第 26 卷第 11 期 电 子 与 信 息 学 报 Vol.26No.11
2004 年 11 月 Journal of Electronics & Information Technology Nov. 2004

广义自缩序列的一种比较快速的密码学分析方法 [1]

董丽华 * ** 曾 勇 ** 胡予濮 * **

*(西安电子科技大学 ISN 国家重点实验室 西安 710071)
**(西安电子科技大学 CNIS 教育部重点实验室 西安 710071)

摘 要: 对广义自缩序列生成器，利用猜测攻击的思想给出了一种比较快速的初态重构算法. 得到了: (1) 当线性反馈移位寄存器 (LFSR) 的特征多项式与线性组合器均已知时，算法的复杂度为 $O((L/2)^3 2^{L-2)})$, $l \le L/2$; (2) 当线性组合器未知时，算法的复杂度为 $O(L^3 2^{2L-l})$, $l \le L$; (3) 当 LFSR 的特征多项式未知时，算法的复杂度为 $O(\varphi(2L-1)L^{-1}2^{2L-l})$, $l \le L$. 其中 L 为 LFSR 的长度, φ 为欧拉函数.

关键词: 广义自缩序列, m 序列, 密码学分析
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 1009-5896(2004)11-1783-04

A Fast Cryptanalysis of the Generalized Self-shrinking Sequences

Dong Li-hua* ** Zeng Yong** Hu Yu-pu* **

*(*ISN National Key Lab., Xidian University, Xi'an* 710071, *China*)

**(*CNIS Key Lab., Ministry of Education, Xidian University, Xi'an* 710071, *China*)

Abstract An initial reconstruction algorithm is given for the generalized self-shrinking sequences using the ideas of the guessing attack. The result shows that: (1) when both the characteristic polynomial of the Linear Feedback Shift Register (LFSR) and the linear combiner are known, the algorithm ensures the cryptanalysis with complexity $O((L/2)^3 2^{L-l})$ $l \le L/2$; (2) when the linear combiner is unknown, the algorithm ensures the cryptanalysis with complexity $O(L^3 2^{2L-l})$, $l \le L$; (3) When the characteristic polynomial of the LFSR is unknown, the algorithm ensures the cryptanalysis with complexity $O(\varphi(2L-1)L^{-1}2^{2L-l})$, $l \le L$. Here L is the length of the LFSR, φ is the Euler's totient function.

Key words Generalized self-shrinking sequences, m sequence, Cryptanalysis

1 引言

广义自缩序列是一种新型的序列密码体制，其核心思想是使用 m 序列对它的一个平移序列进行不规则钟控，定义如下:

定义 1[1] 设 $a = a_0 a_1 a_2 \cdots$ 是 GF(2) 上的 n 级 m 序列，另设 GF(2) 上的 n 维向量 $\boldsymbol{G} = [g_0 \ g_1 \ \cdots \ g_{n-1}]$, 定义序列 $v = v_0 v_1 v_2 \cdots$ 使得 $v_k = g_0 a_k + g_1 a_{k-1} + \cdots + g_{n-1} a_{k-n+1}$, 对于 $k = 0, 1, 2, \cdots$, 如 $a_k = 1$, 则输出 v_k , 否则放弃输出. 如此得到的输出序列 $b = b_0 b_1 b_2 \cdots$, 记为 $b(v)$ 或 $b(\boldsymbol{G})$, 称其为基于 m 序列 a 的广义自缩序列.

以下称 m 序列 a 为控制序列，称其平移序列 v 为被控序列，且设其平移距离为 u , 即 $v = a_u a_{u+1} a_{u+2} \cdots$. 另设 a 的最小周期为 $2^L - 1$, 极小多项式为 $f(x) = x^L + c_{L-1} x^{L-1} + \cdots +$

[1] 2003-05-18 收到, 2003-09-30 改回
国家自然科学基金 (60273084) 和高等学校博士点科研专项基金 (20020701013) 资助项目

c_1x+1，则 m 序列 a 满足线性递归关系式 $a_t=c_1a_{t-1}+c_2a_{t-2}+\cdots+c_{L-1}a_{t-L+1}+a_{t-L}$，$t=0,1,2,\cdots$.

2 算法分析

钟控移位寄存器密码学分析的一般概念最初出现在文献 [2,3] 中，但是由于它们没有考虑到自钟控这一事实，因而不适于对广义自缩序列族这类自钟控序列进行安全性分析.

在文献 [4] 中，我们曾经利用二叉树的思想对广义自缩序列生成器的安全性进行了讨论，结果表明该方法只对广义自缩序列生成器中被控序列的平移距离小于 L 的情形造成了威胁.

本文利用猜测攻击的思想对广义自缩序列生成器，给出了一种比较快速的初态重构算法，算法的基本思想是：首先猜测线性反馈移位寄存器 (LFSR) 的可能初始状态，其次求解相应参数的线性方程组，确定所需参数，最后进行验证. 在进行猜测攻击的过程中利用类似于文献 [5] 中所给出的对自缩序列的安全性进行讨论的概率方法，缩减需要测试的假设集的规模.

2.1 LFSR 的特征多项式和线性组合器均已知

在此条件下，广义自缩序列生成器的密钥由 LFSR 的初始状态唯一确定.

设二进制 m 序列 $a=\{a_m\}_{m=0}^{M-1}$ 与其平移序列 $v=\{a_{m+u}\}_{m=0}^{M-1}$ 为 L 长 LFSR 的输出 (为简化讨论，设 L 为偶数，即 $L=2n$)，另设已知广义自缩序列生成器的 $N(N<M)$ 长输出比特为 $b=\{b_n\}_{n=0}^{N-1}$.

设 n 维二进制向量 $\boldsymbol{A}_k=[a_{nk}\ a_{nk+1}\ \cdots\ a_{nk+n-1}]$，$\boldsymbol{V}_k=[a_{nk+u}\ a_{nk+u+1}\ \cdots\ a_{nk+u+n-1}]$，使用广义自缩规则，在向量 $\boldsymbol{A}_k$ 的控制下由相应的 $\boldsymbol{V}_k$ 中删去 $n-n_k$ 个比特生成的 n_k 维二进制向量记为 $\boldsymbol{B}_k$ ($n_k<n$，但大小不定，取决于向量 $\boldsymbol{A}_k$ 中“1”的个数)，$k=0,1,\cdots,\lfloor M/n\rfloor-1$.

算法中，首先猜测向量 $\boldsymbol{A}_k$ 以及相应的 $\boldsymbol{V}_k$ 的可能值，其次由于每个 $\boldsymbol{A}_k$ 即为 LFSR 状态的一半，而该状态的另一半可以由向量 $\boldsymbol{V}_k$ 加以确定，这是由于：向量 $\boldsymbol{V}_k$ 中的每一个比特都可以利用序列 a 所满足的线性递归关系式，以与 $\boldsymbol{A}_k$ 相对应的 LFSR 的状态线性表出，而向量 $\boldsymbol{A}_k$ 的值已经确定，因而向量 $\boldsymbol{V}_k$ 中的每一个比特和与 $\boldsymbol{A}_k$ 相对应的 LFSR 的状态的另外 n 个比特参数构成了一个线性方程，一共可得到 n 个这样的线性方程，求解这 n 个线性方程可得到相应的 LFSR 的状态，求解的复杂度为 $O(n^3)$，特别地，当平移距离 $u=n$ 时，只要级联 $\boldsymbol{A}_k$ 及相应的 $\boldsymbol{V}_k$，即可得到 LFSR 的状态. 最后，使用广义自缩序列生成器的生成规则以本次猜测得到的 LFSR 的状态生成长度大于 L 的 LFSR 序列，若它与已知的生成器的输出比特相一致，则结束，输出相应的初态；否则继续.

引理 1 n 维二进制向量 $\boldsymbol{A}_k$ 和 $\boldsymbol{V}_k$ 生成相应的 n_k 长，$n_k<n$，向量 $\boldsymbol{B}_k$ 的概率等于在向量 $\boldsymbol{A}_k$ 中恰有 n_k 个“1”的概率，设 n_k 是整数随机变量 $\boldsymbol{N}_k$ 的一个实现，则 $\Pr(\boldsymbol{N}_k=n_k)=2^{-n}C_n^{n_k}$，$n_k=0,1,2,\cdots,n$.

引理 2 对于序列 $b=\{b_n\}_{n=0}^{N-1}$，在测试了 $2^n(C_n^l)^{-1}$ 个连续不重叠的 l 维片断 $\boldsymbol{B}_k, l<n$，之后，可以期望我们的假设在一种情形下是正确的.

2.2 LFSR 的特征多项式和线性组合器其中之一未知的情形

此时，取二进制 m 序列 $a=\{a_m\}_{m=0}^{M-1}$ 与其平移序列 $v=\{a_{m+u}\}_{m=0}^{M-1}$ 的 L 维二进制向量 $\boldsymbol{A}_k=[a_{Lk}\ \ a_{Lk+1}\ \cdots\ a_{Lk+L-1}]$，$\boldsymbol{V}_k=[a_{Lk+u}\ \ a_{Lk+u+1}\ \cdots\ a_{Lk+u+L-1}]$，使用广义自缩规则，在向量 $\boldsymbol{A}_k$ 的控制下由相应的 $\boldsymbol{V}_k$ 中删去 $L-l_k$ 个比特生成的 l_k 维二进制向量记为 $\boldsymbol{B}_k(l_k<L$，但大小不定，取决于向量 $\boldsymbol{A}_k$ 中“1”的个数)，$k=0,1,\cdots,\lfloor M/L\rfloor-1$.

引理 3 L 维二进制向量 $\boldsymbol{A}_k$ 与 $\boldsymbol{A}_k$ 生成相应的 l_k 长 ($l_k<L$) 向量 $\boldsymbol{B}_k$ 的概率等于在向量 $\boldsymbol{A}_k$ 中恰有 l_k 个“1”的概率，设 l_k 是整数随机变量 $\boldsymbol{L}_k$ 的一个实现，则 $\Pr(\boldsymbol{L}_k=l_k)=2^{-L}C_L^{l_k}$，$l_k=0,1,2,\cdots,L$.

引理 4　对于序列 $b=\{b_n\}_{n=0}^{N-1}$ 的一个任意的 l 维片断 B_k，$l<L$，在测试了 $2^L(C_L^l)^{-1}$ 个连续不重叠的 l 维片断之后，可以期望我们的假设在一种情形下是正确的。

2.2.1 线性组合器未知　在此条件下，广义自缩序列生成器的密钥由 LFSR 的初始状态以及线性组合器系数唯一确定. 算法中：首先猜测向量 $\boldsymbol{A}_k$ 以及相应的 $\boldsymbol{V}_k$ 的可能值；其次由于每个 $\boldsymbol{A}_k$ 即为 LFSR 的状态，所以可以使用 LFSR 生成状态 $\boldsymbol{A}_k$ 的前一状态，而向量 $\boldsymbol{V}_k$ 中的每一个比特由广义自缩序列的定义可知是以向量 $\boldsymbol{A}_k$ 以及 $\boldsymbol{A}_k$ 的前一状态中的比特为系数，以线性组合器的参数为未知数的一个线性方程，一共可得到 L 个这样的线性方程，求解这 L 个线性方程可同时得到 LFSR 的初始状态以及线性组合器的参数，求解的复杂度为 $O(L^3)$；最后，使用广义自缩序列生成器的生成规则以本次猜测得到的 LFSR 的初始状态以及线性组合器的参数生成长度大于 L 的 LFSR 序列，若它与已知的生成器的输出比特相一致，则结束，输出相应的线性组合器的参数及初态；否则继续。

2.2.2 LFSR 的特征多项式未知　在此条件下，广义自缩序列生成器的密钥由 LFSR 的初始状态以及 LFSR 的特征多项式唯一确定. 算法中：首先使用文献 [6] 中给出的算法生成所有可能的 $\varphi(2L-1)/L$ 个 L 次本原多项式 (这一步可在预计算中完成，其时间复杂度为 $O(L^3)\sim O(L^4)$)，之后对所有可能的 L 次本原多项式执行随后的操作：首先猜测向量 $\boldsymbol{A}_k$ 以及相应的 $\boldsymbol{V}_k$ 的可能值；其次由于每个 $\boldsymbol{A}_k$ 即为 LFSR 的状态，因而可以使用广义自缩序列生成器的生成规则以本次猜测得到的本原多项式和 LFSR 的状态生成长度大于 L 的 LFSR 序列，若它与已知的生成器的输出比特相一致，则结束，输出相应的本原多项式及初态；否则继续. 特别地，当广义自缩序列生成器中被控序列的平移距离 u 等于 L 时，猜测得到的向量 $\boldsymbol{A}_k$ 以及相应的 $\boldsymbol{V}_k$ 显然为 LFSR 的连续的 $2L$ 个比特，因而可直接使用 B-M 算法来恢复相应的 LFSR 的联接多项式。

3 算法

我们仅给出 LFSR 的特征多项式与线性组合器均已知时的算法 (如算法 1 所示)，而 LFSR 的特征多项式与线性组合器其中之一未知时，由第 2 节的分析，其算法只要对算法 1 稍作修改即可得到.

算法 1　(LFSR 初态重构算法)

输入：LFSR 的特征多项式，线性组合器 G，已知生成器的输出比特 $b=\{b_n\}_{n=0}^{N-1}$.

预计算：确定算法的参数值 l，$l<n$，使得 l 成为式 $\lfloor(N-n)/l\rfloor 2^{-n}C_n^l\geq 1$ 成立的最大可能值. 将 $b=\{b_n\}_{n=0}^{N-1}$ 划分成 $\lfloor(N-n)/l\rfloor$ 个 l 维连续不重叠的比特片断 B_k，$k=0,1,\cdots,\lfloor(N-n)/l\rfloor-1$.

输出：重构的初态.

步骤 1　(构造假设集合)

(1) 对 n 维向量 $\boldsymbol{A}_k$ 的 l 个未考虑过的位置，设置为 “ 1 ”，剩余的位置设置为 “ 0 ”. 若所有 C_n^l 种情形均考虑完毕，为无解，则停；否则转 (2).

(2) 将 (1) 中向量 $\boldsymbol{A}_k$ 设置为 “ 1 ” 的位置 i 的向量 $\boldsymbol{V}_k$ 的对应位置设置为 $b_{kl+i}, i=0,1,2,\cdots,l-1$, 若对于比特片断 B_k 的 $\lfloor(N-n)/l\rfloor$ 种情形均考虑完毕，为无解，则停；否则转 (3).

(3) 对在 (2) 中向量 $\boldsymbol{V}_k$ 剩余的 $n-l$ 个位置设置为前边未使用过的 “ 0 ”，“ 1 ” 组合，若所有 2^{n-l} 种情形均考虑完毕，为无解，则停；否则转步骤 2.

步骤 2　(求解) 根据步骤 1 确定的 n 维向量 $\boldsymbol{A}_k$ 与 $\boldsymbol{V}_k$ 求解线性方程组，确定 LFSR 的当前初始状态，并根据所求得的初始状态由广义自缩序列生成器生成 $L^*\geq L$ 个输出比特.

步骤 3　(验证) 如果在步骤 2 中生成的 L^* 长片断等同于 $[b_{(k+1)/l+i}]_{i=0}^{L^*-1}$，$L^*\geq L$，则我们就已经重构了初态并输出，停；否则转步骤 1.

4 讨论

对于算法的复杂度，我们容易得到如下结论：

定理 1 LFSR 的特征多项式和线性组合器均已知时，需要测试的假设集 $\#H$ 的数目的上界为 $\#H \le (L/2)^3 C_{L/2}^{l} \lfloor (N-L/2)/l \rfloor 2^{L/2-l}$，需要测试的假设集的期望数目 $\#\overline{H}$ 的上界为 $\#\overline{H} \le (L/2)^3 2^{L-l}$.

定理 2 线性组合器未知时，需测试的假设集的期望数 $\#\overline{H}$ 的上界为 $\#\overline{H} \le L^3 2^{2L-l}$.

定理 3 LFSR 的特征多项式未知时，需要测试的假设集的期望数 $\#\overline{H}$ 的上界为 $\#\overline{H} \le \varphi(2L-1)2^{2L-l} \cdot L^{-1}$.

5 结论

本文使用猜测攻击的思想并结合文献 [6] 中的概率方法对广义自缩序列提供了一种比较快速的分析方法，突破了文献 [5] 中对广义自缩序列生成器的安全性分析要求被控序列的平移距离小于 L 的限制. 但同时，由引理 2 和 4，我们注意到该方法对已知的输出序列长度有很大的限制. 因而对于广义自缩序列而言，更为切实可行的密码分析方法仍有待进一步研究。

参 考 文 献

[1] Hu Yupu, Xiao Guozhen. Generalized self-shrinking sequences. *IEEE Trans. on Inform. Theory*, 2004, 50(4): 714–719.

[2] Golic J Dj, O'Connor L. Embedding and probabilistic correlation attacks on clock-controlled shift registers. Advances in Cryptology-EUROCRYPT'94, *Lecture Notes in Computer Science*, 1995, vol.950: 230–243.

[3] Golic J Dj. Towards fast correlation attacks on irregularly clocked shift registers. Advances in Cryptology-EUROCRYPT'95, *Lecture Notes in Computer Science*, 1995, vol.921: 248–261.

[4] 董丽华，胡予濮. 广义自缩序列的安全性研究. 西安电子科技大学学报， 2003, 30(3): 81–85.

[5] Mihaljevic M J. A faster cryptanalysis of the self-shrinking generator. Proc.of ACIPS'96, Lecture Notes in Computer Science. Springer-Verlag. 1996, vol.1172: 182–189.

[6] Saxena N R, McCluskey E J. Degree-r primitive polynomial generation- $O(r^3) \sim O(kr^4)$ algorithms. www-crc.stanford.edu/crc_papers/primitive.pdf, July 29, 2000.

董丽华： 女， 1977 年生，博士生，研究方向：序列密码与分组密码的设计与分析.

曾 勇： 男， 1978 年生，博士生，研究方向：计算机网络与信息安全.

胡予濮： 男， 1955 年生，教授，博士生导师，研究方向：信息与网络安全.