文章编号： 1000-5013(2012)04-0392-04

采用 Chen-Möbius 斜正交性的保密通信系统设计与仿真

吴春法，李国刚

（华侨大学 信息科学与工程学院，福建 厦门 361021）

摘要： 为克服传输线带宽受限的困难，利用 Chen-Möbius 变换生成的函数族的斜正交性设计一种高速保密的通信系统，并通过 DSP Builder 仿真平台验证了通信系统的正确性．采用高速 A/D 转换将各种信号都转换成数字信号，然后将串行的数字信号转换成 N 位一组的并行信号，每位信号(1 或 0)用一个特殊变换函数族的逆变换波形进行编码．输出时，这 N 位(或 N 个)编码波形是直接叠加在一起，从一条传输线上输出的，而在接收端，这些输出的信号被同时输入 N 个并行的信号判别端．每个判别端生成一个特殊变换函数的正函数信号与送入的 N 个编码波形的叠加进行正交积分运算，判别出每一位的数字信号．

关键词： Chen-Möbius 变换；斜正交性；正交积分；通信系统；数字信号

中图分类号： TN 919.72 **文献标志码：** A

20 世纪 90 年代以来，陈难先教授使用无穷级数的 Möbius 反演公式解决了一系列物理中的逆问题，引起国际学术界的高度重视[1-2]．苏武浔等[3-5]把 Möbius 变换运用于通信系统，通过对信号进行调制解调实现通信．近两年，该通信系统在现场可编程门阵列(field programmable gate array，FPGA)上实现了其硬件电路及语音通信领域的应用研究[6-7]．利用调制解调原理的通信系统把信号调制到频率较高的频带进行传输，提高了信号的抗干扰能力，但同时也限制了系统的使用范围，在传输线带宽受限情况下，信号将无法通过．本文利用 Chen-Möbius 变换生成的函数族的斜正交性，设计一种高速保密的通信系统，克服了传输线带宽受限的困难．

1 Möbius 函数性质

在数论中，Möbius 函数定义为

$$\mu(n)=\begin{cases}1, & n=1,\\ (-1)^r, & n\text{ 是 }r\text{ 个不同质数的乘积},\\ 0, & \text{其他}.\end{cases} \tag{1}$$

由式(1)可知：$\mu(n)$只取 1，−1，0 共 3 个值．故其前 10 个自然数的 Möbius 函数值分别为 $\mu(1)=1$，$\mu(2)=-1$，$\mu(3)=-1$，$\mu(4)=0$，$\mu(5)=-1$，$\mu(6)=1$，$\mu(7)=-1$，$\mu(8)=0$，$\mu(9)=0$，$\mu(10)=1$．

Möbius 函数的一个重要的特性为

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1,\\ 0, & n=2,3,4,\cdots.\end{cases}$$

其中：d 为 n 的因子，$\sum_{d|n}$ 为对每一个 n 的多个因子 d 求和(包括 1 和 n)．

例如，对于 $n=8$，有

收稿日期： 2011-12-22

通信作者： 李国刚(1973-)，男，副教授，主要从事密码学与集成电路设计的研究．E-mail：lgg@hqu.edu.cn.

基金项目： 福建省自然科学基金资助项目(A0640005)；中央高校基本科研业务费专项资金资助项目，国务院侨办科研基金资助项目(10QZR02)；福建省泉州市科技计划项目(2011G6)

$$\sum_{d|n}\mu(d) = \mu(1)+\mu(2)+\mu(4)+\mu(8) = 0.$$

若 $F(x)$为连续变量 x 的函数，且满足

$$G(x) = \sum_{n=1}^{\infty} F(\frac{x}{n}),$$

则有

$$F(x) = \sum_{n=1}^{\infty}\mu(n)G(\frac{x}{n}).$$

根据赫利条件，只要满足它的周期就可以展开成一系列正(余)弦函数的傅里叶级数，而 Chen-Möbius 变换正好实现把正(余)弦函数展开成周期函数信号.

2　新型 Chen-Möbius 变换通信原理

根据 $\widetilde{F}_K(\omega t)$和 $F(n\omega t)$正交的性质，可得

$$\frac{1}{\pi}\int_{\omega t=0}^{2\pi} F(l\omega t)\widetilde{F}_K(\omega t)\mathrm{d}(\omega t) = \delta_{k_1}.$$

其中：$F(\omega t)$为周期矩形脉冲信号、奇偶对称方波信号、奇偶对称三角波信号、锯齿波信号等周期信号的正信号；$\widetilde{F}_K(\omega t)$是通过 Möbius 逆变换与 $F(\omega t)$相正交的的逆信号. 这些正交周期函数族是现代数字通信技术中最常用信号，如方波 、矩形波 、三角波 、锯齿波，以及全 、半波余弦等的 Chen-Möbius 逆变换函数族[8-9].

通信模拟示意图，如图 1 所示 . 图 2 中：$\bar{s}_{d,n(t)}$为 Möbius 逆变换得到的 $\widetilde{F}_K(\omega t)$，$s_{d,n(t)}$为与 $\widetilde{F}_K(\omega t)$正交的 $F(\omega t)$，f_n 是要传送的二值数字信号. 在信号发送时，信号控制着正交周期波形发生器的开关；而在信号接收时，把这些数字信号作为解信号与接收信号分别进行正交. 当信号 f_x，f_y 的两位数值是 1，其他为 0 时，只有信号 f_x，f_y 控制的波形发生器产生波形，然后把两组波形相加合成混合信号. 接收端把接收的混合信号分别与 $s_{d,n(t)}$作卷积运算，根据正交定理，只有 $\bar{s}_{d,x(t)}$与 $s_{d,x(t)}$的卷积为 1，$\bar{s}_{d,y(t)}$与 $s_{d,y(t)}$的卷积为 1，结果与要传送的信号值相一致. 这就是通过 $\widetilde{F}_K(\omega t)$与 $F(\omega t)$的正交性质来实现通信的另一种高速保密的通信原理.

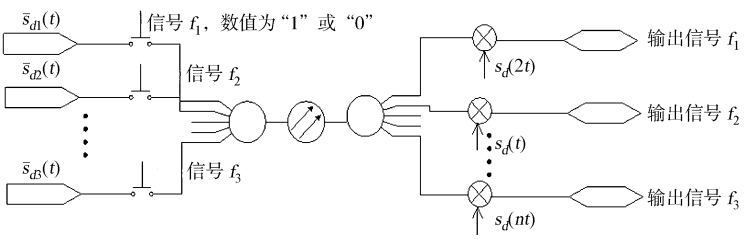


图 1　通信模拟示意图

Fig. 1　Simulation diagram of the communication

3　新型 Chen-Möbius 变换通信系统的仿真

根据 Chen-Möbius 变换通信原理，基于 DSP Builder 平台[10]设计得到的正交积分电路，如图 2 所示. 图 2 中：根据直接数字频率合成技术(direct digital synthesis，DDS)原理，5 阶锯齿波 sawtooth _jtb 和 sawtooth _jtb1 波形发生器模块分别输出不同频率的锯齿波 $F_1(\omega t)$，$F_2(\omega t)$；sawtooth _tzb 波形发生器模块输出与锯齿波 $F_1(\omega t)$正交的逆波 $\widetilde{F}_K(\omega t)$. sawtooth _tzb 波形发生器模块由子模块 subdds 与 sudds1 组成，根据调制函数表达式 $\widetilde{S}(t) = \sum_{m\backslash k} I(k/m)\sin(m\omega t)$，即 $k=5$ 时，m 只可能取 1，5 两个值才有意义，所以 5 阶锯齿波的 Möbius 调制信号波形表达式为

$$\widetilde{S}(t) = A[I(1)\sin(5\omega t)+I(5)\sin(\omega t)].$$

其中：subdds 与 sudds1 分别为上面两正弦波波形发生器模块.

把 sawtooth _jib 和 sawtooth _jib1 输出波形相加合成 $F(\omega t)$，然后与 sawtooth _tzb 输出的波形

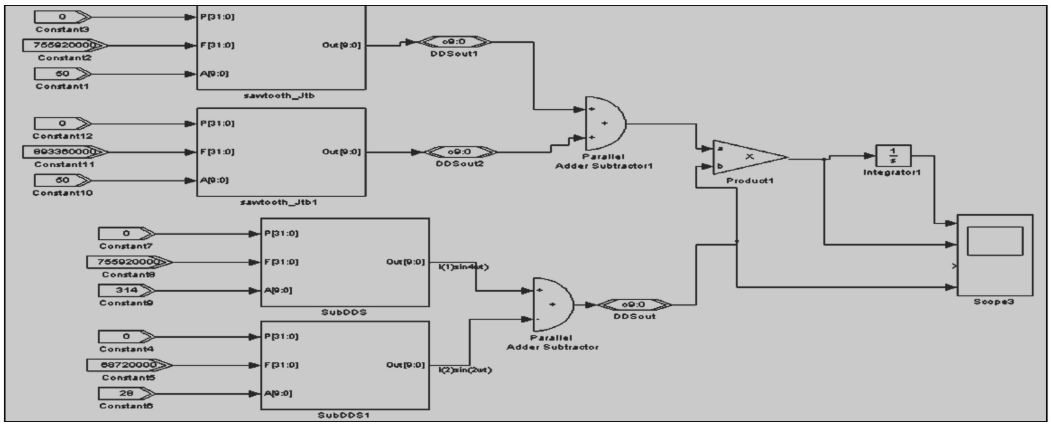
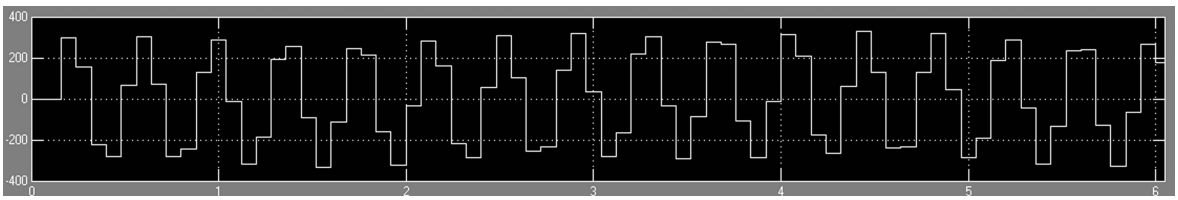


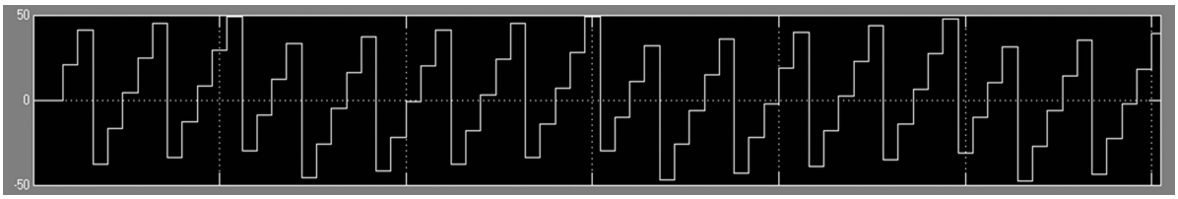
图 2 正交积分电路图

Fig. 2 Integration circuit of orthogonal integral

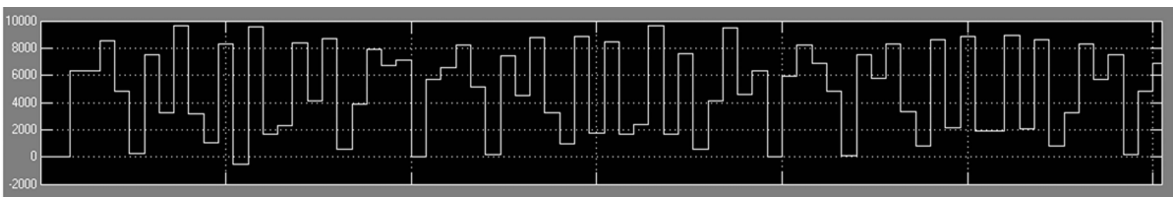
$\widetilde{F}_K(\omega t)$进行卷积($\widetilde{F}_K(\omega t) \cdot F(\omega t)$),以周期 T 为 5 μs 的方波为例进行仿真,结果如图 3 所示. 调制波与解调波的正交积分运算,如图 4 所示



(a) 解调波波形输出



(b) 调制波波形输出



(c) 调制波与解调波的乘积运算

图 3 周期 T 为 5 μs 的方波仿真波形图

Fig. 3 Square-wave simulation waveform at the period T of 5 μs

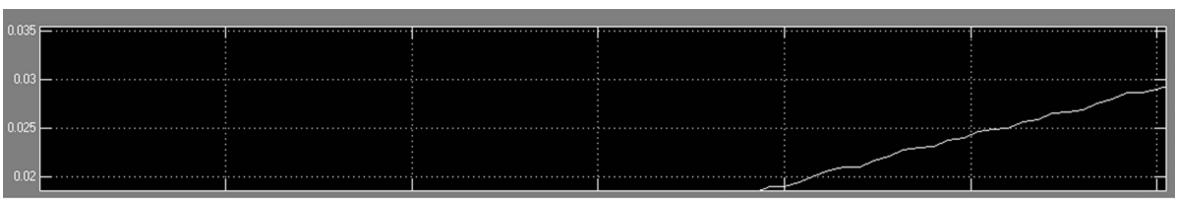


图 4 调制波与解调波的正交积分运算

Fig. 4 Orthogonal integral operator of wave from modulated and demodulated

在 T 时刻波形输出的结果为 2.5 μs,其值刚好是周期的一半,与 $\int_{t=0}^{T} F(l\omega t)\widetilde{F}_K(\omega t)\mathrm{d}(\omega t) = T/2$ 推演的结果相同. 因此,通过 DSP Builder 平台验证了提出的新型通信原理的正确性.

4　结束语

利用 Chen-Möbius 变换生成的函数族斜正交性设计出一种新型通信方式，并通过 DSP Builder 仿真平台验证通信系统的正确性，为进一步采用 VHDL 等硬件描述语言实现芯片化设计提供了理论基础. 为加强系统的保密性，在 N 个编码波形输出前，N 位一组的并行信号还可以乘以一个 $N\times N$ 的加密变换矩阵，将原先的 N 位数字信号转换顺序，而后将其用编码波形编码输出. 同时，提出的新方法在进行积分运算时需要严格的同步信号，增加了发送端和接受端的硬件开销，有待进一步改善.

参考文献：

[1] CHEN Nan-xian. Modified Möbius inverse formula and its applications in physics[J]. Phys Rev Lett，1990，64(11)：1193-1195.

[2] MADDOX J. Möbius and problems of inversion[J]. Nature，1990，344(6265)：377.

[3] 孙桂杰，苏武浔. Chen-Möbius 八路数字通信系统的性能仿真[J]. 华侨大学学报：自然科学版，2009，30(4)：384-388.

[4] 郭捷敏，王建成，苏武浔. Chen-Möbius 数字基带通信系统及其仿真[J]. 华侨大学学报：自然科学版，2006，27(1)：96-98.

[5] 林顺达，苏武浔. Möbiuss 变换在模拟通信中的应用与仿真[J]. 华侨大学学报：自然科学版，2006，27(1)：108-110.

[6] 曹炜. Chen-Möbius 通信系统的 FPGA 硬件实现与应用[D]. 泉州：华侨大学，2007.

[7] 许金龙，新型 Chen-Möbius 语音通信系统研究及 FPGA 设计与实现[D]. 泉州：华侨大学，2010.

[8] 苏武浔，张渭滨，王建成. 几种常见信号波形的逆变换计算(Ⅰ)：矩形脉冲与奇偶对称方波的逆变换[J]. 华侨大学学报：自然科学版，2005，26(1)：80-84.

[9] 苏武浔，张渭滨，王建成. 几种常见信号波形的逆变换计算(Ⅱ)：奇偶对称三角波与锯齿波和整流余弦波的逆变换[J]. 华侨大学学报：自然科学版，2005，26(4)：416-419.

[10] 潘松，黄继业，王国栋. 现代 DSP 技术[M]. 西安：西安电子科技大学出版社，2003.

Design and Simulation of High-Confidentiality Communication System Based on Chen-Möbius Oblique Orthogonality

WU Chun-fa，LI Guo-gang

(College of Information Science and Engineering，Huaqiao University，Xiamen 361021，China)

Abstract：To overcome the difficulties of limited bandwidth transmission in line，a high-speed confidentiality communication system is designed using the oblique-orthogonality of function sets evaluated by Chen-Möbius transform，and the correctness of the communication system is verified through DSP Builder simulation platform. By using the high-speed A/D converter，a variety of the signals are converted to digital signals，then，the serial digital signals are converted into a set of N-bit parallel signals，each signal (1 or 0) be coded by the inverse transform of a special transformation function sets evaluated by Chen-Möbius transform. When they been transmitted through the line，this N-bit (or N) encoded waveform is directly mixed together. At the receiver，these output signals are simultaneously put into N parallel discriminations of signal. When the N-bit (or N) encoded waveform was calculated by means of the orthogonality integral with each function set which was generated by the discriminations of signal，we can identify each of the digital signal.

Keywords：Chen-Möbius transform；oblique-orthogonality；orthogonality integral；communication system；digital signal

(责任编辑：钱筠　　英文审校：吴逢铁)