GMW-序列的三项生成多项式

祁传达[1],李 刚[2]
QI Chuan-da[1],LI Gang[2]

1.信阳师范学院 数学与信息科学学院,河南 信阳 464000
2.信阳师范学院 计算机与信息技术学院,河南 信阳 464000
1.College of Mathematics and Information Science,Xinyang Normal University,Xinyang,Henan 464000,China
2.College of Computer and Information Technology,Xinyang Normal University,Xinyang,Henan 464000,China

QI Chuan-da,LI Gang.Generation trinomials of GMW-sequences.Computer Engineering and Applications,2009,45(13):90-92.

Abstract: The problem of generation trinomials for GMW-sequences is studied.The structure and count of generation trinomials for GMW-sequences is presented.It is proved that the amount of generation trinomials for GMW-sequences is less than m-sequences with the same period.It is explained that intensity of GMW-sequences resist the fast correlation attacks is greater than m-sequences with the same period.

Key words: GMW sequences;m-sequences;auto-correlate function;trace function

摘 要:研究了GMW-序列的三项生成多项式问题,给出了其三项生成多项式的结构和计数,证明了其三项生成多项式个数远远少于同周期的m-序列,这说明GMW-序列在抵抗快速相关攻击的能力方面要强于同周期的m-序列。

关键词:GMW-序列;m-序列;自相关函数;迹函数
DOI:10.3778/j.issn.1002-8331.2009.13.027 **文章编号:**1002-8331(2009)13-0090-03 **文献标识码:**A **中图分类号:**TP309

在现代扩频通信中,需要使用线性复杂度高、自相关值低的伪随机序列。GMW-序列[1]不仅具有与m-序列一样理想的自相关函数值,而且具有比同周期m-序列更高的线性复杂度,这使得GMW-序列在抵抗B-M算法[2]攻击方面比m-序列更安全。也正是由于这些原因,GMW-序列被大量推广和引用[3-6]。

本文将对GMW-序列的三项生成多项式进行研究,给出了其三项生成多项式的结构和计数,证明了GMW-序列在抵抗快速相关攻击方面具有比m-序列更高的安全性。

1 基本概念

设$n=pm$,$Tr_m^n(\alpha)=\sum\limits_{i=0}^{p-1}\alpha^{2^{mi}}$为$GF(2^n)\to GF(2^m)$的迹函数,则容易验证下列性质[7]:

(1)$Tr_m^n(\alpha)=Tr_m^n(\alpha^{2^{mi}})$,$\forall\alpha\in GF(2^n)$,$(i=1,2,\cdots)$。

(2)$Tr_m^n(\lambda\alpha\oplus\mu\beta)=\lambda Tr_m^n(\alpha)\oplus\mu Tr_m^n(\alpha)$,$\forall\alpha,\beta\in GF(2^n)$,$\lambda,\mu\in GF(2^m)$。

(3)$Tr_1^n(\alpha)=Tr_1^m(Tr_m^n(\alpha))$,$\forall\alpha\in GF(2^n)$。

定义1 设α是$GF(2^n)$的本原元,$m|n$,$r:1\leqslant r<2^m-1$,且$\gcd(r,2^m-1)$,则称序列$a_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}(i=0,1,2,\cdots)$为GMW-序列[1]。

GMW-序列是$GF(2)$上周期$T=2^n-1$的二元序列。特别地,当$m\in\{1,n\}$时,$a_i=Tr_1^n(\alpha^i)$,这时$\{a_i\}_{i=1}^{\infty}$为m-序列;当用二进制表示的r的汉明重$w(r)=1$(即存在$t(0\leqslant t<m)$,使得$r=2^t$)时,

$$a_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^{2^t}\}=\{Tr_1^m[Tr_m^n(\alpha^i)]\}^{2^t}=Tr_1^n(\alpha^i)$$

故$\{a_i\}_{i=1}^{\infty}$也是m-序列。这说明GMW-序列是m-序列的推广。

在定义1中,之所以限定$\gcd(r,2^m-1)=1$,是因为当$\gcd(r,2^m-1)=1$时,所得到的序列周期退化。

2 GMW-序列的三项生成多项式

本章主要讨论GMW-序列$a_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}(i=0,1,2,\cdots)(m|n,r:1\leqslant r<2^m-1$,且$\gcd(r,2^m-1)=1)$的三项生成多项式的结构和计数问题。

三项式$f(x)=1\oplus x^k\oplus x^h(k\neq h)$是序列$\{a_i\}_{i=0}^{\infty}$的生成多项式的充要条件是:对任意的$i:i\geqslant 0$,有$a_i\oplus a_{i+k}\oplus a_{i+h}=0$。鉴于若$1\oplus x^k\oplus x^h$是$\{a_i\}_{i=0}^{\infty}$的生成多项式,则$1\oplus x^{k_1}\oplus x^{h_1}$(其中$k_1=k \bmod T$,$h_1=h \bmod T$,$T$是$\{a_i\}_{i=0}^{\infty}$的周期)也是$\{a_i\}_{i=0}^{\infty}$的生成多项式,以下

基金项目:河南省自然科学基金(the Natural Science Foundation of Henan Province of China under Grant No.072300410030)。
作者简介:祁传达(1965-),男,博士,教授,硕士生导师,主要研究方向为密码理论。
收稿日期:2008-10-06 **修回日期:**2008-11-14

只需讨论$\{a_i\}_{i=0}^{\infty}$的满足条件$0<k,h<T$的生成多项式$f(x)=1\oplus x^k\oplus x^h$的结构和计数。

记$M=\dfrac{2^n-1}{2^m-1}$，$i=j+sM$，其中$0\leqslant j<M$，$0\leqslant s<2^m-1$，由$(\alpha^{sM})^{2^m-1}=\alpha^{(2^n-1)s}=1$知$\alpha^{sM}\in GF(2^m)$，由第1章迹函数性质2，有$Tr_m^n(\alpha^i)=Tr_m^n(\alpha^{j+sM})=\alpha^{Ms}Tr_m^n(\alpha^j)$，从而

$$\begin{aligned}&a_i\oplus a_{i+k}\oplus a_{i+h}=\\&Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}\oplus Tr_1^m\{[Tr_m^n(\alpha^{i+k})]^r\}\oplus Tr_1^m\{[Tr_m^n(\alpha^{i+h})]^r\}=\\&Tr_1^m\{[Tr_m^n(\alpha^i)]^r\oplus[Tr_m^n(\alpha^{i+k})]^r\oplus[Tr_m^n(\alpha^{i+h})]^r\}=\\&Tr_1^m\{\alpha^{Mrs}([Tr_m^n(\alpha^j)]^r\oplus[Tr_m^n(\alpha^{j+k})]^r\oplus[Tr_m^n(\alpha^{j+h})]^r)\}=\\&Tr_1^m(\delta(k,h,j)\alpha^{Mrs})\end{aligned}$$

其中

$$\delta(k,h,j)=[Tr_m^n(\alpha^j)]^r\oplus[Tr_m^n(\alpha^{j+k})]^r\oplus[Tr_m^n(\alpha^{j+h})]^r\qquad(1)$$

所以$a_i\oplus a_{i+k}\oplus a_{i+h}\equiv0(j\geqslant0)$等价于$\delta(k,h,j)\equiv0(0\leqslant j<M)$。由此得到：

定理1 $f(x)=1\oplus x^k\oplus x^h$是GMW-序列$\{a_i\}_{i=0}^{\infty}$的生成多项式的充要条件是：对任意的$j$：$0\leqslant j<M$，都有

$$\delta(k,h,j)\triangleq[Tr_m^n(\alpha^j)]^r\oplus[Tr_m^n(\alpha^{j+k})]^r\oplus[Tr_m^n(\alpha^{j+h})]^r$$

定理2 若$\{a_i\}_{i=0}^{\infty}$是m-序列，则对任意的k：$0<k<T$，都存在唯一的$h(0<h<T,h\neq k)$，使得$1\oplus x^k\oplus x^h$是$\{a_i\}_{i=0}^{\infty}$的生成多项式。

证明 若GMW-序列$\{a_i\}_{i=0}^{\infty}$是m-序列，即$r=2^t(0\leqslant t<2^m)$，这时

$$\begin{aligned}\delta(k,h,j)&=[Tr_m^n(\alpha^j)\oplus Tr_m^n(\alpha^{j+k})\oplus Tr_m^n(\alpha^{j+h})]^{2^t}=\\&[Tr_m^n(\alpha^j\oplus\alpha^{j+k}\oplus\alpha^{j+h})]^{2^t}\end{aligned}$$

由于α是$GF(2^n)$的本原元，故对任意的k：$0<k<T$，都存在唯一的$h(0<h<T,h\neq k)$，使得$1\oplus\alpha^k\oplus\alpha^h=0$，从而$\alpha^j\oplus\alpha^{j+k}\oplus\alpha^{j+h}=0$$(\forall j\geqslant0)$，故

$$\delta(k,h,j)=[Tr_m^n(\alpha^j\oplus\alpha^{j+k}\oplus\alpha^{j+h})]^{2^t}=0$$

由定理1得：对任意的k：$0<k<T$，都存在$h(0<h<T,h\neq k)$，使得$1\oplus x^k\oplus x^h=0$是$\{a_i\}_{i=0}^{\infty}$的生成多项式。

为了讨论GMW-序列三项生成多项式的结构，先给出两个引理。

引理1 对任意的k：$0<k<T$，$k=0\bmod M$，存在唯一的$h(0<h<T)$，使得$\delta(k,h,j)\equiv0(0\leqslant j<M)$，且$k_2=0\bmod M$，$k_2\neq k_1$。

证明 先证α^{Mr}是$GF(2^m)$的本原元。由于$(\alpha^M)^{2^m-1}=\alpha^{2^n-1}=1$，假定存在$k$：$0<k<2^m-1$，使得$(\alpha^M)^k=\alpha^{Mk}=1$，但$Mk<2^n-1$，此与$\alpha$是$GF(2^n)$的本原元矛盾。故$\alpha^M$是$GF(2^m)$的本原元，又由于$\gcd(r,2^m-1)$，故$\alpha^{Mr}$是$GF(2^m)$的本原元。

对任意的k：$0<k<T$，$k=0\bmod M$，不妨设$k=i_1M(1\leqslant i_1<2^m-1)$，由$\alpha^{Mr}$是$GF(2^m)$的本原元知：存在唯一的$i_2(1\leqslant i_2<2^m-1,i_2\neq i_1)$，使得$1\oplus\alpha^{i_1Mr}\oplus\alpha^{i_2Mr}=0$，令$h=i_2M$，则$0<h<T$，$h=0\bmod M$，$h\neq k$，这时有

$$\begin{aligned}\delta(k,h,j)&=[Tr_m^n(\alpha^j)]^r\oplus[Tr_m^n(\alpha^{j+i_1M})]^r\oplus[Tr_m^n(\alpha^{j+i_2M})]^r=\\&[Tr_m^n(\alpha^j)]^r\oplus[\alpha^{i_1M}Tr_m^n(\alpha^j)]^r\oplus[\alpha^{i_2M}Tr_m^n(\alpha^j)]^r=\\&(1\oplus\alpha^{i_1Mr}\oplus\alpha^{i_2Mr})[Tr_m^n(\alpha^j)]^r=0\end{aligned}$$

下证唯一性。假定存在$h'(0<h'<P)$，使得$\delta(k,h',j)\equiv0$$(0\leqslant j<M)$，根据定理1有$a_i\oplus a_{i+k}=a_{i+h}$和$a_i\oplus a_{i+k}=a_{i+h'}$$(i=0,1,\cdots)$，所以$a_{i+h}=a_{i+h'}(i=0,1,\cdots)$，故$h'=h\bmod P$，又$0<h,h'<P$，所以$h'=h$。唯一性得证。

引理2 设$m\notin\{1,n\}$，$1\leqslant r<2^m-1$，且$w(r)\neq1$。若$\delta(k,h,j)\equiv0(0\leqslant j<M)$，则必有$k=h=0\bmod M(0<k,h<T)$。

证明 若$\delta(k,h,j)\equiv0(0\leqslant j<M)$，记$x=\alpha^{(2^m-1)j}$，则

$$\begin{aligned}&[Tr_m^n(\alpha^{j+k})]^r=\left[\alpha^{j+k}\oplus\alpha^{2^m(j+k)}\oplus\alpha^{2^{2m}(j+k)}\oplus\cdots\oplus\alpha^{2^{(p-1)m}(j+k)}\right]^r=\\&\alpha^{rj}\left[\alpha^k\oplus\alpha^{2^mk}\oplus\alpha^{(2^m-1)j}\oplus\alpha^{2^{2m}k}(\alpha^{(2^m-1)j})^{2^m+1}\oplus\right.\\&\left.\cdots\oplus\alpha^{2^{(p-1)m}k}(\alpha^{(2^m-1)j})^{\frac{2^{(p-1)m}-1}{2^m-1}}\right]^r=\\&\alpha^{rj}\left(\alpha^k\oplus\alpha^{2^mk}x\oplus\alpha^{2^{2m}k}x^{2^m+1}\oplus\cdots\oplus2^{2^{(p-1)m}k}x^{\frac{2^{(p-1)m}-1}{2^m-1}}\right)^r=\\&\alpha^{rj}\left[(\alpha^k\oplus\alpha^{2^mk}x)\oplus\alpha^{2^m+1}g_k(x)\right]^r=\\&\alpha^{rj}\left(\sum_{i=0}^{r}(C_r^i\bmod2)\alpha^{k(r-i)+2^mki}x^i\oplus\alpha^{2^m+1}g_k(x)\right)\end{aligned}\qquad(2)$$

其中$g(x)$是关于x的多项式，记$x^{2^m+1}g_k(x)$的次数为N，则

$$N=\frac{2^{(p-1)m}-1}{2^m-1}r<2^{(p-1)m}-1<M$$

让式(2)中的k分别取$0,k,h$并代入式(1)得：

$$\begin{aligned}\delta(k,h,j)=&\alpha^{rj}\left[\sum_{i=0}^{r}(C_r^i\bmod2)(1\oplus\alpha^{k(r-i)+2^mki}\oplus\alpha^{h(r-i)+2^mhi})x^i\right.\\&\left.\oplus x^{2^m+1}(g_0(x)\oplus g_k(x)\oplus g_h(x))\right]=\\&\alpha^{rj}\left[\sum_{i=0}^{r}(C_r^i\bmod2)(1\oplus\beta^{ki}\alpha^{kr}\oplus\beta^{hi}\alpha^{hr})x^i\right.\\&\left.\oplus x^{2^m+1}(g_0(x)\oplus g_k(x)\oplus g_h(x))\right]\end{aligned}$$

其中，$\beta=\alpha^{2^m-1}$。因为对于不同的j：$0\leqslant j<M$，$x=\alpha^{(2^m-1)j}$互不相同，所以$\delta(k,h,j)\equiv0(0\leqslant j<M)$等价于$N$次方程

$$\sum_{i=0}^{r}(C_r^i\bmod2)(1\oplus\beta^{ki}\alpha^{kr}\oplus\beta^{hi}\alpha^{hr})x^i\oplus x^{2^m+1}(g_0(x)\oplus g_k(x)\oplus g_h(x))=0\qquad(3)$$

有M个不同的根。由于$M>N$，由Lagrange插值公式知：方程(3)的系数全为零。

由于$w(r)\neq1$，则$C_r^i\bmod2(1\leqslant i\leqslant r-1)$不全为零。事实上，若$C_r^i=0\bmod2(1\leqslant i\leqslant r-1)$，则对任意的$\beta,\gamma\in GF(2^n)$，有$(\beta\oplus\gamma)^r=\beta^r\oplus\gamma^r$，此与$w(r)\neq1$矛盾。不妨设$C_r^{i_0}=1\bmod2(1\leqslant i_0\leqslant r-1)$。考虑方程(3)左边常数项和$x^{i_0}$，$x^r$的系数，有

$$\begin{cases}1\oplus a^{rk}\oplus a^{rh}=0\\1\oplus\beta^{ki_0}\alpha^{kr}\oplus\beta^{hi_0}\alpha^{hr}=0\\1\oplus\beta^{kr}\alpha^{kr}\oplus\beta^{hr}\alpha^{hr}=0\end{cases}$$

由于$1,a^{kr},a^{hr}$不全为零,故

$$\begin{vmatrix}1 & 1 & 1\\ 1 & \beta^{ki_0} & \beta^{hi_0}\\ 1 & \beta^{kr} & \beta^{hr}\end{vmatrix}=0$$

所以,存在不全为零的数$c_1,c_2,c_3\in GF(2)$,使得

$$c_1\begin{pmatrix}1\\1\\1\end{pmatrix}\oplus c_2\begin{pmatrix}1\\ \beta^{ki_0}\\ \beta^{kr}\end{pmatrix}\oplus c_3\begin{pmatrix}1\\ \beta^{hi_0}\\ \beta^{hr}\end{pmatrix}=\begin{pmatrix}c_1\oplus c_2\oplus c_3\\ c_1\oplus c_2\beta^{ki_0}\oplus c_3\beta^{hi_0}\\ c_1\oplus c_2\beta^{kr}\oplus c_3\beta^{hr}\end{pmatrix}=\mathbf{0}$$

由第一行为零可知:c_1,c_2,c_3中必有两个为1,一个为零。由第三行可得

$$(\beta^{kr}\oplus 1)(\beta^{hr}\oplus 1)(\beta^{kr}\oplus\beta^{hr})=0$$

若$\beta^{kr}=1$,即$(\alpha^{kr})^{2^m-1}=1$,所以$\alpha^{kr}\in GF(2^m)$,又$\gcd(r,2^m-1)=1$,所以r在Z_{2^m}中有乘法逆元,故$\alpha^k\in GF(2^m)$,从而$k=0 \bmod M$,再由引理1知:$h=0 \bmod M$。

同理可证,当$\beta^{kr}=1$时,也有$k=h=0 \bmod M$。

若$\beta^{kr}\neq 1$且$\beta^{hr}\neq 1$,则必有$\beta^{kr}=\beta^{hr}$,即$\alpha^{(2^m-1)kr}=\alpha^{(2^m-1)hr}$,或写为$(\alpha^{(h-k)r})^{(2^m-1)}=1$,所以$\alpha^{(h-k)r}\in GF(2^m)$,等价于$\alpha^{h-k}\in GF(2^m)$,从而$M|(h-k)$。记$h=k+i_1M$,由于$\alpha^{Mr}$是$GF(2^m)$的本原元,故存在的$i_2$,使得$1\oplus\alpha^{i_1Mr}=\alpha^{i_2Mr}$,所以

$$[Tr_m^n(\alpha^{j+k})]^r\oplus[Tr_m^n(\alpha^{j+h})]^r=[Tr_m^n(\alpha^{j+k})]^r\oplus[Tr_m^n(\alpha^{j+k+i_1M})]^r=$$

$$(1\oplus\alpha^{i_1Mr})[Tr_m^n(\alpha^{j+k})]^r=\alpha^{i_2Mr}[Tr_m^n(\alpha^{j+k})]^r=[Tr_m^n(\alpha^{j+k+i_2M})]^r \quad (4)$$

根据定理1:式(4)等价于$a_{i+k}\oplus a_{i+h}\oplus a_{i+k+i_2M}=0(i\geqslant 0)$。又$\delta(k,h,j)\equiv 0(0\leqslant j<M)$等价于$a_i\oplus a_{i+k}\oplus a_{i+h}=0(i\geqslant k)$,故$a_{i+k+i_2M}=a_i(i\geqslant 0)$。所以$k+i_2M=0 \bmod P$,又$M|T$,故$k=0 \bmod M$。再由引理1知:$h=0 \bmod M$。

综合上述引理1、引理2及定理1得:

定理 3 对于GMW-序列$a_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}(i=0,1,2,\cdots)$,有

(1)对于任意的$k=0 \bmod M(0<k<T)$,都存在唯一的$h(0<h<T)$,使得$1\oplus x^k\oplus x^h$是序列$\{a_i\}_{i=0}^{\infty}$的生成多项式,且$k_2=0 \bmod M(k_2\neq k_1)$;

(2)当$m\notin\{1,n\}$,且$w(r)\neq 1$(非m-序列)时,若$1\oplus x^k\oplus x^h$是序列$\{a_i\}_{i=0}^{\infty}$的生成多项式,则必有$k=h=0 \bmod M$。

由定理3容易得出:

推论 1 除m-序列外,任一GMW-序列的次数小于周期T的三项生成多项式能且仅能写成$1\oplus x^{i_1M}\oplus x^{i_2M}(1\leqslant i_1<i_2<2^m-1)$形式。

推论 2 除m-序列外,GMW-序列的次数小于周期T的三项生成多项式共有$2^{m-1}-1$个。

证明 因为满足条件$k=0 \bmod M(0<k<T)$的k共有2^m-2个,又$1\oplus x^k\oplus x^h$与$1\oplus x^h\oplus x^k$为同一三项式,由定理3可得:GMW-序列(m-序列除外)的次数小于周期T的三项生成多项式共有$\frac{2^m-2}{2}=2^{m-1}-1$个。

3 GMW-序列的安全性分析

假设$\{a_i\}_{i=0}^{\infty}$是由$a_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}(1\leqslant r<2^m-1,\gcd(r,2^m-1)=1,r\neq 2^t(\forall t))$产生的GMW-序列,$\{b_i\}_{i=0}^{\infty}$是由$b_i=Tr_1^n(\alpha^i)$产生的$m$-序列,则$\{a_i\}_{i=0}^{\infty}$和$\{b_i\}_{i=0}^{\infty}$的周期均为$T=2^m-1$。

定理 4 GMW-序列$\{a_i\}_{i=0}^{\infty}$的三项生成多项式均为m-序列$\{b_i\}_{i=0}^{\infty}$的r-采样序列$\{b_{ri}\}_{i=0}^{\infty}$的三项生成多项式。

证明 设$1\oplus x^k\oplus x^h$是序列$\{a_i\}_{i=0}^{\infty}$三项生成多项式,由定理3知:存在$i_1,i_2(1\leqslant i_1,i_2<2^{m-1})$,使得$k=i_1M,h=i_2M$,由引理1的证明可得:$1\oplus\alpha^{i_1Mr}\oplus\alpha^{i_2Mr}=0$。故

$$b_{ri}\oplus b_{r(i+k)}\oplus b_{r(i+h)}=Tr_1^n(\alpha^{ri})\oplus Tr_1^n(\alpha^{r(i+k)})\oplus Tr_1^n(\alpha^{r(i+h)})=$$

$$Tr_1^n(\alpha^{ri}\oplus\alpha^{r(i+k)}\oplus\alpha^{r(i+h)})=Tr_1^n[(1\oplus\alpha^{i_1Mr}\oplus\alpha^{i_2Mr})\alpha^{ri}]=0$$

即$1\oplus x^k\oplus x^h$是序列$\{b_{ri}\}_{i=0}^{\infty}$的三项生成多项式。

特别地,若$\gcd(r,2^n-1)=1$,则α^r也是$GF(2^n)$的本原元,所以序列$\{b_i\}_{i=0}^{\infty}$的r-采样序列$b_{ri}=Tr_1^n(\alpha^{ri})(i=0,1,\cdots)$也是周期为$2^n-1$的$m$-序列[12],这时,$\{a_i\}_{i=0}^{\infty}$的三项生成多项式均为某一同周期$m$-序列的三项生成多项式。

定理 5 GMW-序列(m-序列除外)的三项生成多项式的个数小于同周期m-序列的$\frac{1}{M}$,其中,$M=\frac{2^n-1}{2^m-1}$。

证明 由定理3的推论2知,GMW-序列(m-序列除外)的三项生成多项式的个数为$2^{m-1}-1$,当$m=n$时,$\{a_i\}_{i=0}^{\infty}$是m-序列,由定理3(1)可得:m-序列的三项生成多项式的个数为$2^{n-1}-1$,所以有$\frac{2^{m-1}-1}{2^{n-1}-1}>\frac{2^m-1}{2^n-1}=\frac{1}{M}$。

定理 6 记$d=\min\{h|1\oplus x^k\oplus x^h(1\leqslant k<h<T)\}$是GMW-序列($m$-序列除外)的生成多项式},则当$M=2$时,$d=2M$;当$m>2$时,$d\geqslant 3M$。

证明 当$m=2$时,α^{Mr}是$GF(2^2)$的生成元,故必有$1\oplus\alpha^M\oplus\alpha^{2M}=0$,故由引理1的证明知:$1\oplus x^M\oplus x^{2M}$是次数最低的$\{a_i\}_{i=0}^{\infty}$的三项生成多项式,故$d=2M$。

当$m>2$时,设$1\oplus x^{i_1M}\oplus x^{i_2M}\in H_a(1\leqslant i_1<i_2<2^m-1)$,如果$i_2=2$,则$i_1=1$,$1\oplus\alpha^{Mr}\oplus\alpha^{2Mr}=0$,则

$$(1\oplus\alpha^{Mr}\oplus\alpha^{2Mr})^2=1\oplus\alpha^{2Mr}\oplus\alpha^{4Mr}=0$$

所以$\alpha^{Mr}=\alpha^{4Mr}$,从而$(2^n-1)|3M$,故$m=2$,矛盾。故当$m>2$时,GMW-序列的三项生成多项式的次数不低于$3M$,即$d\geqslant 3M$。

定理5和定理4说明:GMW-序列的三项生成多项式不仅远比m-序列的三项生成多项式少,而且GMW-序列的三项生成多项式都是某一m-序列的生成多项式。这意味着GMW-序列在抵抗快速相关攻击方面比m-序列具有更高的安全性。

由于增加序列的三项生成多项式的次数,可以有效阻止快速相关攻击。所以,构造GMW-序列时,在n一定的条件下,应选择n的较小的因子作为m,这样可使$M=\frac{2^n-1}{2^m-1}$较大,由定理6,GMW-序列的三项生成多项式的最低次数也比较大;但

(下转132页)