DOI: 10.13656/j.cnki.gxkx.2000.02.002
广西科学 Guangxi Sciences 2000, 7 (2): 85~87

组合前馈网络的并行算法*
Parallel Algorithm of Combining Feedback Network

黄文海 苏德富
Huang Wenhai Su Defu

(广西大学计算机与信息工程学院 南宁市西乡塘路 10号 530004)
(College of Computer and Information Engineering, Guangxi University, 10 Xixiangtanglu, Nanning, Guangxi, 530004, China)

摘要 讨论并分析组合前馈网络在 SIMD-CREW 模型上的并行算法。
关键词 伪随机序列 线性反馈移位寄存器 组合前馈网络 并行算法
中图法分类号 TP 301.6

Abstract The parallel algorithm of combing feedback network in SIMD-CREW model is discussed.
Key words pseudo-random sequence, linear feedback shift register, combining feedback network, parallel algorithm

伪随机序列在它形成的初期，便在通信、雷达、导航以及密码学等重要领域得到广泛应用。在密码学领域，Shannon证明了一次一密的密码体制是不可破的。这一结果给密码学研究以很大的刺激。若能以一种方式产生一随机序列，这一序列由密钥所确定，则利用这样的序列就可进行加密。遗憾的是要确定产生一真正的随机序列是极为困难的，从而使得一次一密体制没能得到广泛应用。

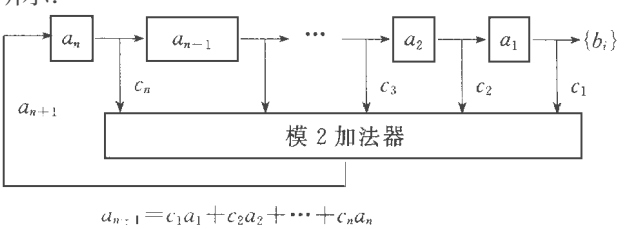
近年来，随着计算机理论及技术的发展，基于伪随机序列的流密码得到了广泛重视，成为人们研究的热点。在流密码系统中，为了提高整个系统的密码强度，常通过非线性函数对若干个模块的输出进行组合重整来实现，如基于线性反馈移位寄存器（LFSR)的前馈序列产生器。产生伪随机序列的其他方法还有非线性组合序列产生器、钟控序列产生器和非线性反馈移位寄存器等。

文献 [1] 介绍了组合前馈网络的基本概念和设计方法，文献 [3] 提出了一类用于流密码设计的性能优良而又结构简单的非线性组合函数。研究伪随机序列产生器的计算机快速并行实现的工作开展尚不多。本文探讨组合前馈网络在 SIMD-CREW 模型上的并行算法，并作实验验证。

2000-03-14收稿。
* 广西自然科学基金（9712010)资助项目。

1 n级线性反馈移位寄存器（LFSR）并行实现及分析

n级线性反馈移位寄存器（LFSR）的原理如图 1 所示：



$$a_{n+1}=c_1a_1+c_2a_2+\cdots+c_na_n$$

图 1 n级线性反馈移位寄存器（LFSR）原理图
Fig. 1 Principles of n-class linear feedback shift register

多项式 $f(x)=c_0+c_1x^n+c_2x^{n-1}+\cdots+c_nx$，($c_0=c_n=1$) 称为 LFSR的联接多项式。当一个 n级线性移位寄存器产生的序列的周期周期长度为 2^n-1时，这个序列称为 m 序列。LFSR产生 m 序列的充要条件是它的联接多项式为本原多项式。

在 SIMD-CREW模型上可如下实现 n级线性反馈移位寄存器（LFSR):

设 n是 2的幂，当前各寄存器的值存储在 boolean 数组 A [ ]中，联接多项式的系数存储在 boolean数组 C [ ]，boolean数组 B [ ]是辅存。以各寄存器为节点构造平衡二叉树，然后自节点向根遍历，计算反馈输

出值。算法用 Multipascal语言描述 (下同)。

算法 **1** 在 SIMD-CREW 模型上实现 n 级线性反馈移位寄存器 (LFSR)。

```
输入: 各寄存器的初始值
输出: 伪随机 m 序列
  begin
    for all i: = 1 to n do
      B [0, i] = A [i] and C [i];
    for h: = 1 to log n do (* 求联接多项式的值* )
      for all i: = 1 to n/2^ h do
          B [h, i] = B (h- 1, 2i- 1) xor B [h-
          1, 2i];
      for all i: = 1 to n do (* 移位寄存器移一位* )
        A [i- 1] = A [i];
      A [n] = B [log n, 1];
      输出 A [0];
  end
```

显然有:

定理 **1** 算法 1在实现 n 级 LFSR时,使用 n 个处理器在 $O(\log n)$ 的时间内产生序列的 1位。

而串行算法却要 $O(n)$ 的时间。

2 组合前馈网络及其设计

在密码学中,要使产生的二进制伪随机序列能够达到实用,加密后密文不可破或实际上不可破,一般地伪随机序列要满足以下的一些条件:

(1) 序列周期充分长,线性复杂度充分高,周期长度通常不少于 10^{16} 比特。任何由确定算法产生的伪随机序列都是周期的,得到 2倍周期的密文即可破译密文,故序列周期应远长于明文的长度。

一个 q 元有限域 $GF(q)$ 上序列 a 的线性复杂度 $C(a)$ 是指产生该序列的 $GF(q)$ 上级数最少的 LFSR 的级数。如下的结论告诉我们线性复杂度必须要充分高的理由。

设 $a = \{a_i\}$ 是 $GF(q)$ 上周期序列,且 $C(a) = L >= 1$,则只要知道 $\{a_i\}$ 中任意相继的 $2L$ 位就可确定整个序列 $\{a_i\}$ 及产生 $\{a_i\}$ 的极小多项式。

上述定理证明可参见文献 [1]。由定理 1可得如下推论: 用 n 级 m 序列加密后的密文只要知道密文相继的 $2n$ 位即可破译,尽管序列有很长的周期及很好的随机统计特性。

然而,对一个有限长的伪随机序列,线性复杂度太高,以至接近序列长度是不好的。直观地看,线性复杂度为序列周期一半左右为好。

(2) 良好的随机统计特性。

(3) 尽可能减少和避免熵漏,提高密钥序列的抗攻击能力。

任何一种密码系统产生的密文都在一定程度上"漏出"明文的有关信息,我们称之为"熵漏" (即信息漏),破译者根据这些熵漏可能获得有关明文的知识,甚至可能破译出相应的明文。就前馈组合网络而言,它主要有以下两种熵漏:

1) 相关性熵漏。组合函数 $f(x_1,\cdots,x_n)$ 的相关免疫度越大,前馈组合网络的相关性熵漏就越小。

2) 线性逼近熵漏。组合前馈序列是一种性能优良,结构规整,易于工程实现的、比较理想的伪随机密钥序列。

一般的组合前馈序列产生器如图 2所示,其中 $\{a_{1i}\},\{a_{2i}\},\cdots,\{a_{ni}\}$ 是 n 个级数分别为 $N1, N2,\cdots, Nn$ 的 m 序列,$f(x_1,x_2,\cdots,x_n)$ 为 n 元非线性组合函数,序列 $\{b_i\}$ 为:

$$b_i = f(a_{1i}, a_{2i},\cdots, a_{ni}), i = 0, 1, 2,\cdots$$

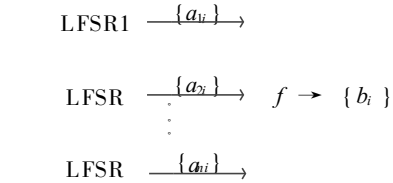


图 2 Fig. 2

称 $\{b_i\}$ 为由序列 $\{a_{1i}\},\{a_{2i}\},\cdots,\{a_{ni}\}$ 及 f 产生的组合前馈序列,f 称为组合函数。

组合前馈序列的周期及线性复杂度计算有如下结论:

设 $\{b_i\}$ 是由 n 个级数分别为 $N1, N2,\cdots, Nn$ 的 $GF(2)$ 上 m 序列和组合函数 $f(x_1, x_2,\cdots, x_n)$ 产生的组合前馈序列,若两两互素且 $x_1, x_2,\cdots, x_n$ 在 $f(\cdot)$ 的正则形式表示中都出现,则 $\{b_i\}$ 的周期为 $(\prod_{i=1}^{n}(2^{Ni}-1))$,其线性复杂度 $C(\{b_i\}) = f(N1, N2,\cdots, Nn)$,其中 $f(N1, N2,\cdots, Nn)$ 的计算是按整数运算的 (参见文献 [5])。

m 序列的选取可参看文献 [4]. 组合函数的选取最为关键,因为它直接影响组合序列的线性复杂度,周期和抗相关熵漏和线性逼近熵漏攻击的能力。

不重复的齐次 k 次型 (定义及有关性质参见文献 [2]) 具有较好的相关免疫性及抗线性逼近攻击的能力,而且结构规整。不失一般性,本文的组合函数均采用不重复的齐次 k 次型,其他的组合函数有同样的结果。

3 组合前馈网络的并行算法

假定组合前馈网络的线性移位寄存器共有 N 个,各个线性移位寄存器的级数分别为 $n_1, n_2, \cdots, n_N$,这里的 N 和 $n_i (i = 1, 2, \cdots, N)$ 均是 2的幂, $\max\{n_1, n_2, \cdots, n_N\} = n_{\max}$, $n = \sum_{i=1}^{N} n_i$; 组合函数 $f(x_1, x_2, \cdots, x_N)$ 为不重复的齐次 k次型, k为 2的幂。

$f(x_1, x_2, \cdots, x_N) = \sum_{i=1}^{N/k} x_{(i,1)} x_{(i,2)} \cdots x_{(i,k)}$, (这里是模 2连加)

其中 $(i, 1), (i, 2), \cdots, (i, k)$ $(i = 1, \cdots, N/k)$ 是 $1, 2, \cdots, N$ 的一个 k-排列。

利用平衡二叉树算法实现如下:

算法 2 在 SIMD-CREW模型上实现组合前馈网络。

```
输入: 各 LFSR的初值
输出: 组合前馈序列的 m位伪随机数
begin
  for x: = 1 to m do
    begin
      for all h: = 1 to N do
        调用算法 1, 并使第 (i, j) 个 (这里 j是 1, 2, …, k中的一个)
        LFSR的输出置于 D [0, (i, j)];
        for h: = 1 to log k do (* 进行 '乘' 运算 *)
        begin
          for all j = 1 to N /2^ h do
          D [h, j] = D [h- 1, 2j- 1] and D [h- 1, 2j];
        end;
        for all h: = logk + 1 to logN do (* 进行 '模 2加' 运算* )
          begin
            for all j = 1 to N /2^ h do
              D [h, j] = D [h- 1, 2j- 1] xor D [h- 1, 2j];
          end;
        输出 D [logN, 1];
end.
```

4 组合前馈网络并行实现算法的正确性证明和算法复杂度分析

正确性证明的关键在于证明在计算组合函数值中,作模 2加运算的有 $\log(N/k)$ 层,作乘运算的有 $\log k$ 层。由于组合函数 $f(x_1, x_2, \cdots, x_N)$ 为不重复的齐次 k次型, N和 k均为 2的幂,故利用平衡二叉树计算组合函数的值,自树的叶子往上计算 k次项的层数有 $\log k$ 层。又因为 $f(x_1, x_2, \cdots, x_N)$ 含有 N/k个 k次项,所以作模 2加的有 $\log(N/k)$ 层。从而至多使用 $N/2$个处理器,在 $O(\log N)$的时间内即可计算出组合函数的值。再由定理 1,即得:

定理 **2** 对含有 N (这里的 N为 2的幂) 个线性反馈移位寄存器 (级数分别为 $n_1, n_2, \cdots, n_N$; $n_{\max}$ 是其中最大的一个数) 的组合前馈,当组合函数 $f(x_1, x_2, \cdots, x_N)$ 为不重复的齐次 k次型 (k为 2的幂) 时,算法 2至多使用 $n(= \sum_{i=1}^{N} n_i)$ 个处理器,在 $O[(\log N + \log n_{\max})m]$ 的时间内即可产生 m 位的组合前馈序列。

5 结语

本文讨论的实现组合前馈网络的并行算法,组合函数采用不重复的齐次 k次型,算法规整,易于大规模并行实现,因而具有实际意义。另外,并行快速地生成伪随机序列是一个尚需进一步深入研究的很有意义的课题。

参考文献

1 杨义先, 林须端. 编码密码学. 北京: 人民邮电出版社, 1992.

2 卢开澄. 计算机密码学. 第 2版. 北京: 清华大学出版社, 1998.

3 张木想, 肖国镇. 流密码学中非线性组合函数的分析与设计. 电子学报, 1996, 24 (1), 48~ 52.

4 肖国镇等. 伪随机序列及其应用. 北京: 国防工业出版社, 1985.

5 Rueppel R, O Staffelbach. Products of seqences with maximum linear complexity, IEEE Trans. On Inform, Theory, 1987, 33 (1): 124~ 131.

(责任编辑: 蒋汉明)