现代密码学

第十三讲 m-序列的安全性

信息与软件工程学院

m-序列的安全性

- 寻找m序列的递推关系式。
  - 已知一段序列，如果知道其反馈多项式，就可以将其后的序列依次求出
  - 已知序列能否获得相应的反馈多项式(或线性递推式)呢？
    - 解方程方法——已知序列$\{a_i\}$是由**n** 级线性移存器产生的，并且知道$\{a_i\}$的连续**2n**位，可用解线性方程组的方法得到反馈多项式
    - 线性反馈移位寄存器综合解——**Berlekamp-Massey**算法

第十三讲 m-序列的安全性

- 解方程方法
- 线性反馈移位寄存器综合

例1 设序列$\underline{a}=(01111000\ldots)$是由4级线性移存器所产生序列的连续8个信号，求该移存器的线性递推式。

解：设该4级移存器的线性递推式为：

$$\boxed{a_n = c_1 a_{n-1} \oplus c_2 a_{n-2} \oplus c_3 a_{n-3} \oplus c_4 a_{n-4} \quad (n \geq 4)}$$

由于知道周期序列的连续8个信号，不妨设为开头的8个信号，即

$$a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 = 01111000$$

当n=4时，由递归式可得： $a_4 = c_1 a_3 \oplus c_2 a_2 \oplus c_3 a_1 \oplus c_4 a_0$

即： $c_1 \oplus c_2 \oplus c_3 = 1 \qquad (1)$

同理可得： $c_1 \oplus c_2 \oplus c_3 \oplus c_4 = 0 \qquad (2)$

$c_2 \oplus c_3 \oplus c_4 = 0 \qquad (3)$

$c_3 \oplus c_4 = 0 \qquad (4)$

解方程组得 $c_1 = 0, c_2 = 0, c_3 = 1, c_4 = 1$

故所求移存器递推式为： $\boxed{a_n = a_{n-3} \oplus a_{n-4} \ (n \geq 4)}$

例　　设敌手得到密文串：101101011110010

和相应的明文串：011001111111001

因此，可得相应的密钥流：110100100001011

进一步假定敌手还知道密钥流是使用5级线性反馈移位寄存器产生的，那么敌手可分别用密钥流中的前10个比特建立如下方程

$$\begin{pmatrix} a_6 & a_7 & a_8 & a_9 & a_{10} \end{pmatrix} = \begin{pmatrix} c_5 & c_4 & c_3 & c_2 & c_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_7 \\ a_4 & a_5 & a_6 & a_7 & a_8 \\ a_5 & a_6 & a_7 & a_8 & a_9 \end{pmatrix}$$

即

$$\begin{pmatrix}0 & 1 & 0 & 0 & 0\end{pmatrix}=\begin{pmatrix}c_5 & c_4 & c_3 & c_2 & c_1\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1\\ 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0\end{pmatrix}$$

而

$$\begin{pmatrix}1 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1\\ 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0\end{pmatrix}^{-1}=\begin{pmatrix}0 & 1 & 0 & 0 & 1\\ 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 0\end{pmatrix}$$

从而得到

$$\begin{pmatrix} c_5 & c_4 & c_3 & c_2 & c_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

所以

$$\begin{pmatrix} c_5 & c_4 & c_3 & c_2 & c_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

密钥流的递推关系为

$$a_{i+5} = c_5 a_i \oplus c_2 a_{i+3} = a_i \oplus a_{i+3}$$

第十三讲 m-序列的安全性

- 解方程方法
- 线性反馈移位寄存器综合

线性反馈移位寄存器综合

根据密码学的需要，对线性反馈移位寄存器(**LFSR**)主要考虑下面两个问题：

（1）如何利用级数尽可能短的**LFSR**产生周期大、随机性能良好的序列。

这是从密钥生成角度考虑，用最小的代价产生尽可能好的、参与密码变换的序列。

（2）当已知一个长为N序列$\underline{a}$时，如何构造一个级数尽可能小的**LFSR**来产生它。

这是从密码分析角度来考虑，要想用线性方法重构密钥序列所必须付出的最小代价。

线性综合解

设$\underline{a}=(a_0,a_1,\cdots,a_{N-1})$是$F_2$上的长度为N的序列，而

$\boxed{f(x)=c_0+c_1x+c_2x^2+\cdots+c_lx^l}$ 是 F_2 上的多项式，$\boldsymbol{c_0=1}$.

如果序列中的元素满足递推关系：

$$\boxed{a_k=c_1a_{k-1}\oplus c_2a_{k-2}\oplus\cdots\oplus c_la_{k-l},k=l,l+1,\cdots,N-1 \qquad (2)}$$

则称$\langle f(x),l\rangle$产生二元序列$\underline{a}$。其中$\langle f(x),l\rangle$表示以$\boldsymbol{f(x)}$为特征多项式的$\boldsymbol{l}$级线性移位寄存器。

如果$\boldsymbol{f(x)}$是一个能产生$\underline{a}$并且级数最小的线性移位寄存器的特征多项式，$\boldsymbol{l}$是该移存器的级数，则称$\langle f(x),l\rangle$ 为序列$\underline{a}$的线性综合解。

线性移位寄存器的综合问题

线性移位寄存器的综合问题可表述为：给定一个N长二元序列$\underline{a}$，如何求出产生这一序列的最小级数的线性移位寄存器，即最短的线性移存器。

1、特征多项式$f(x)$的次数$\leq l$。因为产生$\underline{a}$且级数最小的线性移位寄存器可能是退化的，在这种情况下 $f(x)$的次数$<l$；并且此时 $f(x)$中的$c_l=0$，因此在特征多项式$f(x)$中仅要求$c_0=1$，但不要求$c_l=1$。

2、规定：0级线性移位寄存器是以$f(x)=1$为特征多项式的线性移位寄存器，且n长($n=1, 2, \ldots, N$)全零序列，仅由0级线性移位寄存器产生。事实上，以$f(x)=1$为反馈特征多项式的递归关系式是：$a_k=0$，$k=0, 1, \ldots, n-1$.因此，这一规定是合理的。

3、给定一个N长二元序列$\underline{a}$，求能产生$\underline{a}$并且级数最小的线性移位寄存器，就是求$\underline{a}$的线性综合解。利用B-M算法可以有效的求出。

Berlekamp-Massey算法（B-M算法）

用归纳法求出一系列线性移位寄存器：

$$\langle f_n(x), l_n \rangle \quad \partial^0 f_n(x) \le l_n, \quad n = 1, 2, \cdots, N$$

每一个 $\langle f_n(x), l_n \rangle$ 都是产生序列**a**的前**n**项的最短线性移位寄存器，在 $\langle f_n(x), l_n \rangle$ 的基础上构造相应的 $\langle f_{n+1}(x), l_{n+1} \rangle$ ，使得是 $\langle f_{n+1}(x), l_{n+1} \rangle$ 产生给定序列前**n+1**项的最短移存器，则最后得到的 $\langle f_N(x), l_N \rangle$ 就是产生给定*N*长二元序列**a**的最短的线性移位寄存器。

B-M算法（续）

任意给定一个N长序列 $\underline{a}=(a_{0},a_1,\cdots,a_{N-1})$，按n归纳定义

$$\langle f_n(x), l_n\rangle \qquad n=0,\ 1,\ 2,\cdots,N-1$$

1、取初始值：$f_0(x)=1,\quad l_0=0$

2、设 $\langle f_0(x),l_0\rangle,\langle f_1(x),l_1\rangle,\cdots,\langle f_n(x),l_n\rangle\ (0\le n<N)$ 均已求得，

且 $l_0\le l_1\le\cdots\le l_n$

记：$f_n(x)=c_0^{(n)}+c_1^{(n)}x+\cdots c_{l_n}^{(n)}x^{l_n},c_0^{(n)}=1,$ 再计算：

$$d_n=c_0^{(n)}a_n+c_1^{(n)}a_{n-1}+\cdots+c_{l_n}^{(n)}a_{n-l_n}$$

称d_n为第n步差值。然后分两种情形讨论：

B-M算法（续）

（ i ） 若 d_n =0，则令：

$$f_{n+1}(x)=f_n(x),\quad l_{n+1}=l_n\text{。}$$

（ ii ） 若 d_n =1，则需区分以下两种情形：

① 当：$l_0=l_1=\cdots=l_n=0$ 时，

取：$f_{n+1}(x)=1+x^{n+1}, l_{n+1}=n+1$。

② 当有 **m**（$0\le m<n$），使：$l_m<l_{m+1}=l_{m+2}=\cdots=l_n$。

便置：$f_{n+1}(x)=f_n(x)+x^{n-m}f_m(x), l_{n+1}=\max\{l_n, n+1-l_n\}$

最后得到的 $\langle f_N(x), l_N\rangle$ 便是产生序列 $\underline{\boldsymbol{a}}$ 的最短线性移位寄存器。

B-M算法举例

输入：S^8=10101111

n	d_n	f_n	L_n	m	f_m
0	1	1	0		
1	1	$1+x$	1	0	1
2	1	1	1	0	1
3	0	$1+x^2$	2		
4	0	$1+x^2$	2		
5	1	$1+x^2$	2	2	1
6	0	$1+x^2+x^3$	4		
7	1	$1+x^2+x^3$	4	5	$1+x^2$
8		$1+x^3+x^4$	4		

输出：⟨$1+x^3+x^4$, 4⟩

$$f_n(x)=c_0^{(n)}+c_1^{(n)}x+\cdots c_{l_n}^{(n)}x^{l_n},c_0^{(n)}=1,$$

$$d_n=c_0^{(n)}a_n+c_1^{(n)}a_{n-1}+\cdots+c_{l_n}^{(n)}a_{n-l_n}$$

（i） 若 d_n=0，则令：

$$f_{n+1}(x)=f_n(x),\quad l_{n+1}=l_n\text{。}$$

（ii） 若 d_n=1，则需区分以下两种情形：

① 当：$l_0=l_1=\cdots=l_n=0$ 时，

取：$f_{n+1}(x)=1+x^{n+1},l_{n+1}=n+1$。

② 当有 m（$0\le m<n$），使：

③ $l_m<l_{m+1}=l_{m+2}=\cdots=l_n$。

便置：$f_{n+1}(x)=f_n(x)+x^{n-m}f_m(x),$
$l_{n+1}=\max\{l_n,n+1-l_n\}$

感 谢 聆 听!

xynie@uestc.edu.cn