(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103412738 B
(45)授权公告日 2016.02.17

(21)申请号 201310284391.X

(22)申请日 2013.07.08

(73)专利权人 中国航空无线电电子研究所
地址 200233 上海市徐汇区桂平路 432 号

(72)发明人 李金喜 陈顺方 徐丁海 方正 丁勇飞 何俊婷

(74)专利代理机构 上海和跃知识产权代理事务所(普通合伙) 31239
代理人 杜林雪

(51)Int.Cl.
*G06F 7/58*(2006.01)

(56)对比文件

CN 101019099 A,2007.08.15, 全文.

CN 101292223 A,2008.10.22, 全文.

US 2009/0292752 A1,2009.11.26, 全文.

US 2013/0036146 A1,2013.02.07, 全文.

柴先明等. 基于匹配搜索的伪随机序列生成多项式的轨迹. 《光学精密工程》.2011, 第 19 卷(第 9 期), 第 2222-2227 页.

吕辉等. 伪随机序列中本原多项式生成算法. 《计算机工程》.2004, 第 30 卷(第 16 期), 第 108-109 页.

Institut für Mathematik, Universit&auml t Zürich, Winterthurerstrasse. Multivariate permutation polynomial systems and nonlinear pseudorandom number generators. 《ELSEVIER》.2009, 第 16 卷第 144-154 页.

A. Marchi et al..Polynomial pseudo-random number generator via cyclic phase. 《ELSEVIER》.2009, 第 3328-3338 页.

审查员 雷青

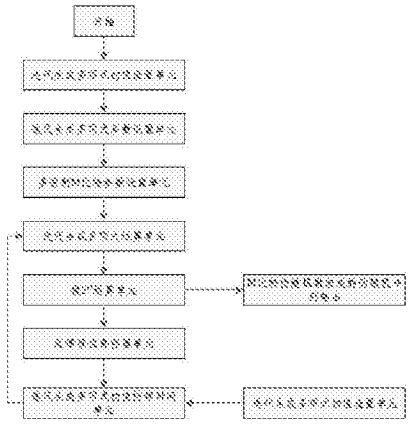
权利要求书1页 说明书3页 附图3页

(54)发明名称

基于单步迭代生成多项式的伪随机序列发生器及其实现方法

(57)摘要

本发明公开了一种基于单步迭代生成多项式的伪随机序列发生器及其实现方法,包含迭代生成多项式初值设置单元、迭代生成多项式系数设置单元、多进制 M 比特参数设置单元、迭代生成多项式初值持续时间单元、迭代生成多项式运算单元、模 $2^M$运算单元、反馈移位寄存器单元,迭代生成多项式运算单元根据多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 及单步迭代运算式 f(k)得到运算结果,其运算结果输入到模 $2^M$运算单元,得到 M 比特的迭代运算结果。本发明能够产生周期更长的多进制伪随机数组成的伪随机序列且方法简单易行,提高了采用伪随机序列系统的可靠性,增强了采用伪随机序列通信设备的安全性。



CN 103412738 B

1.一种基于单步迭代生成多项式的伪随机序列发生器，其特征在于，包含迭代生成多项式初值设置单元、迭代生成多项式系数设置单元、多进制 M 比特参数设置单元、迭代生成多项式初值持续时间单元、迭代生成多项式运算单元、模 $2^M$运算单元、反馈移位寄存器单元，所述迭代生成多项式初值设置单元生成多项式初值 $f(0) \in [0, 2^M-1]$；

所述迭代生成多项式系数设置单元生成多项式系数 $C_1$、$C_2$，$C_1$、$C_2$为质数；

所述多进制 M 比特参数设置单位生成多进制参数 M，M 为大于或等于 2 的自然数；

所述迭代生成多项式初值持续时间单元包含一个设定的初值 T 和一个实际运转的值，通过比较器对这两个值进行比较，如果实际运转的值大于设定的初值 T 就进入迭代生成模式，产生 M 比特伪随机数组成的伪随机序列，反之一直维持迭代生成多项式的初值；

所述迭代生成多项式运算单元根据多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 及单步迭代运算式 f(k) 进行运算生成运算结果，单步迭代运算式为：$f(k) = C_1 f(k-1) \pm C_2$ 或者 $f(k) = f^2(k-1) + C_1 f(k-1) + (2^M - C_2)$；

所述模 $2^M$运算单元对迭代生成多项式运算单元得到运算结果进行模 $2^M$运算，生成 M 比特伪随机数组成的伪随机序列；

所述反馈移位寄存器单元根据迭代生成多项式初值持续时间单元的设置决定将 M 比特伪随机数组成的伪随机序列输送到迭代生成多项式运算单元进入迭代生成模式或者一直维持迭代生成多项式的初值设定。

2.根据权利要求 1 所述的一种基于单步迭代生成多项式的伪随机序列发生器的实现方法，其特征在于包含以下步骤：

步骤一：根据迭代生成多项式、所需伪随机序列比特参数 M 的设置和初值的持续时间，迭代生成多项式初值设置单元产生迭代生成多项式初值 f(0)，迭代生成多项式系数设置单元生成多项式系数 $C_1$、$C_2$，多进制 M 比特参数设置单位生成多进制参数 M，迭代生成多项式初值持续时间单元生成初值持续时间 T，其中迭代生成多项式系数设置单元、多进制 M 比特参数设置单元均为数学赋值运算；

步骤二：迭代生成多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 输送到迭代生成多项式运算单元，根据单步迭代运算式 f(k) 得到运算结果；

步骤三：根据步骤二得到的运算结果输入到模 $2^M$运算单元，得到 M 比特的迭代运算结果并送入反馈移位寄存器单元；

步骤四：迭代生成多项式初值持续时间单元通过比较器对设定的初值 T 和一个实际运转的值进行比较，如果实际运转的值大于设定的初值 T，就指令反馈移位寄存器单元进入迭代生成模式，产生 M 比特伪随机数组成的伪随机序列，反之一直维持迭代生成多项式的初值。

# 基于单步迭代生成多项式的伪随机序列发生器及其实现方法

## 技术领域

[0001] 本发明涉及通信的遥控遥测领域，尤其涉及数字信息传输系统中的扩谱通信技术，是一种伪随机序列发生器及其实现方法。

## 技术背景

[0002] 伪随机序列具有类似随机噪声的某些统计特性，同时又能够重复产生。由于它具有随机噪声的优点，又避免了随机噪声的缺点，因此伪随机序列现已广泛地应用于许多重要领域，如密码学、扩频通讯、导航、现代战争中的电子对抗技术等等。比如在作战时跳频通信系统常采用m序列来进行频点的跳变控制，发送控制代码对无人机进行操控，由于m序列的伪随机性，在敌方截获我方地面所发的控制信号后，不易检测跳频通信系统的跳频图案，为信息战争赢得时间；同样，在密码学中对信息进行加密处理也需要伪随机序列，降低被敌方破解的概率。

[0003] 常用的伪随机序列为m序列，是最长线性反馈移位寄存器序列的简称，通常我们采用反馈移位寄存器来产生。我们常常希望用尽可能少的级数产生尽可能长的序列，一个N(N>=2,N为自然数）级线性反馈移位寄存器产生的序列最长周期等于（$2^N$-1），例如：4级反馈线性移存器产生的序列的周期最长为15，其对应的本原多项式常用的为$x^4+x+1$。一般，只要找到本原多项式，我们就能由它构成m序列发生器。在制作m序列发生器时，移位寄存器反馈线的数目直接决定于本原多项式的项数，为了使m序列发生器的组成尽量简单，我们希望使用项数最少的本原多项式，但是寻找本原多项式并不是很简单的，经过前人的大量计算，也仅仅找到了部分本原多项式，其生成序列的周期也为有限的，并且随着所需周期长度的增大，所能找到的m序列的本原多项式越来越少，复杂度也越来越高，不利于更长周期伪随机序列的产生。然而，现代的信息战争对通信设备的抗干扰技术要求越来越高，而伪随机序列的产生即是通信抗干扰技术中一个最为关键的要素。这一迫切的作战需求要求我们寻找更为简单的数学运算来构造周期更长的伪随机序列，从而满足快速发展的信息对抗战争的要求。

[0004] 发明目的

[0005] 本发明的发明目的是提供一种基于单步迭代生成多项式的伪随机序列发生器及其实现方法，降低伪随机序列实现长周期的复杂度。

[0006] 为实现以上目的，本发明通过以下技术方案实现：

[0007] 一种基于单步迭代生成多项式的伪随机序列发生器，包含迭代生成多项式初值设置单元、迭代生成多项式系数设置单元、多进制M比特参数设置单元、迭代生成多项式初值持续时间单元、迭代生成多项式运算单元、模$2^M$运算单元、反馈移位寄存器单元，所述迭代生成多项式初值设置单元生成多项式初值f(0)；

[0008] 所述迭代生成多项式系数设置单元生成多项式系数$C_1$、$C_2$；

[0009] 所述多进制M比特参数设置单位生成多进制参数M；

[0010] 所述迭代生成多项式初值持续时间单元包含一个设定的初值 T 和一个实际运转的值，通过比较器对这两个值进行比较，如果实际运转的值大于设定的初值 T 就进入迭代生成模式，产生 M 比特伪随机数组成的伪随机序列，反之一直维持迭代生成多项式的初值；

[0011] 所述迭代生成多项式运算单元根据多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 及单步迭代运算式 f(k) 进行运算生成运算结果；

[0012] 所述模 $2^M$ 运算单元对迭代生成多项式运算单元得到运算结果进行模 $2^M$ 运算，生成 M 比特伪随机数组成的伪随机序列；

[0013] 所述反馈移位寄存器单元根据迭代生成多项式初值持续时间单元的设置决定将 M 比特伪随机数组成的伪随机序列输送到迭代生成多项式运算单元进入迭代生成模式或者一直维持迭代生成多项式的初值设定。

[0014] 根据上述特征，一种基于单步迭代生成多项式的伪随机序列发生器的实现方法，包含以下步骤：

[0015] 步骤一：根据迭代生成多项式、所需伪随机序列比特参数 M 的设置和初值的持续时间等参数，迭代生成多项式初值设置单元产生迭代生成多项式初值 f(0)，迭代生成多项式系数设置单元生成多项式系数 $C_1$、$C_2$，多进制 M 比特参数设置单位生成多进制参数 M，迭代生成多项式初值持续时间单元生成初值持续时间 T，其中迭代生成多项式系数设置单元、多进制 M 比特参数设置单元均为数学赋值运算；

[0016] 步骤二：迭代生成多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 输送到迭代生成多项式运算单元，根据单步迭代运算式 f(k) 得到运算结果；

[0017] 步骤三：根据步骤二得到的运算结果输入到模 $2^M$ 运算单元，得到 M 比特的迭代运算结果并送入反馈移位寄存器单元；

[0018] 步骤四：迭代生成多项式初值持续时间单元通过比较器对设定的初值 T 和一个实际运转的值进行比较，如果实际运转的值大于设定的初值 T，就指令反馈移位寄存器单元进入迭代生成模式，产生 M 比特伪随机数组成的伪随机序列，反之一直维持迭代生成多项式的初值。

[0019] 依据上述特征，所述初值 $f(0) \in [0, 2^M-1]$，多项式系数 C1、C2 为质数，M 比特 >=2，M 为自然数。

[0020] 依据上述特征，所述单步迭代运算式 $f(k) = C_1 f(k-1) \pm C_2$，可以生成周期为 $2^M$ 的多进制（M 比特）伪随机数组成的伪随机序列。且 M 比特伪随机数在 $[0, 2^M-1]$ 区间内遍历。

[0021] 或者 $f(k) = f^2(k-1) + C_1 f(k-1) + (2^M - C_2)$，可以生成周期为 $2^{M-1}$ 的多进制（M 比特）伪随机数组成的伪随机序列。

[0022] 与现有技术相比，本发明的有益效果在于：采用单步迭代生成多项式产生周期更长的多进制伪随机数组成的伪随机序列，扩充了现有产生伪随机序列的方法。相对于已有的伪随机序列发生器的技术，完成了一个很大的突破，其单步迭代生成多项式数学计算简单易行，且由于 $C_1$ 与 $C_2$ 的取值具有随机性，生成多项式的种类也具有随机性且种类更多。在实际应用中，生成多项式被检测到的概率大大降低，大大提高了通信系统的鲁棒性；另外，本发明采用了软件无线电“伪随机序列的重构化和平台通用化”的思想，只需更改 $C_1$、$C_2$ 与 M 的值就可以产生不同的伪随机序列，节省了开发时间和设计成本。

## 附图说明

[0023] 图 1 为本发明基于单步迭代生成多项式的伪随机序列发生器的基本框图

[0024] 图 2 本发明实施例一中多进制(M 比特)伪随机序列发生器实现框图

[0025] 图 3 本发明实施例二中多进制(M 比特)伪随机序列发生器实现框图

## 具体实施方式

[0026] 下面结合附图与实施例,对本发明进一步详细说明 :

[0027] 实施例一 :

[0028] 如图 1 所示,本发明一种基于单步迭代生成多项式的伪随机序列发生器,包含包含迭代生成多项式初值设置单元、迭代生成多项式系数设置单元、多进制 M 比特参数设置单元、迭代生成多项式初值持续时间单元、迭代生成多项式运算单元、模 $2^M$运算单元、反馈移位寄存器单元,其具体实现方法如下 :

[0029] 步骤一 :根据迭代生成多项式、所需伪随机序列比特参数 M 的设置和初值的持续时间等参数,迭代生成多项式初值设置单元产生迭代生成多项式初值 f(0),f(0) ∈ $[0,2^M-1]$,迭代生成多项式系数设置单元生成多项式系数 $C_1$、$C_2$,$C_1$与 $C_2$取质数,多进制 M 比特参数设置单位生成多进制参数 M,M 比特 >=2,M 为自然数,迭代生成多项式初值持续时间单元生成初值持续时间 T,其中迭代生成多项式系数设置单元、多进制 M 比特参数设置单元均为数学赋值运算 ;

[0030] 步骤二 :迭代生成多项式初值 f(0)、多项式系数 $C_1$、$C_2$、多进制参数 M 输送到迭代生成多项式运算单元,根据单步迭代运算式 $f(k) = C_1 f(k-1) \pm C_2$得到运算结果 ;

[0031] 步骤三 :根据步骤二得到的运算结果输入到模 $2^M$运算单元,得到 M 比特的迭代运算结果并送入反馈移位寄存器单元 ;

[0032] 步骤四 :迭代生成多项式初值持续时间单元通过比较器对设定的初值 T 和一个实际运转的值进行比较,如果实际运转的值大于设定的初值 T,就指令反馈移位寄存器单元进入迭代生成模式,可以生成周期为 $2^M$的多进制(M 比特)伪随机数组成的伪随机序列。且 M 比特伪随机数在 $[0,2^M-1]$ 区间内遍历。

[0033] 实施例二

[0034] 与实施例一基本相同,区别在于步骤二中的单步迭代运算式 $f(k) = f^2(k-1)+C_1 f(k-1)+(2^M-C2)$,可以生成周期为 $2^{M\ 1}$的多进制(M 比特)伪随机数组成的伪随机序列。

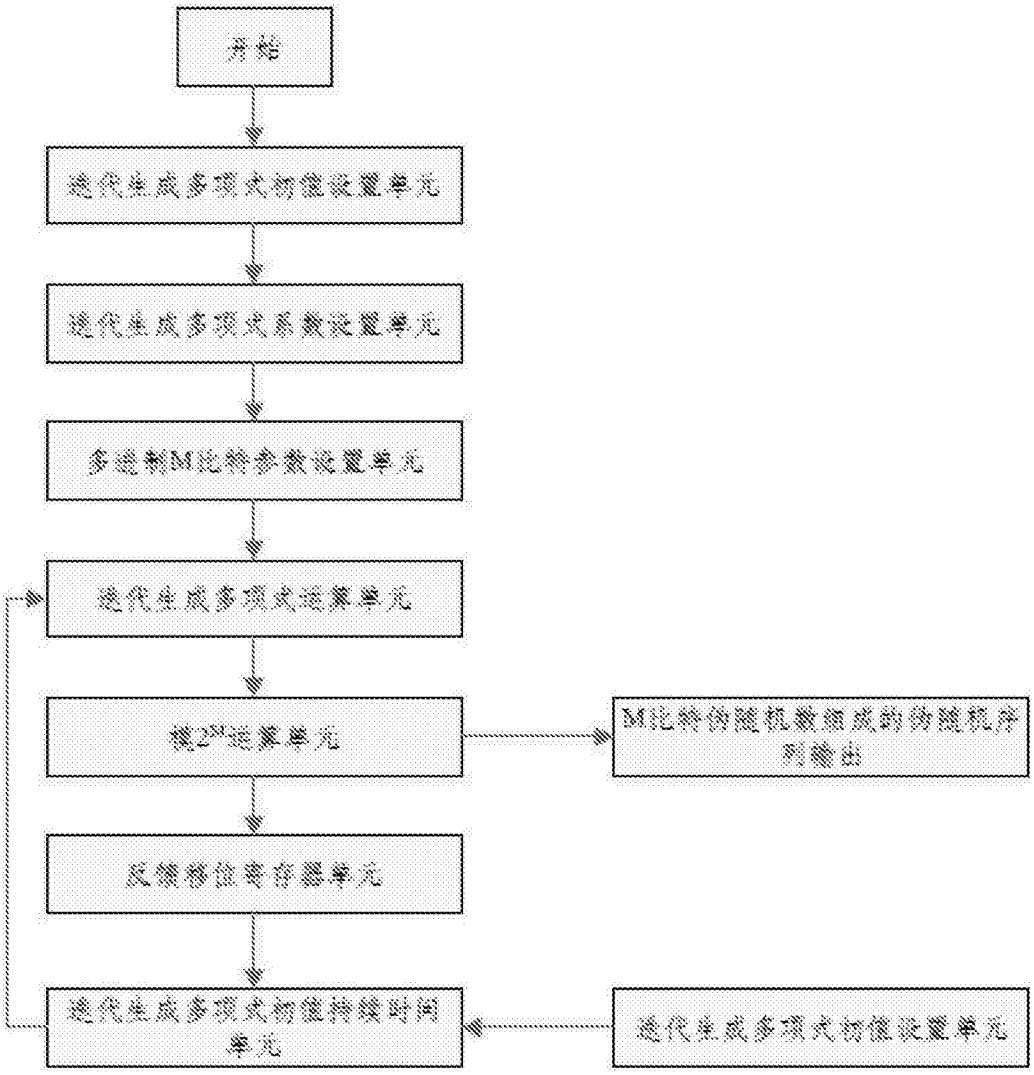

开始
迭代生成多项式初值设置单元
迭代生成多项式系数设置单元
多进制M比特参数设置单元
迭代生成多项式运算单元
模$2^M$运算单元
M比特伪随机数组成的伪随机序列输出
反馈移位寄存器单元
迭代生成多项式初值持续时间单元
迭代生成多项式初值设置单元

图 1

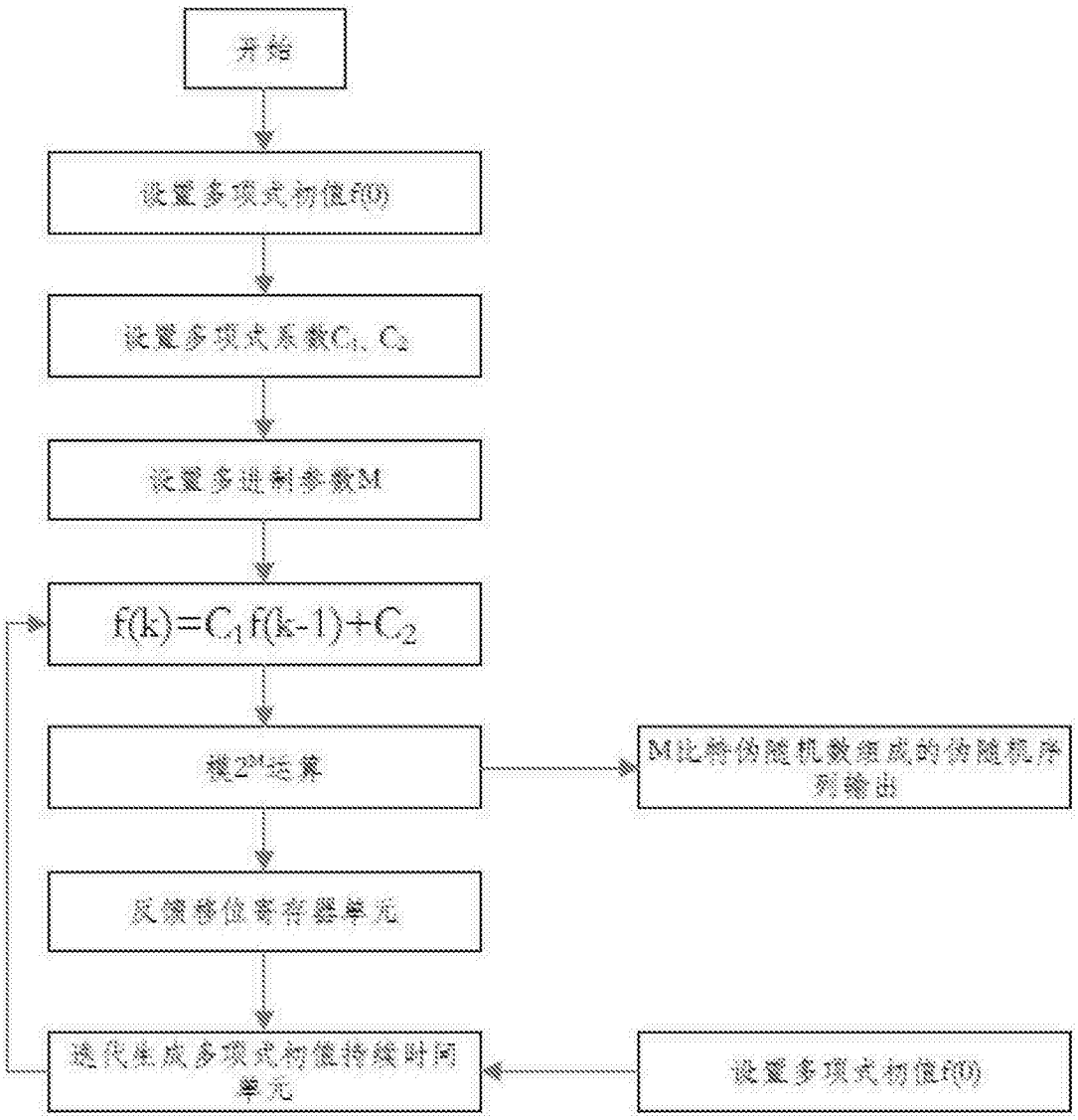

开始
设置多项式初值f(0)
设置多项式系数C1、C2
设置多进制参数M
f(k)=C1f(k-1)+C2
模2M运算
M比特伪随机数组成的伪随机序列输出
反馈移位寄存器单元
迭代生成多项式初值持续时间单元
设置多项式初值f(0)

图 2

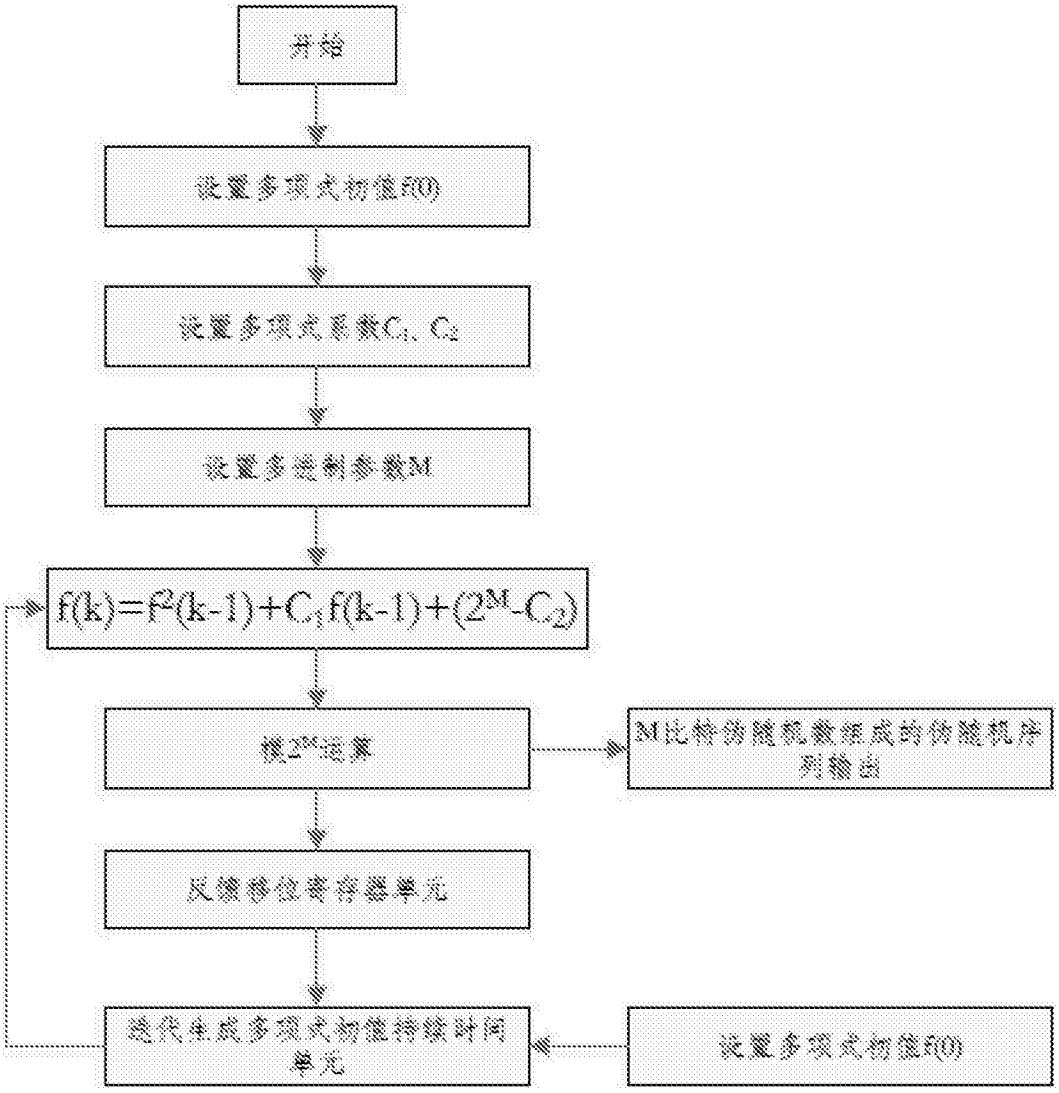

开始
设置多项式初值f(0)
设置多项式系数C1、C2
设置多进制参数M
f(k)=f²(k-1)+C1f(k-1)+(2M-C2)
模2M运算
M比特伪随机数组成的伪随机序列输出
反馈移位寄存器单元
迭代生成多项式初值持续时间单元
设置多项式初值f(0)

图 3