基于余数系统与置换多项式的高速长周期伪随机序列生成方法

马 上* 刘剑锋 杨泽国 张 艳 胡剑浩
(电子科技大学通信抗干扰技术国家级重点实验室 成都 611731)

摘 要：低复杂度长周期数字伪随机序列在现代加密、通信等系统中具有广泛的应用。该文提出一种基于余数系统和有限域置换多项式的伪随机序列生成方法。该方法基于中国剩余定理将多个互质的小周期有限域随机序列进行单射扩展生成长周期数字伪随机序列，置换多项式的迭代计算在多个并行的小动态范围有限域上进行，从而降低了硬件实现中迭代环路的计算位宽，提高了生成速率。该文还给出构建长周期伪随机序列的置换多项式参数选择方法和中国剩余定理优化方法，在现有技术平台下可轻易实现 2^{100} 以上的序列周期。同时，该方法具有极大的迭代多项式选择自由度，例如仅在 $q \equiv 2(\mathrm{mod}\,3)$ 且 $q \le 503$ 的有限域上满足要求的置换多项式就有 10905 种。硬件实现结构简单，基于 Xilinx XC7Z020 芯片实现 2^{90} 的随机序列仅需 20 个 18 kbit 的 BRAM 和少量逻辑资源，无需乘法器，生成速率可达 449.236 Mbps。基于 NIST 的测试表明序列具有良好的随机特性。

关键词：伪随机序列；余数系统；置换多项式；高速；长周期；现场可编程逻辑门阵列
中图分类号： TN918.2 **文献标识码**： A **文章编号**：1009-5896(2018)01-0042-08
DOI: 10.11999/JEIT170421

A Method of Generating High Speed and Long Period Pseudo-random Sequence Based on Residue Number System and Permutation Polynomial

MA Shang LIU Jianfeng YANG Zeguo ZHANG Yan HU Jianhao
(*National Key Laboratory of Science and Technology on Communications*, *University of Electronic and Science Technology of China*, *Chengdu* 611731, *China*)

Abstract: Low complexity and long period pseudo-random sequence is widely used in data encryption and communication systems. A method of generating pseudo-random sequence based on Residue Number System (RNS) and permutation polynomials over finite fields is proposed. This method extends several short period sequences into a long period digital pseudo-random sequence based on Chinese Remainder Theorem (CRT). Several short period sequences are generated by corresponding permutation polynomials over small finite fields parallelly, thereby reducing the bit width in hardware implementation and increased the generation speed. In order to generate long period sequences, a method to find the permutation polynomial and the the optimazition procedure for CRT are also proposed in this paper. Based on most of current hardware platforms, the proposed method can easily generate the pseudo-random sequence with period over 2^{100}. Meanwhile, this method has large space to select polynomials. For example, 10905 permutation polynomials can be used when $q \equiv 2(\mathrm{mod}\,3)$ and $q \le 503$. Based no Xilinx XC7Z020, it only costs 20 18 kbit BRAMs and a small amount of other resources (no multiplier) to generate a pseudo-random sequence whose period over 2^{90}, and the generation rate is over 449.236 Mbps. The results of NIST test show that the sequence has good random property and encryption performance.

Key words: Pseudo-random sequence; Residue Number System (RNS); Permutation polynomial; High speed; Long period; Field Programmable Gate Array (FPGA)

1 引言

数字伪随机序列(digital pseudo-random sequence)在通信、数据加解密及扰码等现代信息处理系统中具有重要作用并得到了广泛应用。常见的伪随机序列生成方法包括基于线性或非线性反馈移位寄存器生成法、同余法、基于 Logistic, Tent 等混沌映射的生成方法等。例如，在扩频通信中伪随机码是整个系统多址接入的基础，多采用反馈移位寄存器方法来实现[1,2]；在第 4 代移通信中的同步序列

收稿日期：2017-05-08；改回日期：2017-09-19；网络出版：2017-11-01
*通信作者：马上 mashang@uestc.edu.cn
基金项目：国家自然科学基金面上项目(61571083)
Foundation Item: The National Natural Science Foundation of China (61571083)

设计也成为系统设计的关键之一[3]。通常，基于反馈移位寄存器的方法具有简单高效的实现结构，但其多项式构造数目较少，因此在保密通信或加密系统中并不合适。而长周期数字随机序列则是基于扩频技术的保密通信的核心[1,4]，也是图像、语音等数据加密的关键[5−7]。近年来，基于混沌方法产生伪随机序列得到了深入研究。其中，文献[6]利用两个 1 维的混沌映射来生成新的混沌映射；Shunsuke 等人[8]分析了在整数域实现 Logistic 映射的相关性能。这些方法与传统的混沌映射存在同样的问题，即为了保证长周期特性其迭代环路计算位宽极长，导致了较低的生成速率，通常在实现 2^{50} 左右周期长度的序列输出速率仅能达到几十兆比特每秒。文献[9]则提出了利用忆阻器来生成伪随机序列的方法，NIST 测试表示具有较好的随机特性，但模拟电路的引入增加了系统同步和设计难度。文献[10]提出了一种基于半导体镭射技术的极高速混沌序列发生器设计方法(可达 480 Gbps)并分析了生成速率可达的理论限制，但设计难度较大，也未给出在保密和通信中的同步方法。

基于混沌方法所生成的伪随机序列具有长周期特性和良好的随机性，非常适合在保密系统或加密系统中使用。混沌映射生成伪随机序列的共同特点是需要迭代运算，在实现中迭代运算位宽与序列周期直接相关，例如常见的 Logistic, Tent 和 Chebyshev 映射在 60 bit 计算位宽下序列周期仅能达到 10^8 量级。因此，对于传统的混沌映射实际应用中通常需要进行周期扩展设计，导致了设计复杂度的上升并很难准确获知其周期性。另一方面，过大的计算位宽将导致硬件实现时迭代边界增加，难以获得高速输出的序列，从而难以胜任大带宽数字随机序列和高速扩频系统的要求。余数系统是中国古代在数学方面对人类的重要贡献之一，其主要思想是利用模运算代替大动态范围的运算，其突出优点在于将大位宽的乘加运算用多个小位宽的并行运算代替，因此在加密系统和乘加密集型的数字信号处理系统中得到了深入研究。针对随机序列迭代计算过程中的大位宽计算问题，Harris 公司[11]首先提出了基于余数系统和特殊混沌多项式的序列生成方法，并在文献[12]中指出了其信息熵与白噪声类似。但在其公开文献中仅给出了具有特定形式的 3 次迭代多项式选取方法及实现方法，在一定位宽内可选择的迭代多项式个数有限，同时未给出详细的原理分析。

针对这些问题，本文提出了一种基于置换多项式和余数系统的高速数字伪随机序列生成方法并对多项式的构造进行了深入分析，该方法利用多个阶互质的有限域置换多项式分别独立进行迭代运算，迭代环路的计算位宽较小，从而保证迭代速度；然后，利用优化的中国剩余定理将各支路的迭代运算结果进行单射扩展，从而将多个小的迭代环路映射到空间极大的计算环路上，保证迭代速度的同时获得长周期特性。本文基于常用的美国国家标准与技术研究院(National Institute of Standard and Technology, NIST)随机数测试标准对所生成的序列进行了测试分析，表明具有较好的随机特性。同时，该方法具有极大的迭代多项式选择自由度，例如仅在有限域 $q \equiv 2(\mathrm{mod}\,3)$ 且 $q \le 503$ 上满足要求的置换多项式就有 10905 种。最后，本文给出了一种基于 FPGA 的实现结构，Xilinx XC7Z020 实现结果表明其生成速率可达 449.236 Mbps，相同设计平台下本文方法所生成的随机序列在速度方面是传统方法的约 11 倍，而周期却可达传统方法的 2^{50} 倍；资源消耗方面，主要使用了片内存储器资源，无需乘法器资源。

2　余数系统与置换多项式

2.1 余数系统

余数系统(Residue Number System, RNS)是一种非权重数值表征系统，一个余数系统由一组两两互质的余数基 $\{m_1, m_2, \cdots, m_L\}$ 确定[13]。对于基为 $\{m_1, m_2, \cdots, m_L\}$ 的 RNS，余数向量 $\{x_1, x_2, \cdots, x_L\}$ ($x_i \in [0, m_i)$)所能表示的整数 X 动态范围为 $[0, M)$，其中 $M = \prod_{i=1}^{L} m_i$。令 $[0, M)$ 范围内的整数 a , b , c 的 RNS 表示分别为 $\{a_1, a_2, \cdots, a_L\}$, $\{b_1, b_2, \cdots, b_L\}$ 和 $\{c_1, c_2, \cdots, c_L\}$，若 $c_i = (a_i \Delta b_i) \bmod m_i$，则 $C = \langle A \Delta B \rangle_M$，其中“$\Delta$”表示加、减及乘法运算。著名的中国剩余定理(Chinese Remainder Theorem, CRT)给出了余数向量 $\{x_1, x_2, \cdots, x_L\}$ 到整数 X 的计算方法。

$$X = \left\langle \sum_{i=1}^{L} M_i \left\langle M_i^{-1} \right\rangle_{m_i} x_i \right\rangle_M \tag{1}$$

其中，$M_i = M / m_i$，$\left\langle M_i^{-1} \right\rangle_{m_i}$ 为 M_i 对 m_i 的模倒数。

由 RNS 整数的乘加运算和 CRT 可见，余数系统可以将位宽极大的整数运算划分到多个小位宽的有限域上进行，本文正是利用这一点来将各有限域上的迭代运算扩张至周期极大的整数环上，在获得长周期的同时提高序列生成速度。

2.2 置换多项式

置换多项式是一种完全剩余系的多项式[14,15]，设 $f(x) \in F_q(x)$，如果 $f: a \to f(a)$ 是 F_q 到 F_q 的一一映射，则称 $f(x)$ 是有限域 F_q 上的一个置换多项式。若

$f(x)$ 是 F_q 的置换多项式，当且仅当以下条件之一成立：

(1)函数 $f:c\to f(c)$ 是单射；

(2)函数 $f:c\to f(c)$ 是满射；

(3)对任意的 $a\in F_q$，$f(x)=a$ 在 F_q 中都有解；

(4)对任意的 $a\in F_q$，$f(x)=a$ 在 F_q 中都有唯一解。

符合上述 4 个条件中的任意一个时，$f(x)$ 为有限域上的置换多项式，但是由这 4 点只能去验证一个多项式是否为置换多项式，无法直接得出一个置换多项式。“可以用迪克逊多项式”来生成给定有限域上的置换多项式：

$$g_k(x,a)=\sum_{j=0}^{[k/2]}\frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j} \tag{2}$$

式中，k 为多项式次数，$a\in F_q$。迪克逊多项式决定了当 q 为奇数时，F_q 的所有次数为 6 的标准形置换多项式。表 1 给出了不超过 5 次的标准形置换多项式[15]，当次数大于 6 时，只有一些零碎的结果，没有比较完全的标准置换多项式表。利用表 1，可以得到低于 6 次的标准置换多项式。置换多项式保证了在有限域内的单射特性，使得每个有限域的迭代运算周期最长，这是本文所提出方法长周期特性的基础。

3 基于余数系统和置换多项式的伪随机序列生成方法

3.1 生成方法

(1)有限域置换多项式迭代方法及迭代周期：

令 L 个有限域 F_{q_l} 上的置换多项式为 $f_l(x)$，有限域的阶为 $m_l, l=1,2,\cdots,L$，根据 2.2 节中有关置换多项式的描述可知，若 $x\in[0,m_l)$，则 $f_l(x)\in[0,m_l)$，满足单射和满射关系。有限域 F_{q_l} 上的置换多项式 $f_l(x)$ 的迭代过程为

$$x_{k+1}^l=f_l\left(x_k^l\right) \tag{3}$$

对于式(3)，其迭代周期为：令迭代初始值为 x_0^l，N ($N=1,2,\cdots$)次迭代结果的集合为 $\left\{x_1^l,x_2^l,\cdots,x_N^l\right\}$，若第 $N+1$ 次迭代结果是集合 $\left\{x_1^l,x_2^l,\cdots,x_N^l\right\}$ 的元素，则迭代周期为 $p_l=N+1$，由于 $f_l(x)$ 是置换多项式，显然 $0<p_l\le m_l$。

(2)基于 CRT 的迭代周期扩展：假设每个有限域多项式的迭代周期 $p_l=m_l$ 且满足 $i\ne j$ 时 $\mathrm{GCD}\left(m_i,m_j\right)=1$ ($\mathrm{GCD}\left(m_i,m_j\right)$ 表示 m_i 和 m_j 的最大公约数)，即有限域的阶互质，显然迭代多项式最多形成 $\prod_{l=1}^{L}m_l$ 个不同的余数向量 $\left\{x_k^1,\cdots,x_k^l,\cdots,x_k^L\right\}$ $\left(k=\prod_{l=1}^{L}m_l\right)$。根据中国剩余定理：$L$ 个有限域迭代过程中生成的余数向量 $\left\{x_k^1,\cdots,x_k^l,\cdots,x_k^L\right\}$ 与权重系统中的整数 X_k 一一对应，由于 $p_l=m_l$ 且 $\mathrm{GCD}\left(m_i,m_j\right)=1$，因此生成的整数 X_k 的周期为 $\prod_{l=1}^{L}m_l$。

这一过程可由图 1 来表示，L 个有限域上的多项式迭代形成 L 个数环 $R_i(i=1,2,\cdots,L)$，数环的元素为 $\{0,1,\cdots,m_l-1\}$，且满足 $i\ne j$ 时 $\mathrm{GCD}\left(m_i,m_j\right)=1$。由于选取的迭代多项式 $f_l(x)$ 是有限域 F_{q_l} 上的置换多项式，当迭代周期满足 $p_l=m_l$ 时，可以利用 CRT 进行转换。CRT 将向量 $\left\{x_k^1,\cdots,x_k^l,\cdots,x_k^L\right\}$ 一一对应地转换至整数域，且形成了在有限域 $[0,M)$ 上的置换映射并形成数环 R，其迭代周期可达 $\prod_{l=1}^{L}m_l$。若选取的迭代多项式 $f_l(x)$ 具有非线性随机特性，所生成的数环 R 也具有非线性随机特性，对迭代所生成的样点 X_k 进行优化处理则可以得到需要的随机序列。图 1 中，后处理部分根据不同的应用场景可能含有高斯映射、序列平衡度调整、比特映射等，不作为本文讨论的重点。

可见，基于 CRT 的映射将多个小的迭代环路映射至等价的周期极大的迭代环路上。反过来，这种方法也将动态范围极大的有限域迭代用多个并行计算的小动态范围有限域迭代运算代替，减小了环路的迭代边界，从而提高了序列的生成速率。图 1 所示的方法中置换多项式的选择是影响输出序列伪随机性的关键；而基于 CRT 的映射优化则是决定序列周期的核心，同时也是实现复杂度优化的关键之一。

表 1 次数不超过 5 的标准形置换多项式

F_q 的标准形置换多项式	q 值
x	任何 q
x^2	$q\equiv 0(\mathrm{mod}\,2)$
x^3	$q\equiv 2(\mathrm{mod}\,3)$
x^3-ax (a 非平方)	$q\equiv 0(\mathrm{mod}\,3)$
$x^4\pm 3x$	$q=7$
$x^4+a_1x^2+a_2x$ (且 $x=0$ 是其唯一根)	$q\equiv 0(\mathrm{mod}\,2)$
x^5	$q\ne 1(\mathrm{mod}\,5)$
x^5-ax (a 非四次方)	$q\equiv 0(\mathrm{mod}\,5)$
$x^5+ax\left(a^2=2\right)$	$q=9$
$x^5\pm 2x^2$	$q=7$
$x^5+ax^3\pm x^2+3a^2x$ (a 非平方)	$q=7$
$x^5+ax^3+5^{-1}a^2x$	$q\equiv\pm 2(\mathrm{mod}\,5)$
$x^5+ax^3+3a^2x$ (a 非平方)	$q=13$
$x^5-2ax^3+a^2x$ (a 非平方)	$q\equiv 0(\mathrm{mod}\,5)$

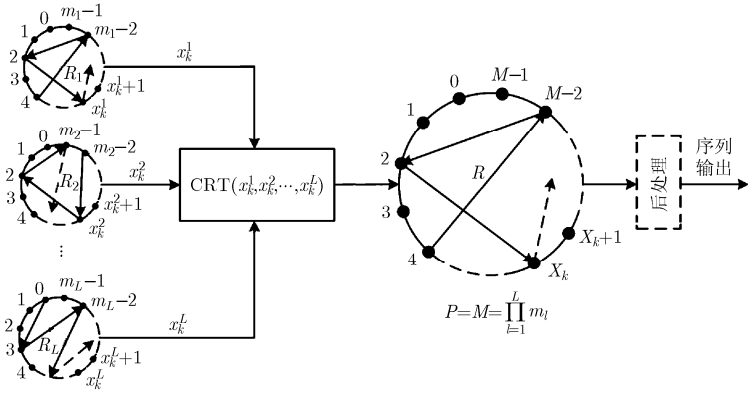

图 1 基于余数系统的混沌序列生成方法

3.2 多项式选择方法

有限域上的置换多项式形式是迭代周期的关键，恰当的多项式选择可以保证其迭代周期达到有限域的阶，从而使周期最大化。由 2.2 节中有关置换多项式的定义可知，函数 $f(x)$ 的自变量域与值域一一映射且自变量域与值域相同时即为置换多项式。置换多项式保证了自变量域和值域的一一映射，但迭代方程按式(4)定义时，需要进行仔细讨论，以使得各环路的迭代周期互质并达到有限域的阶，从而保证整个输出序列的周期最大化。

$$x_{k+1} = f(x_k) \tag{4}$$

(1)消失态与多环路：　由 3.1 节的描述可知，利用 CRT 进行合并时，所生成环路 R 的最大动态范围要达到 M，则每个小的迭代环路不同元素应达到有限域的阶 m_l $(l=1,2,\cdots,L)$，若置换多项式存在 $x_a^l = f_l\left(x_a^l\right)$ 的映射(a 为使 $x_a^l = f\left(x_a^l\right)$ 的集合)，则当迭代初始值选择为 x_a^l 时，显然有

$$x_{k+1}^l = f_l(x_k^l) = x_k^l \tag{5}$$

则每次迭代的结果相同，从而在该有限域上的迭代周期仅为 1，称之为消失态。即使未选择 x_a^l 作为迭代初始值，因为存在消失态，迭代的周期也不能达到 m_l，从而无法保证最长周期特性。例如：以 $q=2(\mathrm{mod}\,3)$ 的有限域上置换多项式 $f(x)=\left\langle x^3+3x^2+3x+1\right\rangle_5$ 为例，按照式(4)的迭代过程状态转移图 2 所示。

图 2 中状态转移环路为 $0\to1\to3\to4\to0$ 和 $2\to2$，最长的迭代环路周期为 4，状态 2 为消失态。

另一方面，若迭代初始值选择为 x_a^l，迭代周期 $1<p_l<m_l-1$，则存在多环路问题，此时任意迭代环路 $f_l(x)$ 均不能达到最长迭代周期 m_l，从而也无法保证最长周期特性。仍然以 $q=2(\mathrm{mod}\,3)$ 的有限域上置换多项式 $f(x)=\left\langle x^3+x^2+2x+3\right\rangle_5$ 为例，其状态转移如图 3 所示。

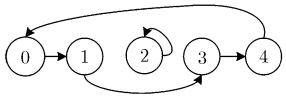

图2 $f(x)=\left\langle x^3+3x^2+3x+1\right\rangle_5$ 状态转移图

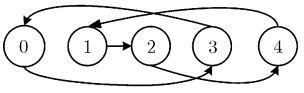

图3 $f(x)=\left\langle x^3+x^2+2x+3\right\rangle_5$ 状态转移图

图 3 中具有两个迭代环路，$0\to3\to0$ 和 $1\to2\to4\to1$，显然两个环路的周期均不能达到 5，从而也无法达到长周期特性。

因此，对于任何初始值具有最长周期特性的置换多项式迭代环路只有一个，具有迭代单环路特性。

(2)置换多项式选择方法：　首先，为了保证序列的随机特性，置换多项式应具有非线性特性。其次，由于置换多项式并不能保证迭代过程中的最长周期特性，为了使 CRT 扩展后的随机序列具有最长的确定周期 $\prod_{l=1}^{L} m_l$ (即每个迭代环路的迭代周期为 m_l)，需对置换多项式进行仔细选择，以避免上述的消失态和多环路问题。

通过表 1 的标准置换多项式可以生成很多新的置换多项式，实际上迭代多项式的常数项表示了置换多项式在有限域 F_q 上的映射偏移量，不同的偏移量导致按照式(4)的迭代环路的个数不同，不会改变多项式的置换特性。利用迭代周期的定义，可以用表 2 的算法 1 对置换多项式的常数项进行筛选。

按照迭代周期定义，算法的基本思路如下：首先选择去掉常数项的置换多项式 $\left\langle f(x)\right\rangle_m$ 并令其常数项 c 取值范围为 0～$m-1$；然后设定一个初始值 $x_0=k$ 进行 $x_{k+1}=\left\langle f\left(x_k\right)+c\right\rangle_m$ 迭代运算，由置换多项式的单射性可知，当首次出现当前迭代结果与初始迭代结果相同则说明存在环路并停止迭代；最后，判断当前的迭代次数与最长周期 m 是否相等，若相等则当前的 c 满足单环路迭代条件，否则存在消失

表 2 置换多项式选择方法

算法 1 具有最长迭代周期的置换多项式常数项选择算法

选择置换多项式 $\langle f(x)\rangle$：

$x_0=k,\ x_1=\langle f(x_0)+c\rangle_m$ %设置迭代初始值并计算与初始值对应的迭代结果

for $c=0,1,\cdots,m-1$ %迭代多项式的常数项 c 的取值范围

for $i=1,2,\cdots,m$ %迭代次数累加

$x_{i+1}=\langle f(x_i)+c\rangle_m$; %迭代多项式计算

if $x_{i+1}=x_1$ 若迭代计算结果同初始迭代值相同

break;

if $i\neq m$ %若与初始迭代值相同且迭代次数小于最长周期 m

环路周期为 i，存在多环路，常数 c 不符合长周期特性

else

环路周期为 m，迭代周期达到最大，常数 c 符合长周期特性

end if

end if;

end for

end for

态或多环路情况。

根据算法 1，我们进行了有限域 $q\equiv 2(\mathrm{mod}\,3)$ 且 $q\le 503$ 上的单环路置换多项式搜索，共有 10905 个多项式满足要求。可见，本文提出的这种方法在多项式选择方面具有极大的自由度。

3.3 中国剩余定理优化

式(1)给出了中国剩余定理的计算方法，CRT 的计算保证了余数向量与传统权重系统的计算一一对应。然而，对于本文提出的伪随机序列生成方法，并不需要将各迭代环路的迭代结果通过 CRT 计算来获得准确的在权重系统中的数值。这是由于系统本身需要的输出就是随机序列，只要保证其长周期特性不变，每次迭代结果的准确数值是可以改变的。至于序列的随机性，无论是否通过 CRT 进行了准确的数值映射，都需要进行专门测试，将在后文进行专门讨论。基于以上考虑，可以对中国剩余定理进行优化，以便减小实现复杂度，简化 CRT 如式(6)所示。

$$X_k=\sum_{l=1}^{L}M_l x_k^l \tag{6}$$

式(6)去掉了乘积中的模倒数 $\left\langle M_i^{-1}\right\rangle_{m_i}$ 和模 M 运算，下面将给出详细证明式(6)的映射是单射过程，从而保证经式(6)的运算得到序列 X_k 具有长周期特性。

由于经过适当的置换多项式系数选择可以使其迭代周期 $p_l=m_l$，且满足 $i\neq j$ 时 $\mathrm{GCD}\left(m_i,m_j\right)=1$，因此多个迭代环路任意初始值的迭代将产生 M 种不同的余数向量 $\left\{x_k^1,\cdots,x_k^l,\cdots,x_k^L\right\}$。若式(6)的映射满足 $\left\{x_k^1,\cdots,x_k^l,\cdots,x_k^L\right\}$ 到数域 X 上是单射的，则必然存在 M 个不同的映射结果 X_k，从而保证了得到最长周期序列 X_k。下面给出式(6)的映射过程是单射的证明。

证明 令余数向量 $\left\{x_i^1,\cdots,x_i^l,\cdots,x_i^L\right\}$ 和 $\left\{x_j^1,\cdots,x_j^l,\cdots,x_j^L\right\}$ 经式(6)映射得到的结果为 X_i 和 X_j，假设 $X_i=X_j$，若能证明 $\left\{x_i^1,\cdots,x_i^l,\cdots,x_i^L\right\}$ 和 $\left\{x_j^1,\cdots,x_j^l,\cdots,x_j^L\right\}$ 相同则说明式(6)是单射的。由式(6)：

$$X_i-X_j=\sum_{l=1}^{L}M_l\left(x_i^l-x_j^l\right)=\sum_{l=1}^{L}M_l\alpha_l \tag{7}$$

其中，$\alpha_l=x_i^l-x_j^l$。由于 $x_i^l\in[0,m_i)$，因此 $\alpha_l\in(-m_i,m_i)$。

首先考虑两通道余数向量 $\left\{x_i^1,x_i^2\right\}$ 和 $\left\{x_j^1,x_j^2\right\}$，其映射结果分别为 X_i 和 X_j，若映射结果相同，则

$$X_i-X_j=M_1\alpha_1+M_2\alpha_2=m_2\alpha_1+m_1\alpha_2=0 \tag{8}$$

从而有

$$\frac{m_2}{m_1}=-\frac{\alpha_2}{\alpha_1} \tag{9}$$

由于 $\mathrm{GCD}(m_1,m_2)=1$，显然式(9)要成立必然有 $\alpha_1\ge m_1$，$\alpha_2\ge m_2$，这不符合 $\alpha_l\in(-m_l,m_l)$ 的条件。因此，要使等式(8)成立，必然有 $\alpha_1=\alpha_2=0$。

对于三通道余数向量 $\left\{x_i^1,x_i^2,x_i^3\right\}$ 和 $\left\{x_j^1,x_j^2,x_j^3\right\}$，其映射结果分别为 X_i 和 X_j，若映射结果相同，则

$$\begin{aligned}X_i-X_j&=m_2m_3\alpha_1+m_1m_3\alpha_2+m_1m_2\alpha_3\\&=\left(m_2\alpha_1+m_1\alpha_2\right)m_3+m_1m_2\alpha_3=0\end{aligned} \tag{10}$$

从而，

$$\frac{m_2\alpha_1+m_1\alpha_2}{\alpha_3}=-\frac{m_1m_2}{m_3} \tag{11}$$

由于 $\mathrm{GCD}\left(m_3,m_1m_2\right)=1$，且 $\alpha_3\in\left(-m_3,m_3\right)$，因此要满足式(10)，必然有

$$\alpha_3=m_2\alpha_1+m_1\alpha_2=0 \tag{12}$$

对于式(8)的讨论已知要满足式(10)和式(11)，则必然有 $\alpha_1=\alpha_2=\alpha_3=0$。因此，对于三通道余数系统 $\left\{x_i^1,x_i^2,x_i^3\right\}$ 和 $\left\{x_j^1,x_j^2,x_j^3\right\}$ 若通过式(6)的映射得到相同的结果，余数向量必然相同，即式(6)的映射是单射的。 证毕

对于 L 通道余数向量 $\left\{x_i^1,\cdots,x_i^l,\cdots,x_i^L\right\}$ 和 $\left\{x_j^1,\cdots,x_j^l,\cdots,x_j^L\right\}$，其映射结果分别为 X_i 和 X_j，若映射结果相同，则：

$$\begin{aligned}X_i-X_j=m_L\big(&m_{L-1}\big(\cdots m_3\left(m_2\alpha_1+m_1\alpha_2\right)\\&+m_1m_2\alpha_3\big)+m_1m_2\cdots m_{L-2}\alpha_{L-1}\big)\\&+m_1m_2\cdots m_{L-1}\alpha_L=0\end{aligned} \tag{13}$$

同理，由于 $\mathrm{GCD}(m_L, m_1 m_2 \cdots m_{L-1}) = 1$ 且 $\alpha_L \in (-m_L, m_L)$，必然要求 α_L 和式(13)的第 1 个求和项为 0，以此类推满足式(13)的条件为 $\alpha_l = 0 (l = 1, 2, \cdots, L)$，即余数向量 $\left\{x_i^1, \cdots, x_i^l, \cdots, x_i^L\right\}$ 和 $\left\{x_j^1, \cdots, x_j^l, \cdots, x_j^L\right\}$ 相同时才能得到相同的映射结果。

通过改进如式(6)所示的 CRT 映射，从而消除了 CRT 中的大位宽的模 M 运算，也消除了常数项 $\left\langle M_i^{-1} \right\rangle_{m_i}$ 的乘法运算，可以大幅度降低实现复杂度。

4　序列测试与分析

伪随机序列最重要的特性为其随机性，本节将基于本文提出的伪随机序列生成方法来生成伪随机序列并对其进行随机性测试。为了简化序列映射的后处理过程，根据拓扑传递性取式(6)输出的低 16 位，然后取最高位作为比特序列输出。

4.1 测试环境设置

由表 1，以 $q = 2 (\mathrm{mod}\, 3)$ 有限域上的标准置换多项式为基础并结合 3.2 节中的常数项选择方法，用于测试的 6 个置换多项式如式(14)所示。

$$\left.\begin{aligned} f_1(x) &= \left\langle x^3 + 3x^2 + 3x + 59 \right\rangle_{251} \\ f_2(x) &= \left\langle x^3 + 6x^2 + 12x + 77 \right\rangle_{347} \\ f_3(x) &= \left\langle x^3 + 9x^2 + 27x + 111 \right\rangle_{443} \\ f_4(x) &= \left\langle x^3 + 12x^2 + 48x + 42 \right\rangle_{467} \\ f_5(x) &= \left\langle x^3 + 15x^2 + 75x + 288 \right\rangle_{479} \\ f_6(x) &= \left\langle x^3 + 21x^2 + 147x + 8 \right\rangle_{503} \end{aligned}\right\} \tag{14}$$

该组多项式生成的序列 X_k 的周期为 $M = 251 \times 347 \times 443 \times 467 \times 479 \times 503$ (约 2^{52})，若生成速率为 100 Mbps，则需要约 1.38 年左右才能完成一个周期循环。

测试工具介绍：

有大量手段来评估序列的随机性，包块统计学测试和时频域测试等。目前采用较多的为美国国家标准与技术研究院(NIST)随机数测试标准作为序列随机性的衡量方法。NIST 随机数测试标准中包含 15 个测试大项，包括序列的频数检测、游程检测、线性复杂度检测等。本文采用了与随机数测试标准 NIST SP800-22 对应的最新软件 STS-2.1.2 作为测试工具[16]。NIST 测试标准中，每个测试项都会生成一个 P_value，当 P_value ≥ 0.001 时，则可认为该项测试通过；当 P_value < 0.001 时，则认为该项测试不通过。

4.2 测试结果及分析

STS-2.1.2 每次测试长度最长为 100 万点，测试中对式(14)的迭代多项式组给予随机的初值来生成 2000 个长度为 1000000 的伪随机序列，然后调用 NIST 测试工具进行测试，同时选择最新文献[6]作为测试的对比参考文献，在文献[6]中仅测试了 100 组长度为 1000000 的伪随机序列，最终统计分析测试结果如表 3 所示。

表 3 的第 2 和第 3 列测试结果分别为 p_value>0.001 和 p_value>0.01 条件下本文的测试通过率，第 4 列为本文不同测试项的 p_value 的均值，最右侧两列为文献[6]在 p_value>0.01 时的测试结果及其不同测试项的 p_value 均值。从表 3 中可知，本文的测试通过成功率全部在 96.5%以上，符合通常使用 NIST SP800-22 标准的测试成功率判断阈值[17]。同时，由表 3 可知本文所提出的方法生成的

表 3　NIST 测试结果

测试项	测试通过率(%) p_value>0.001	测试通过率(%) p_value>0.01	p_value 均值	文献[6]测试通过率(%) p_value>0.01	文献[6] p_value 均值 p_value>0.01
Frequency Test	100.00	99.20	0.4994	98.00	0.1538
Frequency Test within a Block	99.85	99.15	0.4948	99.00	0.7792
Runs Test	99.90	98.65	0.5065	100.00	0.4944
Test for the Longest Run of Ones in	99.85	99.05	0.4971	99.00	0.5141
Binary Matrix Rank Test	99.90	98.70	0.4985	99.00	0.8832
Discrete Fourier Transform Test	99.85	99.00	0.4842	98.00	0.0428
Non-overlapping Template	99.95	99.20	0.5043	98.38	0.4794
Overlapping Template Matching	99.85	98.90	0.5249	100.00	0.2493
Maurer's "Universal Statistical"	99.80	98.75	0.4960	100.00	0.1917
Linear Complexity Test	99.85	99.00	0.5034	98.00	0.1154
Serial Test	99.85	98.85	0.4936	98.50	0.2523
Approximate Entropy Test	99.85	98.85	0.4936	99.00	0.4373
Cumulative Sums Test	100.00	99.35	0.5012	98.00	0.5087
Random Excursions Test	99.65	97.75	0.5183	98.89	0.4506
Random Excursions Variant Test	99.75	98.95	0.5134	99.01	0.2544
成功数目	15/15	15/15	15/15	15/15	15/15

随机序列测试结果的 p_value 均值绝大多数明显大于文献[6]的对应项的均值，而 p_value 的值越大表明序列的随机性越好[17]。因此，本文所提出的方法生成的序列的随机性优于文献[6]。

通过对 2000 组数据的测试结果进一步分析，表 4 给出了 NIST 的 15 个单项测试中不通过项数目对应的序列组数统计情况。

表 4 单组序列测试不通过项数

单次 15 项测试中 p_value < 0.01 项数	序列组数
5	2
4	3
3	7
2	37
1	215
0	1736
合计	2000

表 4 中 2000 组数据中的 1736 组数据能够通过所有的测试项，有 215 组数据只有 1 项未通过，只有 5 组数据超过 4 项测试未通过。可见本文提出的序列生成方法得到的序列中，没有一组序列在所有测试项中都无法通过随机数测试标准，只有少数的序列有不通过项存在，表明生成的序列具备良好的随机性。

5 基于 FPGA 的算法实现及性能分析

本文提出的伪随机序列生成方法主要优点在于可通过多个小位宽的迭代环路来合成周期极长的伪随机序列，而各迭代环路的迭代多项式具有极大的选择自由度。如此，各迭代环路的迭代边界较小，在硬件实现中易于做到高速输出。图 4 为基于本文方法的 FPGA 实现结构框图。由于每个余数通道可以取动态范围较小的有限域(例如 10 bit 以内)，通过多个通道的合并来获得大动态范围和长周期输出，因此每个通道的迭代环路计算可以采用查找表方式实现。同时，为了进一步提高生成速率在基于 CRT 的扩展部分也采用了查找表方式实现。每个迭代环路的 LUT 深度即为该通道有限域的阶 m_l，对应位宽为 B；根据拓扑传递性，取 CRT 扩展后的数据的低 16 bit 输出作为二进制比特映射模块的输入。按照 10 个通道，每个通道 10 bit 迭代环路位宽，CRT 映射查找表位宽 16 bit 计算，共需要 260 kbit 的存储空间，这对于现代主流 FPGA 芯片的存储资源来讲绰绰有余。

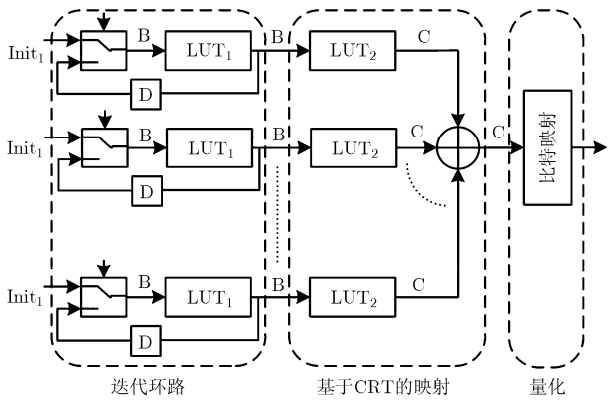

图 4 基于本文方法的 FPGA 实现框图

这种基查找表的结构还有一个优点在于，LUT 中的数据可根据所选择的有限域置换多项式计算并配置，从而为应用带来了灵活性。

基于 Xilinx XC7Z020 芯片，表 5 为具有 10 个迭代环路长周期随机序列发生器的FPGA实现结果与基于传统混沌映射实现主要硬件资源比较。对于传统方法，由于仅依赖增加迭代环路位宽来获得长周期特性必然导致极慢的速出速率，因此实现中传统方法中采用了通常使用的周期扩展方法，包括了 1 个 Logistic、1 个 Tent 映射和 1 个 m 序列映射模块，并选择它们之间的相互扰码结果作为最终输出序列以获得长周期特性，图 5 为基于传统混沌序列生成方法的结构。XC7Z020 是目前广泛使用的一种低成本 SoC 芯片，但并非以规模和速度见长，基于该平台本文方法所生成的序列速率仍然达到了 449.236 Mbps 以上。并且获得的序列周期长度是传统方法的 2^{50} 倍。FPGA 资源占用方面，本文方法主要消耗了 14%的片内 BRAM 资源，而传统方法则需要约 12%的片内乘法器，LUT 则只需传统方法的 1/3 左右。因此，无论从序列的长周期性、硬件资源消耗和生成速率方面，本文方法具有显著优势。

6 结论

本文基于有限域上的置换多项式和中国剩余定理，提出了一种长周期高速伪随机序列生成方法，并给出了保证长周期特性的置换多项式选择方法，以及 CRT 扩展映射中的优化方法和详细证明。该方法将多个有限域上的非线性迭代结果合成为周期极长的伪随机序列输出，其主要优点在于：各迭代环路迭代边界较小，可以大幅度提高生成速率；易于

表 5 基于 FPGA 的实现及对比

		传统方法	本文方法
资源占用	LUT	681(1%)	245(0%)
	Register	181(0%)	52(0%)
	BRAM	0(0%)	20(14%)
	DSP	27(12%)	0(0%)
生成速率		39.853 Mbps	449.236 Mbps
周期		2^{40}	2^{90}

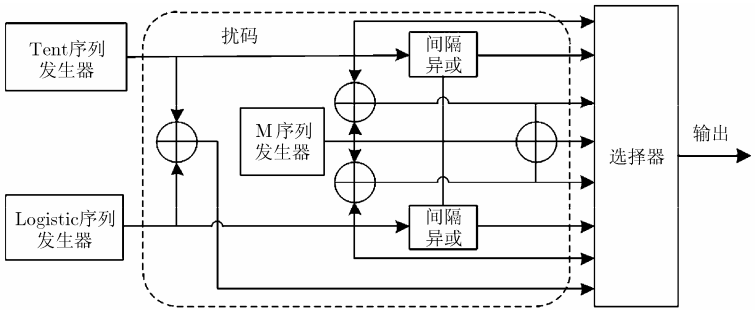

图 5 基于传统混沌序列生成方法的整体架构

做到极长周期扩展，只要增加迭代通道即可；多项式选择具有极大的自由空间；将大位宽计算用小位宽计算来代替且各通道独立并行计算，减小了实现复杂度并可以使用查找表实现，从而可进一步提高生成速率并提供灵活的可配置能力。在此基础上本文给出了基于 NIST 的测试，测试结果表明生成的序列具有良好的随机性能。基于 FPGA 的测试结果表明，相同设计平台下本文方法所生成的随机序列在速度方面是传统方法的约 11 倍，而周期却是传统方法的 2^{50} 倍；资源消耗方面，主要使用了片内存储器资源，但无需乘法器资源。

参 考 文 献

[1] NAWKHARE Rahul, TRIPATHI Amit, and POKLE Praveen. DS-SS communication system using pseudo chaotic sequences generator[C]. International Conference on Communication Systems and Network Technologies, Gwalior, 2013: 78–82.

[2] PEINADO A, MUNILLA J, and FÚSTERSABATER A. Optimal modes of operation of pseudorandom sequence generators based on DLFSRs[J]. *Logical Journal of IGPL*, 2016, 24(6): 933–943. doi: 10.1093/jigpal/jzw050.

[3] De Figueiredo F A P, MATHILDE F S, CARDOSO F A C M, *et al.* Efficient FPGA-based implementation of a CAZAC sequence generator for 3GPP LTE[C]. International Conference on Reconfigurable Computing and Fpgas, Cancun, 2014: 1–6.

[4] MANDAL K and GONG G. Feedback reconstruction and implementations of pseudorandom number generators from composited De Bruijn sequences[J]. *IEEE Transactions on Computers*, 2016, 65(9): 2725–2738. doi: 10.1109/TC.2015.2506557.

[5] SWAMI D S and SARMA K K. A logistic map based PN sequence generator for direct-sequence spread-spectrum modulation system[C]. International Conference on Signal Processing and Integrated Networks, Noida, 2014: 780–784.

[6] ZHOU Y, HUA Z, PUN C M, *et al.* Cascade Chaotic System With Applications[J]. *IEEE Transactions on Cybernetics*, 2015, 45(9): 2001–2012. doi: 10.1109/TCYB.2014.2363168.

[7] TALEB F. A new chaos based image encryption scheme using chaotic logistic maps[C]. International Conference on Multimedia Computing and Systems, Marrakech, 2014: 1222–1228.

[8] SHUNSUKE Araki, HIDEYUKI Muraoka, TAKERU Miyazaki, *et al.* A design guide of renewal of a parameter of the Logistic map over integers on pseudorandom number generator[C]. International Symposium on Information Theory and Its Applications (ISITA), Monterey, 2016: 781–785.

[9] CORINTO F, KRULIKOVSKYI O V, and HALIUK S D. Memristor-based chaotic circuit for pseudo-random sequence generators[C]. Mediterranean Electrotechnical Conference, Lemesos, 2016: 18–20. doi: 10.1109/MELCON.2016.7495319.

[10] OLIVER N, CORNELLES Soriano M, SUKOW D W, *et al.* Fast random bit generation using a chaotic laser: Approaching the information theoretic limit[J]. *Journal of Quantum Electronics IEEE*, 2013, 49(11): 910–918. doi: 10.1109/JQE.2013.2280917.

[11] CHESTER D B and MICHAELS A J. Digital generation of a chaotic numerical sequence[P]. Harris Corporation, Pub.US, No.20080263119A1.

[12] MICHAELS A J. A maximal entropy digital chaotic circuit[C]. IEEE International Symposium on Circuits and Systems, Rio de Janeiro, 2011: 717–720.

[13] 胡剑浩, 马上. 余数系统原理与在高速数字信号处理中的应用[M]. 北京: 科学出版社, 2012: 80–100.

[14] KHACHATRIAN G and KYUREGHYAN M. A new public key encryption system based on permutation polynomials[C]. IEEE International Conference on Cloud Engineering, Boston, 2014: 540–543.

[15] 孙琦, 万大庆. 置换多项式及其应用[M]. 哈尔滨: 哈尔滨工业大学出版社, 2012: 150–180.

[16] BASSHAM Iii L E, RUKHIN A L, SOTO J, *et al.* SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. *Nist Special Publication*, 2010.

[17] 许栋, 崔小欣, 王田, 等. 基于 Logistic 映射的混沌随机数发生器研究[J]. 微电子学与计算机, 2016(2): 1–6.
XU Dong, CUI Xiaoxin, WANG Tian, *et al.* Research on chaotic random bit generator based on Logistic map[J]. *Microelectronics & Computer*, 2016(2): 1–6.

马　上：　男，1978 年生，副教授，主要研究方向为通信信号基带处理、高速低功耗电路设计等.

刘剑锋：　男，1989 年生，硕士生，研究方向为大规模 FPGA 设计、伪随机序列等.

杨泽国：　男，1994 年生，硕士生，研究方向为通信信号处理、大规模 FPGA 设计等.