一种新的 GF(q)上的广义自缩生成器

高军涛 胡予濮 董丽华

(西安电子科技大学 计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要：设计了一种新的 GF(q)上的广义自缩生成器，该生成器的主要特点在于输出方式不同于原生成器。研究表明生成的大序列族有良好的互相关性、均衡性，并且给出了最小周期的下界。同时也指出该序列有丰富的群结构和线性空间结构。

关键词：保密通信，广义自缩序列，线性复杂度，互相关性

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2005)07-1127-04

A New Generalized Self-shrinking Generator on GF(q)

Gao Jun-tao Hu Yu-pu Dong Li-hua

(*Computer Networking and Information Security Key Lab., Xidian University, Xi'an* 710071, *China*)

Abstract A new q-ary generalized self-shrinking generator is presented. The main difference between the new generator and the old one is the output mode. It is shown that there is good correlation between sequences in the large sequence family, and sequences are balanced in a least period. Simultaneously, the lower bounds of the least period are provided, and the family of sequences takes on a rich group structure and linear space structure.

Key words Privacy communication, Generalized self-shrinking sequences, Linear complexity, Correlation

1 引言

序列密码中需要的是有良好性质的密钥流，即具有以下几个性质：(1)大的周期；(2)均衡性质；(3)良好的游程分布性质；(4)良好的相关性质；(5)大的线性复杂度及好的线性复杂度轮廓。根据上面的这些性质，人们提出了不同的流密码体制。其中 Coppersmith，Krawczyk 和 Mansor 提出了互缩序列生成器[1]，该生成器是由两个线性反馈移位寄存器(LFSR1 和 LFSR2)通过简单的方式组合而成的：LFSR2 当前的输出比特是 1 时，LFSR1 输出对应比特；否则 LFSR1 不输出。可以看出互缩序列生成器的结构是比较简单的。

Meier 和 Staffelbach 提出了自缩生成器[2]。这种生成器具有更为简单的结构：只有一个 LFSR，可以应用于任何由 LFSR 生成的序列。假定初始序列为

$$a=(a_0,a_1,a_2,\cdots)=((a_0,a_1),(a_2,a_3),\cdots)$$

如果任何一组比特对：(a_{2i},a_{2i+1})=(1,0)或(1,1)，LFSR 就输出 0 或 1；其它的情况 LFSR 不输出。自缩生成器和互缩生成器的结构是很简单的，但实现并不简单。同时针对这两种序列生成器的攻击已经出现[3-5]。

胡予濮和肖国镇提出了 GF(2)上的广义自缩序列[6]，该序列包含了自缩序列和互缩序列的一些优点，同时比自缩序列和互缩序列更加安全。除此以外，广义自缩序列族还具有群结构和线性空间结构。在文献[7]中胡予濮等提出了一类 q 元广义自缩序列，该类序列同样具有上述 GF(2)上的一些良好的性质。

本篇文章提出了一类新的 GF(q)上的广义自缩生成器，生成的序列具有大的周期，高的线性复杂度和良好的互相关性质。而且在作为密钥流方面，我们引入了两个参数使得安全性得到进一步提高，这点是原来的序列生成器所没有的。本文结构如下：第 2 节给出了基本定义和一些理论基础；第 3 节讨论该类序列的周期和线性复杂度；第 4 节分析了它的代数性质，互相关性质和均衡性质；第 5 节进行了总结全文，并给出一些设计建议。

2 定义和基础知识

在本文中，总认为 $q=p^m$，p 为一素数，$m\geq 1$ 为一正整数。下面看一个定义，它是我们要提出的新类型生成器的一个特例：

定义 1 设 $a=(\cdots a_{-2},a_{-1},a_0,a_1,a_2,\cdots)$ 是 GF(q)上的 n 级 m 序列，$G=(g_0,g_1\cdots g_{n-1})\in \mathrm{GF}(q)^n$，序列 $v=\cdots v_{-2}v_{-1}v_0v_1v_2\cdots$，其中

$$v_j=g_0a_j+g_1a_{j-1}+\cdots+g_{n-1}a_{j-n+1},\ j=0,1,2,\cdots$$

任意选择两个非零的 GF(q)中的元素 x_0 和 x_1，如果 $a_j=x_0$ 或 x_1，则输出 v_j；否则不输出，这样得到序列 $b_2(G)=b_0b_1b_2\cdots$，称 $b_2(G)$ 为 GF(q)二值输出广义自缩序列。

2004-02-23 收到，2004-12-01 改回
国家自然科学基金(60273084)和高等学校博士点基金(20020701013)资助课题

参照定义 1，我们定义本文研究的对象为 k 值输出广义自缩序列。

定义 2 设 $a=(\cdots a_{-2},a_{-1},a_0,a_1,a_2,\cdots)$ 是 GF(q)上的 n 级 m 序列，$G=(g_0,g_1,\cdots,g_{n-1})\in \mathrm{GF}(q)^n$，序列 $v=\cdots v_{-2}v_{-1}\cdot v_0v_1v_2$，其中

$$v_l=g_0a_l+g_1a_{l-1}+\cdots+g_{n-1}a_{j-n+1},\ j=0,1,2,\cdots$$

任意选择 k (k=2,3,⋯,q-1)个非零的 GF(q)中的元素 $x_0,x_1,\cdots,x_{k-1}$，如果 $a_j=x_i$ (i=0,1,⋯,$k-1$)，则输出 v_j；否则放弃输出。这样输出的序列记为 $b_k(G)$ 或 $b_k(v)$。称 $b_k(G)$ 为 GF(q) 上的 k 值的广义自缩序列。称 $B_k(a)=\{b(G),G\in \mathrm{GF}(q)^n\}$ 为 GF(q)上的基于 m 序列 a 的 k 值的广义自缩序列族。

下一部分将证明该类序列有良好的伪随机性质。同时可以选择一个公钥体制，使得加密算法更为安全。下面我们先来看两个关于 m 序列平凡的引理。

引理 1 设 $a=(\cdots a_{-2},a_{-1},a_0,a_1,a_2,\cdots)$ 是 GF(q)上周期为 q^n-1 的 m 序列，$\overline{a_i}=(a_i+a_{i+1},\cdots,a_{i+n-1})$，则 $\overline{a_i}$ 跑遍了 $GF(q)^n$ 上的 q^n-1 个向量。一个出现一次。

引理 2 设 $a=(\cdots a_{-2},a_{-1},a_0,a_1,a_2,\cdots)$ 是 GF(q)上周期为 q^n-1 的 m 序列，对任意 $x\neq 0$，在一个最小周期内有一个长为 n 的 x 游程；有 q-2 个长为 n-1 的 x 游程；有 $(q-1)\left(q^{i-1}-q^{i-2}\right)$ 个长为 $n-i$ 的 x 游程(i=2,3,⋯,$n-1$)。因此在每个最小周期内每个非零 x 出现 q^{i-1} 次，0 出现 $q^{i-1}-1$ 次。

3 周期和线性复杂度

首先来看周期，引理证明采用如下思想：(1)某些特定的符号串在一个周期内仅出现一次；(2)一个周期内某些符号串中的符号和的个数不能整除周期。两种情况出现任何一种则说明该周期即为最小周期。

为证明引理 3，从现在开始，除了定义 1 中的 x_0,x_1，总是把 GF(q)中任何一个其它的元素记为“*”，即使他们不相等。例如：$x_2,x_3\in \mathrm{GF}(q)$，$x_2\neq x_3$ 且 x_2,x_3 不为 x_0,x_1 中的任何一个，我们把 x_2,x_3 都记为“*”。

序列 v 的最小周期记为 $p(v)$。下面的引理给定了二值输出广义自缩序列的最小周期情况：

引理 3 设 $v(i)=\cdots v_{-2}^{(i)}v_{-1}^{(i)}v_0^{(i)}v_1^{(i)}v_2^{(i)}\cdots$ (i=1~3)是 3 个序列，由以下的方式生成：

$$v_j^{(1)}=a_{j-1};\ \ v_j^{(2)}=a_{j+1};\ \ v_j^{(3)}=xa_{j-1}+ya_{j+1};$$

$$x\in \mathrm{GF}(q),\ y\in \mathrm{GF}(q),\ x\neq 0,\ y\neq 0;$$

当 $a_j=x_i(i=0,1)$ 时，输出 v_j；否则不输出。j=0,1,2,⋯。则我们得到：$p(bv^{(3)})\geq 2q^{n-2}$；

在情况(1)，(2)，(3)下，$p(b(v^{(1)}))=2q^{n-1}$；在情况(4)下，$p(b(v^{(1)}))\geq q^{n-1}$；

证明 首先来看 $p(b(v^{(1)}))$，由生成方式可知：$2q^{n-1}$ 是序列 $b(v^{(1)})$ 的周期。因此，序列 $b(v^{(1)})$ 的最小周期是 $2q^{n-1}$ 的因子。由引理 2，长度为 n 的 $*x_0x_0\cdots x_0*(*\neq x_0)$ 和 $*x_1x_1\cdots x_1*(*\neq x_1)$游程在 m 序列 a 的一个最小周期里面只有一个。根据这两个最长游程后面的元素的不同可以分成以下 4 种情况：

情况(1) $*x_0x_0\cdots x_0x_1*$ 和 $*x_1x_1\cdots x_1x_0$；

情况(2) $*x_0x_0\cdots x_0x_1$ 和 $*x_1x_1\cdots x_1*$；

情况(3) $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1x_0$；

情况(4) $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$。

在情况(1)下，长度为 n 的 $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$ 游程在 $b(v^{(1)})$ 中只出现一次；

在情况(2)下，长度为 n 的 $*x_0x_0\cdots x_0*$ 游程在 $b(v^{(1)})$ 中只出现一次；

在情况(3)下，长度为 n 的 $*x_1x_1\cdots x_1*$ 游程在 $b(v^{(1)})$ 中只出现一次。

所以在情况(1)，(2)，(3)下，$p(b(v^{(1)}))=2q^{n-1}$；

在情况(4)下，由所定义的生成方式得到：

$n-1$ 长的 $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$ 游程在序列 $b(v^{(1)})$ 的一个最小周期中各出现 2 次。(一个由 m 序列 a 中 n 长游程生成，另一个由 m 序列 a 中 $n-1$ 长的游程生成)；因此，在情况(4)时，$p(b(v^{(1)}))\geq q^{n-1}$。同时注意到下面的情况：

$n-2$ 长的 $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$ 在序列 $b(v^{(1)})$ 的一个最小周期中各出现 $2(q-2)$次。($q-3$ 个由 m 序列 a 中 $n-1$ 长游程生成，$q-1$ 个由 m 序列 a 中 $n-2$ 长游程生成)；

$n-3$ 长的 $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$ 在序列 $b(v^{(1)})$ 的一个最小周期中各出现 $2(q-1)(q-1)$次。($(q-2)(q-1)$个由 m 序列 a 中 $n-2$ 长游程生成，$q(q-1)$由 $n-3$ 长游程生成)；

⋮ ⋮

$n-i$ 长的 $*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$ 在序列 $b(v^{(1)})$ 的一个最小周期中各出现 $2(q-1)(q^{i-2}-q^{i-3})$ 次。($(q-2)(q^{i-2}-q^{i-3})$ 个由 m-序列 a 中 $n-i$ 长的游程生成，$(q^{i-1}-q^{i-2})$ 个由 m 序列 a 中 $n-i-1$ 长的游程生成)。

由此可以看出生成的序列包含了 m 序列的部分游程，由所定义的生成方式这是可以理解的。但这也提醒设计者所选择 k 值不要太接近 $q-1$，以免暴露太多的驱动序列信息。也可以看出：当 k 值选取适中的时候，生成序列中的部分游程分布是比较好的。

下面来看一下 $p(b(v^{(2)}))$，根据最长游程前面元素分成以下 4 种情况证明。

情况(1)　$x_1x_0x_0\cdots x_0*$ 和 $x_0x_1x_1\cdots x_1*$；

情况(2)　$x_1x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$；

情况(3)　$*x_{00}x_0\cdots x_0*$ 和 $x_0x_1x_1\cdots x_1*$；

情况(4)　$*x_0x_0\cdots x_0*$ 和 $*x_1x_1\cdots x_1*$；

证明方法相似，在此不赘述。

最后来证明 $p(b(v^{(3)}))$：由 m 序列 a 中长度大于 3 的“$*x_0x_0\cdots x_0*$”游程生成的游程为“$*(x+y)x_0,(x+y)x_0,\cdots,(x+y)x_0*$”($*\neq(x+y)x_0$)；长度为 2 的游程 $*x_0x_0*$，生成“$**$”($*\neq(x+y)x_0$)。

因此以 m 序列 a 中长度大于 3 的“$*x_0x_0\cdots x_0*$”游程生成的长度为 $n-2$ 的“$*(x+y)x_0,(x+y)x_0,\cdots,(x+y)x_0*$”($*\neq(x+y)x_0$)游程有 1 个；长度为 $n-3$ 的有 $q-2$ 个；长度为 $n-i-2$ 的游程有 $(q-1)(q^{i-1}-q^{i-2})$ 个，$i=2,3,\cdots,n-3$。所有的这些游程长度之和为 $(q-1)(q^{n-3}-1)$，该数目不能整除 $2q^{n-2}$，符合证明思想中的第(2)条。对于长度大于 3 的“$*x_1x_1\cdots x_1*$”游程情况是相似的。因此得到 $p(b(v^{(3)}))\geq 2q^{n-2}$。　　证毕

注：在 $p(b(v^{(3)}))$ 的证明过程中，注意到 m 序列中还有其他的游程也可以生成“$*(x+y)x_0,(x+y)x_0,\cdots,(x+y)x_0*$”($*\neq(x+y)x_0$)形式的游程，在此我们没有考虑这种情况，这是因为在我们仅仅考虑由引理中所述的情况下生成的这种游程的长度之和已经非常地逼近 $2q^{n-2}$，对于证明该结论已经足够了。

由引理 3 可以得到下面的定理。

定理 1　设 $v(i)=\cdots v_{-2}^{(i)}v_{-1}^{(i)}v_0^{(i)}v_1^{(i)}v_2^{(i)}\cdots(i=1\sim 3)$ 是按照定义 2 方式生成的 3 个序列：具体生成规则如下：$v_j^{(1)}=a_{j-1};v_j^{(2)}=a_{j+1};v_j^{(3)}=xa_{j-1}+ya_{j+1}$：$x\in GF(q)$，$y\in GF(q)$，$x\neq 0,y\neq 0$。当 $a_j=x_i(i=0,1,2\cdots,k-1)$ 时输出 v_j；否则不输出 j=0,1,2,…。则 $p(b(v^{(3)}))\geq kq^{n-2}$；

在情况 (1)~(k^k-1) 下，$p(b(v^{(1)}))\geq kq^{n-1}$，在情况 (k^k) 下，$p(bv^{(1)})\geq q^{n-1}$；

在情况 $(1)'\sim(k^k-1)'$ 下，$p(b(v^{(2)}))=kq^{n-1}$；在情况 $(k^k)'$ 下，$p(b(v^{(2)}))\geq q^{n-1}$。

证明　m 序列 a 中会出现下面的情况：

“$*x_0x_0\cdots x_0*$ 且 $*x_1x_1\cdots x_1*$ 且……，且

$*x_{k-1}x_{k-1}\cdots x_{k-1}*$”，$*\neq x_i,i=0,1,\cdots k-1$。　　(*)

参考引理 3，对于 $p(b(v^{(1)}))$ 可知除情况(*)以外，其它的情况下生成序列 $b(v^{(1)})$ 的最小周期 $p(b(v^{(1)}))=kq^{n-1}$。

在序列 $b(v^{(1)})$ 中，对每一个 x_i (i=0,1,…, $k-1$)，有 k 个长度为 $n-1$ 的“$x_ix_i\cdots x_i$”游程，$k(q-2)$个长度为 $n-2$ 的“$x_ix_i\cdots x_i$”游程。……，$k(q-1)(q^{i-2}-q^{i-3})$ 个长度为 $n-i(i=3,4\cdots n-1)$的“$x_ix_i\cdots x_i$”游程。因此能得到在情况(*)下：$p(b(v^{(1)}))\geq q^{n-1}$。

$p(b(v^{(2)}))$ 证法相同；同样根据引理 3 的证法可以得到 $p(b(v^{(3)}))\geq kq^{n-2}$。　　证毕

推论 1　根据定理 1 输出的序列，$p(b(v^{(1)}))=p(b(v^{(2)}))=kq^{n-1}$ 的概率为 $1-\left(\frac{q-k}{q-1}\right)^k$；$p(b(v^{(1)}))=p(b(v^{(2)}))\geq q^{n-1}$ 的概率为 $\left(\frac{q-k}{q-1}\right)^k$；$p(b(v^{(3)}))\geq kq^{n-2}$ 的概率为 1。

该推论可以由定理 1 分析的情况得到。从推论可知 k 取值越大，输出长周期序列的概率就越大；但是注意另外一个因素，就是 k 太大时会暴露原来驱动序列的部分游程，这是非常危险的，所以并非 k 值取得越大就越好，而是要取适中的值。

引理 4　对于 GF(q)上周期 $P(v)=kq^r$ 的序列 v，其线性复杂度 $LC(v)>q^{r-1}$，其中，p 为域 GF(q)的特征，$k\in Z^+$。

证明　设 $f(x)$ 是序列 v 的最小多项式，则 $f(x)|(1-x^{kq^r})$，即：$f(x)|(1-x^k)^{q^r}$；而 $1-x^k=(1-x)(1+x+\cdots+x^k)$，所以有：$f(x)|(1-x)^{q^r}(1+x+\cdots x^{k-1})^{q^r}$；

因而 $f(x)=(1-x)^i(1+x+\cdots x^{k-1})^j$，其中 $i,j\leq q^r$，若 $i\leq q^{r-1}$ 且 $j\leq q^{r-1}$，则 $f(x)|(1-x)^{q^{r-1}}(1+x+\cdots x^{k-1})^{q^{r-1}}$；说明序列 v 的周期可以为 kq^{r-1}，这与假设矛盾，所以 i,j 不能同时小于等于 q^{r-1}。所以 $LC(v)>q^{r-1}$。　　证毕

所以可以知道以上生成的 3 种序列的线性复杂度是比较高的。

4　群结构和相关性

定理 2　序列族 $B_k(a)=\{b(G),\ G\in GF(q)^r\}$ 是一个 Abel 群，单位元为 000…；$B_k(a)$ 也是一个 n 维线性空间，$|B_k(a)|=q^r$。

证明　对于任意 $G_1\in GF(q)^r,G_2\in GF(q)^r$，$x\in GF(q)$，$y\in GF(q)$ 有：$xb(G_1)+yb(G_2)=b(xG_1+yG_2)$；$b(G_1)\neq b(G_2)$ 当且仅当 $G_1\neq G_2$。因此，$B_k(a)$ 和 $GF(q)^n$ 同构。　　证毕

对于一个固定的 $b(G)=b_0b_1b_2\cdots\in B_k(a)$，称 $b^*(G)=\{(xb_0)(xb_1)\cdots,x\in GF(q)\}$ 为 $b(G)$ 的同调序列族；称 $b^{**}(G)=\{(x-b_0)(x-b_1)\cdots,x\in GF(q)\}$ 为序列 $b(G)$ 的补序列集，则 $b^*(G)\subset B_k(a)$，$b^{**}(G)\subset B_k(a)$；$b^*(G)$ 也可以称之为 $b(G)$ 的同调序列，$b^{**}(G)$ 也可称之为 $b(G)$ 的补序列。

定理 3 设两个固定的序列：$b^{(1)} \in B_k(a)$，$b^{(2)} \in B_k(a)$，$b^{(1)}$ 与 $b^{(2)}$ 互相不为同调序列和补序列，且 $b^{(1)}$ 与 $b^{(2)}$ 也不是 111…的同调序列，记：

$C(x,y)=\#\{j:0\le j\le kq^{n-1}-1, b_j^{(1)}=x, b_j^{(2)}=y\}$，$x\in \mathrm{GF}(q)$，$y\in \mathrm{GF}(q)$，则 $C(x,y)=kq^{n-3}$。

证明 设 $b^{(1)}=b(G^{(1)})$，它的驱动序列为 m-序列 a，$G^{(1)}=(g_0^{(1)},g_1^{(1)},\cdots,g_{n-1}^{(1)})$，并且

$$v^{(1)}=\cdots v_{-2}^{(1)}v_{-1}^{(1)}v_0^{(1)}v_1^{(1)}v_2^{(1)}\cdots,$$

$$(v_j^{(1)}=g_0^{(1)}a_j+g_1^{(1)}a_{j-1}+\cdots+g_{n-1}^{(1)}a_{j-n+1})$$

设 $b^{(2)}=b(G^{(2)})$，它的驱动序列也为 m 序列 a，$G^{(2)}=(g_0^{(2)},g_1^{(2)}\cdots g_{n-1}^{(2)})$，同样

$$v^{(2)}=\cdots v_{-2}^{(2)}v_{-1}^{(2)}v_0^{(2)}v_1^{(2)}v_2^{(2)}\cdots,$$

$$(v_j^{(2)}=g_0^{(2)}a_j+g_1^{(2)}a_{j-1}+\cdots+g_{n-1}^{(2)}a_{j-n+1})$$

根据定义 2 和引理 2，我们知道 $G^{(1)}$，$G^{(2)}$ 和 $(1,0,\cdots,0)$ 是线性独立的，取任意一个固定的 $x\in \mathrm{GF}(q)$，当 j 跑遍 $[0,q^n-1]$ 使每个 $(a_j,v_j^{(1)})=(x_i,x)$，$(i=0,1,\cdots,k-1)$ 出现 q^{n-2} 次时，$v_j^{(2)}$ 跑遍所有的 $y\in \mathrm{GF}(q)$，每个 y 出现 q^{n-3} 次。

证毕

从该推论可以看出该类序列在族内有良好的互相关性质。

定理 4 (1) $b(G)=000\cdots$，当且仅当 $G=(0,0,\cdots 0)$；(2) $G=(y,0,\cdots 0)$，$(y\in \mathrm{GF}(q))$，$b(G)$ 的元素只能是以下形式：$yx_i\in \mathrm{GF}(q)$，$(i=0,1,\cdots,k-1)$；(3) 对于其他的 G，$b(G)$ 在连续的 kq^{n-1} 个输出元素中是均衡的。

证明 (1)是平凡的；(2)中的 G 所形成的元素：$yx_i\in \mathrm{GF}(q)$，$(i=0,1,\cdots,k-1)$，仅仅是 $\mathrm{GF}(q)$中的一部分。由引理 2 知道其中每个元素在一个周期中出现的次数是相等的，即 $\mathrm{GF}(q)$中部分元素在所生成的序列中是均衡的；(3)由所定义的序列的线性性即得。

证毕

5 结束语

本文提出的 $\mathrm{GF}(q)$上的广义自缩序列生成器与文献[7]中的相比主要有以下的特点：

(1) 新生成器和原生成器都具有生成简洁的特点；

(2)新序列的最小周期更大，线性复杂度有较大的下界。同时在证明的过程中，给出了部分游程的分布情况，表明部分游程的分布是较好的；

(3)本文提出的序列生成器比原生成器增加了两个参数：k 和 $\{x_i\}$ $(i=0,1,\cdots,k-1)$，通信双方可以通过安全信道来传输这两个参数，任何第三方在没有得到这两个参数的情况下破解密文的困难程度会显著增加；

(4)该类序列与原来的广义自缩序列相比具有更加丰富的代数结构；同时由于两个参数 k 和 $\{x_i\}$ $(i=0,1,\cdots,k-1)$的加入使得在生成序列时选择自由度更大。

(5)可以生成互相关性质良好的大序列族。

同时注意到仍有一些问题没有解决，诸如：游程分布总体分析、最小周期的细化分析、两个参数 k 和 $\{x_i\}$ $(i=0,1,\cdots,k-1)$选择不同时，序列之间的互相关性质等等，这些都值得做进一步详细的研究。对于目前存在的攻击，如文献[3－5]中提出的针对缩减序列的攻击，是否对广义自缩序列有效，也是我们将要分析的一个重要的方面。

参 考 文 献

[1] Coppersmith D, krawczy H, Mansour Y. The shrinking generator[C]. in Advance in Cryptology-CRYPTO'93, Berlin Germany: Springer-Verlag, 1994: 22－38.

[2] Meier W, Stafflebach O. The self-shrinking generator[C]. Advanced in Cryptology-Eurocrypt'94. Berlin: Springer-Verlag, 1995: 205－214.

[3] Mihalievic M J. A faster cryptanalysis of the self-shrinking generator. in Proceedings of ACIPS'96, Berlin: Springer-Verlag, 1996, LNCS 1172: 182－189.

[4] Zenner E, Krause M, Lucks S. Improved cryptanalysis of the self-shrinking generator. in Proceedings of ACIPS'2001, Berlin: Springer-Verlag, 2002, LNCS 2119: 21－35.

[5] Krause M. BDD-based cryptanalysis of keystream generators[C]. in Advanced in Cryptology-Eurocrypt'02, L.R.Knudsen (Ed), Springer-Verlag, 2002, LNCS 2332: 222－237.

[6] Hu Yu-pu, Xiao Guo-zhen. The generalized self-shrinking generator[J]. *IEEE Trans. on Information Theory*, 2004, 50(4): 714－718.

[7] 胡予濮, 白国强, 肖国镇. GF(q) 上的广义自缩序列[J]. 西安电子科技大学学报, 2001, 28(1): 5－7.

高军涛: 男，1979 年生，博士生，研究方向为信息安全、序列密码.

胡予濮: 男，1955 年生，教授，博士生导师，主要研究方向为信息安全和网络安全.

董丽华: 女，1977 年生，博士生，研究方向为信息安全、序列密码.