^{(j-1)}, \cdots, X^{(1)}$ 的所有线性函数分类如下

$$I_1=\{w_j\circ X^{(j)}\mid w_j\in GF^n(2)\}$$

$$I_2=\{w_j\circ X^{(j)}+w_{j-1}\circ X^{(j-1)}\mid w_j, w_{j-1}\in GF^n(2), w_{j-1}\neq 0\}\cdots$$

$$I_j=\{w_j\circ X^{(j)}+\cdots+w_1\circ X^{(1)}\mid w_j, \cdots, w_1\in GF^n(2), w_1\neq 0\}$$

由第 2 节的概率模型知输出与输入的相关性与时刻无关, 即

$$C(Z_j, w_j\circ X^{(j)})=C(Z_1, w_j\circ X^{(1)})=S_{(f)}(w_j, 0, 0)$$

$$C(Z_j, w_j\circ X^{(j)}+w_{j-1}X^{(j-1)})=C(Z_2, w_j\circ X^{(2)}+w_{j-1}\circ X^{(1)})=S_{(F^2)}(w_j, w_{j-1}, 0, 0)\cdots$$

所以, Z_j 与 I_1 中的线性函数的相关系数平方和等于 d_0; Z_j 与 I_k 中的线性函数的相关系数平方和等于D_k, $2\leq k\leq j$。再由引理 3 可得

Z_j 与$X^{(j)}, X^{(j-1)}, \cdots, X^{(1)}$ 的所有线性函数的相关系数平方和

$$M_j=d_0+\sum_{k=2}^{j}D_k=d_0+d_1\sum_{k=1}^{j-1}A_k+d_2\sum_{k=1}^{j-1}B_k+d_3\sum_{k=1}^{j-1}C_k$$

由引理4 可得

$$\lim_{j\to\infty}M_j=d_0+d_1\sum_{k=1}^{\infty}A_k+d_2\sum_{k=1}^{\infty}B_k+d_3\sum_{k=1}^{\infty}C_k$$

$$=d_0+d_1+d_2+d_3=1$$

5　结束语

对于带任意 r 比特记忆的组合生成器, 用上面的方法可得完全类似的结果, 只不过证明过程看起来更复杂一些, 这是因为其状态函数是 r 维向量函数, 在做类似引理 1 和引理 2 中的谱分解时, 向量函数各分量的所有 2^r-1 个非零线性和都会出现。

本文对带多比特记忆的组合生成器提出了"广义能量守恒猜想"并给出了部分证明。此猜想的完全证明, 第四节中使行列式 $T(1)=0$ 的条件的分析, 以及更一般的使输出与输入的相关系数平方和的极限小于1 甚至等于0的充分必要条件都是有待进一步研究的问题。这些问题的解决对于带多比特记忆组合生成器的设计和相关性分析有重要意义。

参考文献:

[1] Siegenthaler T. Correlation immunity of nonlinear combining functions for cryptographic applications[J]. IEEE Transactions on Information Theorem, Sep. 1984, vol. IT-30, 776-780.

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, Jan. 1985, vol. C-34, 81-85.

[3] Rueppel R A. Analysis and Design of Stream Cipher[M]. Springer-Verlag, Berlin, 1986.

[4] Rueppel R A. Correlation immunity and the summation generator[A]. Advances in Crypto-Crypto'85[C]. LNCS, vol. 218, Springer-Verlag, Berlin, 1986, 260-272.

[5] 丁存生, 肖国镇. 流密码学及其应用[M]. 国防工业出版社, 1994.

[6] Meier W, Staffelbach O. Correlation properties of combiners with memory in stream cipher[J]. Journal of Cryptology, 1992; 5(1): 67-86.

[7] 李世取, 曾本胜, 廉玉忠. 布尔向量联合分布的分解式及其应用[J]. 通信学报, 1998; 19(11): 61-64.

[8] 张卫明, 李世取. 带记忆组合生成器的相关免疫性[J]. 密码学进展——Chinacrypt'2002. 电子工业出版社, 2002, 21-30.

Conjecture of Generalized Conservation of Energy on Combiners with an Arbitrary Number of Memory and a Partial Proof

ZHANG Wei-ming,　LI Shi-qu

(Department of application mathematics, Information Engineering University, Zhengzhou 450002)

Abstract: Conjecture of generalized conservation of energy on binary combiners with an arbitrary number r of memory is brought up, which means the sum of the correlation coefficients between the output at time j and all linear functions of inputs before time j converges to 1 as j approaching infinity. And a partial proof is given.

Keywords: combiners with memory; conservation of energy theorem; properties of correlation; correlation immunity