蓝牙组合生成器相关系数的计算方法

张卫明 姚 凯 李世取
（信息工程大学信息研究系 郑州 450002）

摘 要： 蓝牙组合生成器是蓝牙协议中使用的密钥流生成算法，它是一个带 4 bit 记忆的非线性组合生成器，其输入和输出之间相关系数的表示和计算是一个困难的问题，而这是对这种生成器进行相关性分析和相关攻击的基础。该文对一般的带记忆组合生成器给出了相关系数和条件相关系数的计算公式，该公式易于实现快速计算。基于此公式计算了蓝牙组合生成器的各种相关系数，并列出了部分结果。

关键词： 流密码，带记忆组合生成器，蓝牙组合生成器，相关系数
中图分类号： TN918.1 **文献标识码：** A **文章编号：** 1009-5896(2005)09-1470-06

Computing Correlation Coefficients of Bluetooth Combiner

Zhang Wei-ming Yao Kai Li Shi-qu
(*Department of Information Research, Information Engineering University, Zhengzhou* 450002, *China*)

Abstract The bluetooth combiner, a combiner with four bit memory, is the stream cipher used in bluetooth protocols. The expression and computation of correlation coefficients between inputs and outputs of this combiner is difficult, while this is the base of correlation analysis and correlation attack to it. In this paper, the formulas for correlation coefficients and conditional correlation coefficients of general combiners with memory are presented, with which the coefficients can be computed fast. By using these formulas, all kinds of correlation coefficients of bluetooth combiner are computed, and some results are list in the paper.

Key words Stream cipher, Combiners with memory, Bluetooth combiner, Correlation coefficients

1 引言

带记忆组合生成器是 Rueppel[1]提出的一类密钥流生成器，因其能生成性能良好的密钥流序列而受到重视，关于带记忆组合生成器的研究结果可参见文献[2－8]。这种密钥流生成器已被应用于“蓝牙技术”中，1999 年“蓝牙特别兴趣组”公布的“蓝牙技术标准 1.0”[9]中保障蓝牙器件之间通信安全的加密算法 E_0 就是一个带 4 bit 记忆的组合生成器，即所谓的“蓝牙组合生成器”[10]。关于带 1bit 记忆组合生成器的研究结果已比较完善，但长期以来，对一般的带多比特记忆组合生成器的研究进展相对缓慢，一个主要原因是其相关系数计算非常复杂，没有一个好的表达方法可作为分析工具。Golić[4]给出过一个概率算法——LSCA 方法，但它不是一个一般性的表达式，不能表示出全部的线性相关性。另外对蓝牙生成器进行相关攻击的先决条件是寻找连续一段输入与对应的连续一段输出之间具有大的相关性的线性函数对，Hermelin 和 Neyberg[10]对蓝牙生成器提出了一个递推公式，并用它对 4 bit 长的输入输出找出了一个具有相关性的线性对，由此对蓝牙生成器给出了一个理论上的攻击方法。Ekdahl 和 Johansson[11]对 5 bit 长和 6 bit 长的情况各找到了一个具有更大相关性的线性对。Golić[12]对蓝牙生成器穷举了 6 bit 长以内的具有相关性和各种条件相关性的线性对，并以此为基础，对蓝牙生成器给出了一种理论攻击方法。

本文利用 Walsh 谱得到了一般的带记忆组合生成器相关系数的计算公式和条件相关系数的计算公式，它们可以表示任意比特长线性对的相关系数，并能实现快速计算。利用这些公式，我们对蓝牙组合生成器计算了 11bit 长以内的所有线性对的相关系数，和 8 bit 长以内所有线性对的条件相关系数，并在第 5 节列出了部分计算结果。

2 带记忆组合生成器的概率模型

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，如无特别说明它们之间的运算都是 GF(2) 上的加法或乘法运算。

具有 r bit 记忆和 n 个输入的非线性组合生成器定义为

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

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

2004-03-18 收到，2005-01-17 收回
国家自然科学基金(60473022)资助课题

其中 $V:\mathrm{GF}^n(2)\times\mathrm{GF}^r(2)\to\mathrm{GF}^r(2)$ 为状态向量函数，$f:\mathrm{GF}^n(2)\times\mathrm{GF}^r(2)\to\mathrm{GF}(2)$ 为输出函数，$\boldsymbol{y}^{(j)}=(y_{1j},y_{2j},\cdots,y_{rj})$ 是时刻 j 的状态向量，$\boldsymbol{y}^{(0)}$ 为初始状态，$\boldsymbol{x}^{(j)}=(x_{1j},x_{2j},\cdots,x_{nj})$ 为时刻 j 的输入向量(如图 1)。

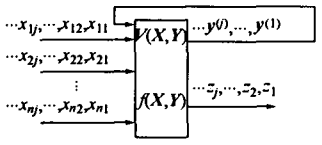

图 1　带记忆非线性组合生成器

作为密钥流生成器，可假设 $f(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r})$ 是平衡的 $n+r$ 元布尔函数，$V(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r})$，$=(g_1(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r}),\cdots,g_r(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r}))$ 是平衡的 $n+r$ 元 r 维布尔向量函数，这等价于当 $X_1,\cdots,X_n,X_{n+1},\cdots,X_{n+r}$ 是相互独立且都具有均匀分布的布尔随机变量时，$g_1(X_1,\cdots,X_n,X_{n+1},\cdots,X_{n+r}),\cdots,g_r(X_1,\cdots,X_n,X_{n+1},\cdots,X_{n+r})$，是 r 个相互独立且都具有均匀分布的布尔随机变量；又设

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

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

最后记

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

由 $\boldsymbol{Y}^{(0)}$和$\boldsymbol{X}^{(1)}$ 相互独立且分布都是均匀的和 $g_1(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r}),\cdots,g_r(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r}))$ 是平衡的 $n+r$ 元 r 维布尔向量函数可递归得到对每个 $j>1$，$\boldsymbol{Y}^{(j)}$ 都与 $\boldsymbol{Y}^{(0)}$ 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；再由 $f(x_1,x_2,\cdots,x_n,x_{n+1},\cdots,x_{n+r})$ 是平衡的 $n+r$ 元布尔函数，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。我们的目的是分析 $\{Z_j,j\geq 1\}$ 和 $\{\boldsymbol{X}^{(j)},j\geq 1\}$ 之间的相关性。

3　带记忆组合生成器相关系数的计算公式

下面设 $\boldsymbol{X}=(X_1,X_2,\cdots,X_n)$ 是布尔随机向量，其中 $X_1,X_2,\cdots,X_n$ 独立均匀分布。对 $\boldsymbol{w}=(w_1,w_2,\cdots,w_n)\in\mathrm{GF}^n(2)$ 记

$$\boldsymbol{w}\cdot\boldsymbol{X}=w_1X_1+w_2X_2+\cdots+w_nX_n$$

V 是上一节定义的向量函数，对 $\boldsymbol{u}=(u_1,u_2,\cdots,u_r)\in\mathrm{GF}^n(2)$ 记

$$\boldsymbol{u}\cdot V=u_1g_1+u_2g_2+\cdots+u_rg_r$$

定义 1　设 $h_1(x_1,x_2,\cdots,x_n)$ 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

$$c(h_1,h_2)=P\{h_1(\boldsymbol{X})=h_2(\boldsymbol{X})\}-P\{h_1(\boldsymbol{X})\neq h_2(\boldsymbol{X})\}$$

若 $h_2=\boldsymbol{w}\cdot\boldsymbol{X},\boldsymbol{w}\in\mathrm{GF}^n(2)$，则利用 Walsh 循环谱[13]有：$c(h_1,h_2)=S_{(h_1)}(\boldsymbol{w})$

下面设 $\mathrm{GF}^r(2)=\{\boldsymbol{0},\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_{2^r-1}\}$（$\boldsymbol{0}$ 表示 r 维零向量），定理 1 给出了带记忆组合生成器的输入与输出的相关系数的谱分解式。

定理 1　具有 r bit 记忆和 n 个输入的组合生成器，对 $j>k>0$，设 $u_j,u_{j-1},u_{j-2},\cdots,u_{j-k}\in\mathrm{GF}(2)$，$\boldsymbol{w}_j,\cdots,\boldsymbol{w}_{j-k}\in\mathrm{GF}^n(2)$，则 $u_jZ_j+\cdots+u_{j-k}Z_{j-k}$ 与 $\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}$ 的相关系数：

$$c(u_jZ_j+\cdots+u_{j-k}Z_{j-k},\ \boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)})$$
$$=(S_{(u_jf)}(\boldsymbol{w}_j,\boldsymbol{0}),S_{(u_jf)}(\boldsymbol{w}_j,\boldsymbol{v}_1),\cdots,S_{(u_jf)}(\boldsymbol{w}_j,\boldsymbol{v}_{2^r-1}))$$
$$\cdot\boldsymbol{E}_{j-1}\cdot\boldsymbol{E}_{j-2}\cdots\boldsymbol{E}_{j-k+2}\cdot\boldsymbol{E}_{j-k+1}\cdot\begin{pmatrix}S_{(u_{j-k}f)}(\boldsymbol{w}_{j-k},\boldsymbol{0})\\S_{(v_1\cdot V+u_{j-k}f)}(\boldsymbol{w}_{j-k},\boldsymbol{0})\\S_{(v_2\cdot V+u_{j-k}f)}(\boldsymbol{w}_{j-k},\boldsymbol{0})\\\vdots\\S_{(v_{2^r-1}\cdot V+u_{j-k}f)}(\boldsymbol{w}_{j-k},\boldsymbol{0})\end{pmatrix}$$

其中

$$\boldsymbol{E}_i=\begin{pmatrix}S_{(u_if)}(\boldsymbol{w}_i,\boldsymbol{0}) & S_{(u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_1) & \cdots S_{(u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_{2^r-1})\\ S_{(v_1\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{0}) & S_{(v_1\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_1) & \cdots S_{(v_1\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_{2^r-1})\\ \vdots & \vdots & \vdots\\ S_{(v_{2^r-1}\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{0}) & S_{(v_{2^r-1}\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_1) & \cdots S_{(v_{2^r-1}\cdot V+u_if)}(\boldsymbol{w}_i,\boldsymbol{v}_{2^r-1})\end{pmatrix}$$
$$j-k+1\leq i\leq j-1$$

证明　由第 2 节的概率模型知，输入与输出的相关系数与时刻无关，只与时间长度有关，因而不失一般性可令 $k=j-1$，即考察 $u_jZ_j+\cdots+u_1Z_1$ 与 $\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\boldsymbol{w}_{j-1}\cdot\boldsymbol{X}^{(j-1)}+\cdots+\boldsymbol{w}_1\cdot\boldsymbol{X}^{(1)}$ 的相关系数即可。为简便，只对 $r=2$，即对带 2 bit 记忆的组合生成器进行证明。

带 2 bit 记忆组合生成器定义为

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

定义复合函数： $G_1^1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})=g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$

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

一般地，可定义 $G_1^j(\boldsymbol{x}^{(j)},\boldsymbol{x}^{(j-1)},\cdots,\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$

类似地定义 $G_2^1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})=g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$

$$G_2^2(\boldsymbol{x}^{(2)},\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})=g_2(\boldsymbol{x}^{(2)},g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)}),g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)}))\cdots$$

$$G_2^j(\boldsymbol{x}^{(j)},\boldsymbol{x}^{(j-1)},\cdots,\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$$

和

$$F^1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})=f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$$

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

$$F^j(\boldsymbol{x}^{(j)},\boldsymbol{x}^{(j-1)},\cdots,\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})$$

这里 G_1^j,G_2^j,F^j 都是 $nj+2$ 元布尔函数。

对给定的 $u\in \mathrm{GF}(2)$， $x\in \mathrm{GF}^n(2)$， $(t_1,t_2,t)\in \mathrm{GF}^3(2)$ ，记

$$N(u,x,t_1,t_2,t)=|\{(y_1,y_2):g_1(x,y_1,y_2)=t_1,\ g_2(x,y_1,y_2)=t_2,uf(x,y_1,y_2)=t\}|$$

易知 $N(u,x,t_1,t_2,t)=4P\{g_1(x,Y_1,Y_2)=t_1,\ g_2(x,Y_1,Y_2)=t_2,uf(x,Y_1,Y_2=t\}$ 。

由 Z_1,Z_2,F^1,F^2 的定义可得

$$c(u_2Z_2+u_1Z_1,\boldsymbol{w}_2\cdot\boldsymbol{X}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{X}^{(1)})=S_{(u_2F^2+u_1F^1)}(\boldsymbol{w}_2,\boldsymbol{w}_1,\boldsymbol{0},\boldsymbol{0}),$$

此处 $(\boldsymbol{0},\boldsymbol{0})\in \mathrm{GF}^2(2)$ 是 2 维零向量。

再由 walsh 谱的定义，

$$\begin{aligned}
&S_{(u_2F^2+u_1F^1)}(\boldsymbol{w}_2,\boldsymbol{w}_1,\boldsymbol{0},\boldsymbol{0})\\
&=\frac{1}{2^{2n+2}}\sum_{\boldsymbol{x}^{(2)}\in \mathrm{GF}^n(2)}\sum_{\boldsymbol{x}^{(1)}\in \mathrm{GF}^n(2)}\sum_{y_{10}\in \mathrm{GF}(2)}\sum_{y_{20}\in \mathrm{GF}(2)}\\
&\quad\cdot(-1)^{u_2f(\boldsymbol{x}^{(2)},g_1(\boldsymbol{x}^{(1)},y_{10},y_{20}),g_2(\boldsymbol{x}^{(1)},y_{10},y_{20}))+u_1f(\boldsymbol{x}^{(1)},y_{10},y_{20})+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&=\frac{1}{2^{2n+2}}\sum_{\boldsymbol{x}^{(2)}\in \mathrm{GF}^n(2)}\sum_{\boldsymbol{x}^{(1)}\in \mathrm{GF}^n(2)}\sum_{t_1\in \mathrm{GF}(2)}\sum_{t_2\in \mathrm{GF}(2)}\sum_{t\in \mathrm{GF}(2)}\\
&\quad\cdot(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+t+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}N(u_1,\boldsymbol{x}^{(1)},t_1,t_2,t)\\
&=\frac{1}{2^{2n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{\boldsymbol{x}^{(1)}}\sum_{t_1}\sum_{t_2}\sum_{t}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+t+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad\cdot 4P\{g_1(\boldsymbol{x}^{(1)},Y_{10},Y_{20})=t_1,g_2(\boldsymbol{x}^{(1)},Y_{10},Y_{20})\\
&=t_2,u_1f(\boldsymbol{x}^{(1)},Y_{10},Y_{20})=t\}\\
&=\frac{1}{2^{2n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{\boldsymbol{x}^{(1)}}\sum_{t_1}\sum_{t_2}\sum_{t}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+t+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad\cdot[P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1\}\\
&\quad+P\{g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_2\}+P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})\\
&\quad+g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1+t_2\}\\
&\quad+P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1+t\}\\
&\quad+P\{g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_2+t\}\\
&\quad+P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})\\
&\quad+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1+t_2+t\}-3] \qquad (1)
\end{aligned}$$

$$\begin{aligned}
&=\frac{1}{2^{2n+3}}\sum_{\boldsymbol{x}^{(2)}}\sum_{\boldsymbol{x}^{(1)}}\sum_{t_1}\sum_{t_2}\sum_{t}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+t+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad\cdot[2P\{u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t\}-1\\
&\quad+2P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1+t\}-1\\
&\quad+2P\{g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_2+t\}-1\\
&\quad+2P\{g_1(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})+g_2(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})\\
&\quad+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{Y}^{(0)})=t_1+t_2+t\}-1]\\
&=\frac{1}{2^{2n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{\boldsymbol{x}^{(1)}}\sum_{t_1}\sum_{t_2}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad\cdot\left[\frac{1}{4}\sum_{y^{(0)}\in \mathrm{GF}^2(2)}(-1)^{u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})}\right.\\
&\quad+\frac{1}{4}\sum_{y^{(0)}\in \mathrm{GF}^2(2)}(-1)^{g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+t_1}\\
&\quad+\frac{1}{4}\sum_{y^{(0)}\in \mathrm{GF}^2(2)}(-1)^{g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+t_2}\\
&\quad\left.+\frac{1}{4}\sum_{y^{(0)}\in \mathrm{GF}^2(2)}(-1)^{g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+t_1+t_2}\right]\\
&=\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{t_1}\sum_{t_2}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}}\\
&\quad\cdot\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(1)}}\sum_{\boldsymbol{y}^{(0)}}(-1)^{u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad+\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{t_1}\sum_{t_2}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+t_1}\\
&\quad\cdot\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(1)}}\sum_{\boldsymbol{y}^{(0)}}(-1)^{g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad+\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{t_1}\sum_{t_2}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+t_2}\\
&\quad\cdot\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(1)}}\sum_{\boldsymbol{y}^{(0)}}(-1)^{g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&\quad+\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(2)}}\sum_{t_1}\sum_{t_2}(-1)^{u_2f(\boldsymbol{x}^{(2)},t_1,t_2)+\boldsymbol{w}_2\cdot\boldsymbol{x}^{(2)}+t_1+t_2}\\
&\quad\cdot\frac{1}{2^{n+2}}\sum_{\boldsymbol{x}^{(1)}}\sum_{\boldsymbol{y}^{(0)}}(-1)^{g_1(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+g_2(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+u_1f(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(0)})+\boldsymbol{w}_1\cdot\boldsymbol{x}^{(1)}}\\
&=S_{(u_2f)}(\boldsymbol{w}_2,0,0)S_{(u_1f)}(\boldsymbol{w}_1,0,0)+S_{(u_2f)}(\boldsymbol{w}_2,1,0)S_{(g_1+u_1f)}(\boldsymbol{w}_1,0,0)\\
&\quad+S_{(u_2f)}(\boldsymbol{w}_2,0,1)S_{(g_2+u_1f)}(\boldsymbol{w}_1,0,0)\\
&\quad+S_{(u_2f)}(\boldsymbol{w}_2,1,1)S_{(g_1+g_2+u_1f)}(\boldsymbol{w}_1,0,0)
\end{aligned}$$

这里式(1)使用了布尔随机向量联合分布的分解式[14]。

一般地，对于 $j>2$，类似可证 $u_jZ_j+\cdots+u_1Z_1$ 与 $\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\boldsymbol{w}_{j-1}\cdot\boldsymbol{X}^{(j-1)}+\cdots+\boldsymbol{w}_1\cdot\boldsymbol{X}^{(1)}$ 的相关系数：

$$\begin{aligned}
&c(u_jZ_j+\cdots+u_1Z_1,\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_1\cdot\boldsymbol{X}^{(1)})\\
&=S_{(u_jf)}(\boldsymbol{w}_j,0,0)S_{(u_{j-1}F^{j-1}+\cdots+u_1F^1)}(\boldsymbol{w}_{j-1},\cdots,\boldsymbol{w}_1,0,0)\\
&\quad+S_{(u_jf)}(\boldsymbol{w}_j,1,0)S_{(G_1^{j-1}+u_{j-1}F^{j-1}+\cdots+u_1F^1)}(\boldsymbol{w}_{j-1},\cdots,\boldsymbol{w}_1,0,0)\\
&\quad+S_{(u_jf)}(\boldsymbol{w}_j,0,1)S_{(G_2^{j-1}+u_{j-1}F^{j-1}+\cdots+u_1F^1)}(\boldsymbol{w}_{j-1},\cdots,\boldsymbol{w}_1,0,0)\\
&\quad+S_{(u_jf)}(\boldsymbol{w}_j,1,1)S_{(G_1^{j-1}+G_2^{j-1}+u_{j-1}F^{j-1}+\cdots+u_1F^1)}(\boldsymbol{w}_{j-1},\cdots,\boldsymbol{w}_1,0,0) \qquad (2)
\end{aligned}$$

而且，一般地对 $2\le i\le j-1$ 类似可证

$$\begin{pmatrix} S_{(u_iF^i+\cdots+u_1F^1)}(w_i,\cdots,w_1,0,0) \\ S_{(G_1^i+u_iF^i+\cdots+u_1F^1)}(w_i,\cdots,w_1,0,0) \\ S_{(G_2^i+u_iF^i+\cdots+u_1F^1)}(w_i,\cdots,w_1,0,0) \\ S_{(G_1^i+G_2^i+u_iF^i+\cdots+u_1F^1)}(w_i,\cdots,w_1,0,0) \end{pmatrix}$$

$$= \begin{pmatrix} S_{(u_if)}(w_i,0,0) & S_{(u_if)}(w_i,1,0) \\ S_{(g_1+u_if)}(w_i,0,0) & S_{(g_1+u_if)}(w_i,1,0) \\ S_{(g_2+u_if)}(w_i,0,0) & S_{(g_2+u_if)}(w_i,1,0) \\ S_{(g_1+g_2+u_if)}(w_i,0,0) & S_{(g_1+g_2+u_if)}(w_i,,1,0) \end{pmatrix}$$

$$\begin{pmatrix} S_{(u_if)}(w_i,0,1) & S_{(u_if)}(w_i,1,1) \\ S_{(g_1+u_if)}(w_i,0,1) & S_{(g_1+u_if)}(w_i,1,1) \\ S_{(g_2+u_if)}(w_i,0,1) & S_{(g_2+u_if)}(w_i,1,1) \\ S_{(g_1+g_2+u_if)}(w_i,,01) & S_{(g_1+g_2+u_if)}(w_i,1,) \end{pmatrix}$$

$$\cdot \begin{pmatrix} S_{(u_{i-1}F^{i-1}+\cdots+u_1F^1)}(w_{i-1},\cdots,w_1,0,0) \\ S_{(G_1^{i-1}+u_{i-1}F^{i-1}+\cdots+u_1F^1)}(w_{i-1},\cdots,w_1,0,0) \\ S_{(G_2^{i-1}+u_{i-1}F^{i-1}+\cdots+u_1F^1)}(w_{i-1},\cdots,w_1,0,0) \\ S_{(G_1^{i-1}+G_2^{i-1}+u_{i-1}F^{i-1}+\cdots+u_1F^1)}(w_{i-1},\cdots,w_1,0,0) \end{pmatrix} \tag{3}$$

由式(3)递推并结合式(2)，$r=2$ 的情况即可得证。

对一般的带 r bit 记忆的组合生成器用上面的方法类似可证。　　证毕

4　带记忆组合生成器条件相关系数的计算公式

在上一节所得结果的基础上，我们还可以考察各种条件相关系数的计算公式。

定义 2　设 $h_1(x_1,x_2,\cdots,x_n)$ 和 $h_2(x_1,x_2,\cdots,x_n)$ 是 n 元布尔函数，在已知 $\chi\subseteq \mathrm{GF}^n(2)$ 的条件下，h_1 和 h_2 的条件相关系数定义为

$$c(h_1,h_2\mid\chi)=P\{h_1(\boldsymbol{X})=h_2(\boldsymbol{X})\mid \boldsymbol{X}\in\chi\}-P\{h_1(\boldsymbol{X})\neq h_2(\boldsymbol{X})\mid \boldsymbol{X}\in\chi\}$$

4.1　已知一条输入序列的条件相关系数计算公式

在相关攻击中，有时可以穷举一条级数较短的移位寄存器序列，在此基础上寻找其它输入与输出间的相关性，亦即在已知一条输入的条件下计算条件相关系数。对 n 元布尔函数 $h(x_1,x_2,\cdots,x_n)$，固定 x_1 的值可得两个 $n-1$ 元布尔函数，分别定义为 $h^0(x_2,\cdots,x_n)=h(0,x_2,\cdots,x_n)$ 和 $h^1(x_2,\cdots,x_n)=h(1,x_2,\cdots,x_n)$。一般地，对于 n 元 k 维向量布尔函数 $\boldsymbol{H}(x_1,\cdots,x_n)=(h_1(x_1,\cdots,x_n),\cdots,h_k(x_1,\cdots,x_n))$ 可定义

$$\begin{aligned}\boldsymbol{H}^0(x_2,\cdots,x_n)&=\boldsymbol{H}(0,x_2,\cdots,x_n)\\&=(h_1(0,x_2,\cdots,x_n),\cdots,h_k(0,x_2,\cdots,x_n))\\ \boldsymbol{H}^1(x_2,\cdots,x_n)&=\boldsymbol{H}(1,x_2,\cdots,x_n)\\&=(h_1(1,x_2,\cdots,x_n),\cdots,h_k(1,x_2,\cdots,x_n))\end{aligned}$$

按照此定义，由第 1 节带记忆组合生成器模型中的输出函数 f，可定义 f^0 和 f^1，由状态向量函数 $\boldsymbol{V}$ 可分别定义 $\boldsymbol{V}^0$ 和 $\boldsymbol{V}^1$。下面假设已知第一条移位寄存器的输出，即已知 $\{X_{1i},i\geq 1\}=\{x_{1i},i\geq 1\}$。现若要在已知 $\{X_{1,j-k}=x_{1,j-k},\cdots,X_{1,j}=x_{1,j}\}$ 的条件下求 $u_jZ_j+\cdots+u_{j-k}Z_{j-k}$ 与 $\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}$，的条件相关系数，只需把定理 1 所给计算公式的各矩阵中的 f 和 $\boldsymbol{V}$ 依次换为 $f^{x_{1,j}}$ 和 $\boldsymbol{V}^{x_{1,j}}$ $(i=j,j-1,\cdots,j-k)$即可。

在已知多条移位寄存器序列的条件下，条件相关系数计算公式亦可类似给出，但在实际应用中由于计算能力的限制，一般不会穷举多条移位寄存器序列。

4.2　已知输出序列的条件相关系数计算

记 $\boldsymbol{Z}_{j-k}^j=\{Z_{j-k},\cdots,Z_j\}$，$\boldsymbol{a}_{j-k}^j=\{a_{j-k},\cdots,a_j\}$，用 $\boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j$ 表示事件 $\{Z_{j-k}=a_{j-k},\cdots,Z_j=a_j\}$。下面在已知 $\boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j$ 的条件下，考察 $\boldsymbol{X}^{(j-k)},\cdots,\boldsymbol{X}^{(j)}$ 的线性函数与零函数的相关系数，定理 2 表明已知输出的条件相关系数可由无条件相关系数线性表出。

定理 2　具有 r bit 记忆和 n 个输入的组合生成器，若其输出 $\{Z_j,j\geq 1\}$ 独立均匀分布，则对 $j>k>0$，$\boldsymbol{w}_j,\cdots,\boldsymbol{w}_{j-k}\in \mathrm{GF}^n(2)$，在已知 $\boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j$ 的条件下，$\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}$ 与零函数的条件相关系数：

$$\begin{aligned}&c(\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)},\ 0\mid \boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j)\\&=\sum_{\substack{\boldsymbol{v}\in \mathrm{GF}^{k+1}(2)\\ \boldsymbol{v}\neq\boldsymbol{0}}}(-1)^{\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^j}c(\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^j,\ \boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)})\end{aligned}$$

证明

$$\begin{aligned}&c(\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)},\ 0\mid \boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j)\\&=2P\{\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0\mid \boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j\}-1\\&=2\frac{P\{\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0,\ \boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j\}}{P\{\boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j\}}-1\\&=2^{k+2}P\{\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0,\boldsymbol{Z}_{j-k}^j=\boldsymbol{a}_{j-k}^j\}-1\\&=2^{k+2}\Bigg(\frac{1}{2^k}\sum_{\substack{\boldsymbol{v}\in \mathrm{GF}^{k+1}(2)\\ \boldsymbol{v}\neq\boldsymbol{0}}}P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^j=\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^j,\ \boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots\\&\quad+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0\}\\&\quad-\frac{2^k-1}{2^k}P\{\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0\}\Bigg)-1\qquad(4)\\&=4\sum_{\substack{\boldsymbol{v}\in \mathrm{GF}^{k+1}(2)\\ \boldsymbol{v}\neq\boldsymbol{0}}}P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^j=\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^j,\ \boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}\\&=0\}-2^{k+1}+1=4\sum_{\substack{\boldsymbol{v}\in \mathrm{GF}^{k+1}(2)\\ \boldsymbol{v}\neq\boldsymbol{0}}}\frac{1}{2}\Big(P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^j=\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^j\}\\&\quad+P\{\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}=0\}\\&\quad+P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^j=\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}\\&\quad+\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^j\}-1\Big)-2^{k+1}+1\qquad(5)\end{aligned}$$

$$
\begin{aligned}
&=2\sum_{\substack{v\in GF^{k+1}(2)\\ v\neq 0}} P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^{j}=\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}+\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^{j}\}\\
&\quad -2^{k+1}+1\\
&=\sum_{\substack{v\in GF^{k+1}(2)\\ v\neq 0}} (2P\{\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^{j}=\boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)}\\
&\quad +\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^{j}\}-1)\\
&=\sum_{\substack{v\in GF^{k+1}(2)\\ v\neq 0}} (-1)^{\boldsymbol{v}\cdot\boldsymbol{a}_{j-k}^{j}} c(\boldsymbol{v}\cdot\boldsymbol{Z}_{j-k}^{j},\ \boldsymbol{w}_j\cdot\boldsymbol{X}^{(j)}+\cdots+\boldsymbol{w}_{j-k}\cdot\boldsymbol{X}^{(j-k)})
\end{aligned}
$$

这里式（4）和式（5）式使用了布尔随机向量联合分布的分解式[14]。 证毕

若结合使用上述方法即可得到在同时已知一条输入和输出序列的条件下的条件相关系数计算公式。

5 蓝牙组合生成器的相关系数

上两节得到的公式把带记忆组合生成器连续输入与输出的线性对的相关系数转化成了矩阵相乘的形式，其中矩阵由输出函数和状态向量函数的 Walsh 循环谱组成，对于实际使用的生成器，为了保证输出序列有好的密码学性质，这些矩阵一般都是稀疏矩阵（如蓝牙组合生成器），而且由定理 1 可看出，运算过程的每一步都只是向量和矩阵的乘法，只要某一步出现零相量，就可知相关系数为零，停止运算，所以这种方法非常适合用来快速搜索具有相关性(即相关系数不为零)的线性对。下面用上述方法计算蓝牙组合生成器的相关系数。

“蓝牙协议”是一个短距离无线通信协议，1999 年“蓝牙特别兴趣组”公布了“蓝牙技术标准 1.0”[9]，其安全机制中采用的密钥流生成算法 E_0，事实上就是一个有 4 个输入带 4 bit 记忆的组合生成器，被称作“蓝牙组合生成器”[10]。作为输入的 4 个 LFSR 的长度分别为 25，31，33，39，其反馈多项式均是本原的，抽头数均为 5 个。记 j 时刻 4 个移位寄存器的输出为 $\boldsymbol{x}^{(j)}=(x_{1j},x_{2j},x_{3j},x_{4j})$，状态向量为 $\boldsymbol{c}^{(j)}=(c_{j+1}^{0},c_{j+1}^{1},c_{j}^{0},c_{j}^{1})$，生成器的输出为 z_j，则此生成器定义如下：

$$
\begin{aligned}
z_j &= x_{1j}+x_{2j}+x_{3j}+x_{4j}+c_j^0\\
c_{j+1}^0 &= s_{j+1}^0+c_j^0+c_{j-1}^0+c_{j-1}^1\\
c_{j+1}^1 &= s_{j+1}^1+c_j^1+c_{j-1}^0
\end{aligned}
$$

其中 $(s_{t+1}^1,s_{t+1}^0)=\left\lfloor\dfrac{x_{1j}+x_{2j}+x_{3j}+x_{4j}+2c_j^1+c_j^0}{2}\right\rfloor\in\{0,1,2,3\}$，（此式中加法为十进制加），$(c_0^0,c_0^1,c_{-1}^0,c_{-1}^1)$ 为 4 bit 记忆的初态。

按照第 2 节一般的带记忆组合生成器的模型，我们把蓝牙组合生成器转化成如下形式：

输出函数为

$$z_j=f(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})=x_{1j}+x_{2j}+x_{3j}+x_{4j}+c_j^0$$

状态向量函数为

$$
\begin{aligned}
\boldsymbol{c}^{(j)}&=\boldsymbol{V}(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})=(g_1(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)}),\\
&\quad g_2(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)}),g_3(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)}),g_4(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)}))\\
g_1(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})&=\boldsymbol{c}_j^1+H_1(j)\boldsymbol{c}_j^0+H_2(j)+\boldsymbol{c}_j^0+\boldsymbol{c}_{j-1}^0+\boldsymbol{c}_{j-1}^1\\
g_2(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})&=H_1(j)c_j^0c_j^1+H_1(j)c_j^1+H_3(j)c_j^0+H_4(j)+c_j^1+c_{j-1}^0\\
g_3(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})&=c_j^0\\
g_4(\boldsymbol{x}^{(j)},\boldsymbol{c}^{(j-1)})&=c_j^1
\end{aligned}
$$

其中

$$
\begin{aligned}
H_1(j)&=x_{1j}+x_{2j}+x_{3j}+x_{4j}\\
H_2(j)&=x_{1j}x_{2j}+x_{1j}x_{3j}+x_{1j}x_{4j}+x_{2j}x_{3j}+x_{2j}x_{4j}+x_{3j}x_{4j}\\
H_3(j)&=x_{1j}x_{2j}x_{3j}+x_{1j}x_{2j}x_{4j}+x_{1j}x_{3j}x_{4j}+x_{2j}x_{3j}x_{4j}\\
H_4(j)&=x_{1j}x_{2j}x_{3j}x_{4j}
\end{aligned}
$$

有了上述输出函数和状态函数的表达式，算出它们各种非零线性和的 Walsh 循环谱值，就可利用第 3 节和第 4 节的公式计算连续的输入输出线性对的相关系数了。正如前言中提到的，寻找具有大的相关性（亦即相关系数绝对值较大）的线性对，是对蓝生成器进行相关攻击的关键。文献 [10－12] 分别采用递推关系或穷举法寻找连续 4 bit 长，5 bit 长和 6 bit 长（蓝牙生成器 4 bit 长以下输入输出无相关性）的有大的相关性或条件相关性的线性对，但用递推关系所能找到的线性对非常有限（仅一两个），用穷举法搜索更长的线性对则是计算上困难的。而我们利用第 3 节的公式，对蓝牙生成器计算了 11 bit 长以内的所有线性对的相关系数，并计算了 8 bit 长以内在分别已知输入或输出的条件下所有线性对的条件相关系数。下面的表 1 列出了 5 bit 长到 11 bit 长线性对所能达到的最大相关系数的绝对值，以及相应的线性对个数；表 2 列出了在已知输入或输出的条件下 5 bit 长到 8 bit 长线性对所能达到的最大条件相关系数的绝对值，以及相应的线性对个数。

表 1 5 bit 长到 11 bit 长线性对所能达到的最大相关系数绝对值以及相应的线性对个数

输入输出长度(bit)	最大相关系数绝对值	相应的线性对个数	输入输出长度(bit)	最大相关系数绝对值	相应的线性对个数
5	0.09765625	16	9	0.03662109	16
6	0.09765625	16	10	0.01451969	16
7	0.03814697	16	11	0.01680851	16
8	0.03839111	16			

表 2　已知输入或输出的条件下 5 bit 长到 8 bit 长线性对所能达到的最大条件相关系数绝对值以及相应的线性对个数

输入输出长度 (bit)	已知输入		已知输出	
	最大条件相关系数绝对值	相应的线性对个数	最大条件相关系数绝对值	相应的线性对个数
5	0.11328125	256	0.11328125	64
6	0.13574219	128	0.13574219	48
7	0.08355713	64	0.08380127	24
8	0.09106445	64	0.09204102	8

6　结束语

以前对蓝牙组合生成器的相关性分析，或是通过特殊的递推关系可求出一两个有相关性的线性对 [10, 11]，或是通过穷举可求 6 bit 长以内的有相关性的线性对 [12]。而本文给出了一般的带记忆组合生成器的相关系数计算公式，它可以表示出带记忆组合生成器的全部线性相关性，这对于这类组合生成器的性质分析和设计有重要意义，例如本文定理 1 是文献 [6] 中引理 1、2 的一般化，在文献 [6] 中我们以相关系数表达式为基础对带记忆组合生成器的相关免疫性作了系统分析，并得到了相应的构造方法。另外，本文的公式可以实现快速运算，所以能尽可能多地找出具有大的相关性的线性对，例如用本文的方法，我们可以对蓝牙生成器找到更多的具有大的相关性和条件相关性的线性对，这对于实现对蓝牙生成器的快速相关攻击有重要作用。

参 考 文 献

[1] Rueppel R A. Correlation immunity and the summation generator. Advances in cryptology---CRYPTO 85, California, USA, 1985, LNCS 218: 260 – 272.

[2] Meier W, Staffelbach O. Correlation properties of combiners with memory in stream cipher. *Journal of Cryptology*, 1992, 5(1): 67 – 86.

[3] Staffelbach O, Meire W. Cryptographic significance of the carry for ciphers based on integer addition. Advances in Cryptology-Crypto'90, California, USA, 1990, LNCS 537: 601 – 614.

[4] Golić J Dj. Correlation properties of a general binary combiner with memory. *Journal of Cryptology*, 1996, 9(2): 111 – 126.

[5] Golić J Dj. Fast correlation attacks on the summation generator. *Journal of Cryptology*, 2000, 13(2): 245 – 262.

[6] 张卫明, 李世取. 带记忆组合生成器的相关免疫性. 密码学进展—Chinacrypt'2002, 威海, 2002: 21 – 30.

[7] 张卫明, 李世取. 带 1bit 记忆组合生成器的条件相关性分析. 信息工程大学学报, 2002, 3(2): 13 – 16.

[8] 张卫明, 李世取. 带多 bit 记忆组合生成器的广义能量守恒猜想及部分证明. 工程数学学报, 2003, 20(3): 63 – 69.

[9] Bluetooth ™ SIG. The Bluetooth specification version1.0 [S]. July 1999.

[10] Hermelin M, Nyberg K. Correlation properties of bluetooth combiner generator. The Second International Conference on Information Security and Cryptology (ICISC'99), Seoul, Korea, 1999, LNCS 1787: 17 – 29.

[11] Ekdahl P, Johansson T. Some results on correlations in the bluetooth stream cipher. The 10th Joint Conference of Communications and Coding, Obertauern, Austria, 2000: 11 – 18.

[12] Golić J Dj, Bagini V, Morgari G. Linear cryptanalysis of bluetooth stream cipher. Advances in Cryptology- EUROCRYPT 2002, Amsterdam, The Netherlands, 2002, LNCS 2332: 238 – 255.

[13] 李世取, 曾本胜, 廉玉忠, 等. 密码学中的逻辑函数. 北京: 北京中软电子出版社, 2003: 10 – 13.

[14] 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. 通信学报, 1998, 19(11): 61 – 64.

张卫明：　男，1976 年生，博士生，研究方向为概率论在密码学中的应用.

姚　凯：　男，1977 年生，硕士生，研究方向为密码学.

李世取：　男，1945 年生，教授，研究方向为概率论在密码学中的应用.