

伪码引信瞄准式欺骗性干扰及硬件实现

胡泽宾 赵惠昌

(南京理工大学电光学院 南京 210094)

摘要 该文首先介绍了伪随机码调相信信的工作原理, 提出了伪随机码调相信信瞄准式欺骗性干扰机方案, 并给出了各部分电路的原理及硬件实现, 主要包括伪码调相信信的解调、解调后的伪码序列的识别与重构、干扰波形的调制发射等关键部件。从各部分电路的试验结果来看, 本设计原理正确, 方案可行。

关键词 伪随机码, 调相信信, 干扰, 调制, 解调

中图分类号: TN972

文献标识码: A

文章编号: 1009-5896(2006)10-1817-03

Jamming of Spot and Deception of Pseudo-Random Code Phase-Modulation Fuze and Hardware Implemented Circuit

Hu Ze-bin Zhao Hui-chang

(School of Electronic Engineering and Optoelectronic Technology, NUST, Nanjing 210094, China)

Abstract Firstly, the working principle of pseudo-random code phase-modulation fuze is described in the paper. The scheme of spot and deception jammer of pseudo-random code phase-modulation fuze is given. The circuit principle of each part and its hardware implemented circuit are presented. It includes mainly that demodulation of pseudo-random code phase-modulation signal, recognition and reconstruction of demodulated code, modulation and transmission of interfered waveform. According to testing results of each part circuit, the designed principle is correct. The scheme is feasible.

Key words Pseudo-random code, Phase-modulation fuze, Jamming, Modulation, Demodulation

1 引言

伪随机码调相信信是利用伪随机 m 序列的自相关函数类似于白噪声相关函数的随机特性而工作的。该引信距离截止特性好、抗干扰能力强, 国内外对这种体制引信的研究已相当深入, 许多产品已投入生产和使用, 如配用于中型水面舰艇上的近程、低空、超低空的舰空导弹引信, 配用于对付飞机和导弹的地空导弹引信等。然而, 或许是研究尚未成熟, 或许由于保密的原因, 专门针对伪码调相信信及其复合引信的干扰机, 目前大部分也只是文字描述, 实际的干扰系统还未见到报道。

2 伪随机码调相信信原理^[1]

伪随机码调相信信原理框图如图1所示。各级信号如下(图1已表明位置)。

伪随机码调相信信发射信号:

$$U_t(t) = A_t m(t) \cos \omega_0 t \quad (1)$$

式中 $m(t) = \sum_{l=-\infty}^{\infty} \sum_{i=0}^{N-1} \text{rect}\left(\frac{t - T_c/2 - iNT_c}{T_c}\right) a(i)$ 为伪随机码

序列。其中 $\text{rect}(1/T_c) = \begin{cases} 1, & |t| \leq T_c/2 \\ 0, & \text{其它} \end{cases}$, T_c 为码元宽度, N 为

码字长度, $a(i) = \pm 1$, A_t 为发射信号的幅值, ω_0 为载波角频率。

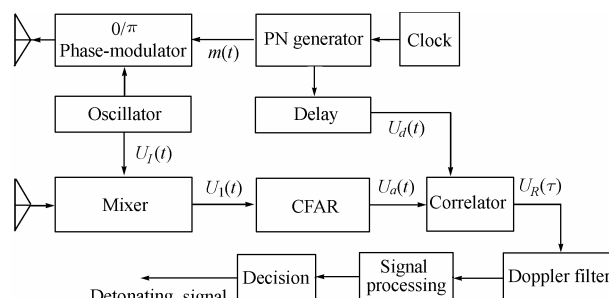


图1 伪随机码调相信信原理框图

Fig.1 Block diagram of pseudo-random code phase-modulation fuze
回波信号:

$$U_r(t) = A_r m(t - \tau_0) \cos(\omega_0 + \omega_d)t \quad (2)$$

式中 A_r 为回波信号幅值, ω_d 为多普勒信号角频率, τ_0 为发射信号延迟时间, $\tau_0 = 2(R - V_t t)/c$, 这里 R 为目标的距离, V_t 为目标相对于引信的相对运动速度, c 为光速。

混频器的输出信号:

$$U_i(t) = A_i m(t - \tau_0) \cos \omega_d t \quad (3)$$

式中 A_i 是混频后信号的幅值。

相关器的输出信号:

$$U_R(\tau) = R(\tau - \tau_0) \cos \omega_d \tau \quad (4)$$

式中 $R(\tau - \tau_0)$ 是伪随机码序列的自相关函数, τ 是本地伪随机码序列的预延迟时间。当 $\tau_0 = \tau$ 时, $R(\tau - \tau_0)$ 取得最大值。

信号处理电路是由峰值检波器、比较器和执行级组成, 如图2所示。 U_{com} 是归一化比较电平, 其值为 $0 < U_{com} < 1$ 。

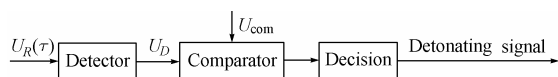


图2 信号处理电路的构成图

Fig.2 Block diagram of signal processing circuit

峰值检波器的输出 U_D 为

$$U_D = |U_R(\tau)| \quad (5)$$

当检波器的输出信号幅度大于或等于比较电平 U_{com} 时, 比较器输出启动电平, 触发执行级产生引爆信号。

根据上面的分析可知伪随机码调相引信的启动特性是由伪随机码序列的自相关函数(准确地说应是预先延迟的本地 m 序列与接收到的 m 序列的相关函数)决定的, 即引信在预定距离时检波器的输出信号幅度达到起爆电平, 引信正常起爆。因此作为干扰方, 在以下情况下都能使该引信非正常作用。

(1) 在引信预定距离之前检波器的输出信号幅度达到起爆电平;

(2) 在引信预定距离之前包括预定距离检波器的输出信号幅度达不到起爆电平, 而在预定距离之后达到起爆电平。

3 伪码引信瞄准式欺骗性干扰机硬件电路实现

伪码引信瞄准式欺骗性干扰采用先搜索、接收伪码引信信号, 对引信信号进行分析、识别, 再采用伪随机码调制, 在引信工作频率上实行欺骗干扰, 使引信早炸或使引信失去识别目标信号的能力, 从而无法启动并引爆战斗部。伪码引信瞄准式欺骗性干扰机原理框图如图3所示。

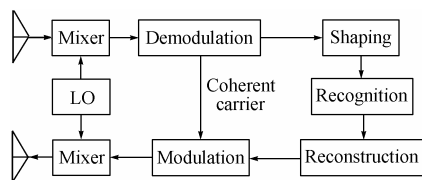


图3 伪码引信瞄准式欺骗性干扰机原理框图

Fig.3 Block diagram of spot and deception jammer of pseudo-random code phase-modulation fuze

3.1 相位解调电路的硬件实现

对伪随机码调相引信信号的解调可以采用相干解调和非相干解调。文献[2]介绍了一种非相干解调方法, 这种方法较好地克服了传统 BPSK 相干解调法解调时的“倒 π ”现象, 且无需恢复本地载波, 但这种方法需要事先知道码元宽度。而在引信对抗中, 伪随机码调相引信信号的码元宽度是未知的, 同时必须恢复同频同相的本地载波以充分利用干扰功率, 达到最佳干扰效果, 一般采用相干解调法。

伪随机码调相引信信号的载波频率一般在微波频段, 且确定的值未知, 一般是把接收到的伪码引信信号先和一个固定的频率混频, 再和一个扫频源混频, 得到一个固定中频, 然后解调。但这种方法在提取同频同相的相干载波时存在一定的麻烦, 需要两次混频两次滤波, 既增加了电路的复杂度, 也给滤波器的设计带来难度。能不能经过一次变频后, 在宽频段内直接解调呢? 答案是肯定的。

由文献[3]可知, Costas环不仅提取出已调信号的相干载波, 同时可以直接得到解调信号。这样可以简化硬件电路的设计, 用较少的器件组成调相信号的解调电路。正交解调集成电路(芯片1)内部包含了产生正交信号的电路和鉴相器, 再加一个乘法器(芯片2)和压控振荡器VCO, 环路滤波器就可构成基本的Costas环, 构成BPSK信号的解调接收系统, 如图4所示。

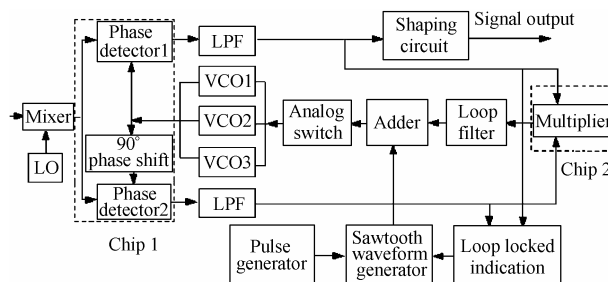


图4 解调电路的实现框图

Fig.4 The implementation diagram of demodulation circuit

由于伪码引信信号的载波频率变化范围很大, 单靠相位误差电压来改变变容管的电容值, 进而改变振荡器的频率很难达到要求, 所以需要外加电压到变容管两端。问题的关键是如何让这个两个电压同时控制变容管的电容值, 使得振荡源的频率变化范围与伪随机码调相信号的载波频率变化范围相一致, 在频率点上可以微调。解决的途径是外加电压以锯齿波的形式通过相加器加到变容管上, 在每个台阶上利用相位误差电压来微调变容管的电容值。

该电路经调试, 证明这一方案是成功的。图5给出了伪码调相引信信号解调电路的输出结果, 图中上下两个信号波形分别是原始伪随机码序列波形和解调得到的伪随机码序列波形。从图5可以看出, 解调得到的信号与原始信号相比有一个延迟, 这是由解调电路本身引起的。

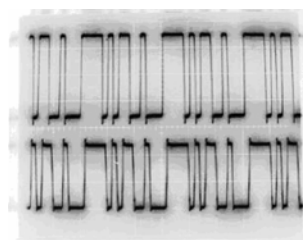


图5 解调电路的输出波形

Fig.5 The output waveform of demodulation circuit

3.2 识别与重构

3.2.1 识别 伪随机码序列是周期序列, 当产生 m 序列的移位寄存器的级数是 n 时, 其周期为 $2^n - 1$, 一个周期共有 $r = 2^{n-1}$ 个游程。每个伪随机码序列的周期都有一些不同长度的 1 或 -1 的游程组成, 对于一个周期序列的两个周期而言, 它们对应位上的值是相同的, 这也就意味着就游程而言, 他们对应位置上的游程也是相同的, 即第 1 个周期的第 1 个游程的长度和电平与第 2 个周期的第 1 个游程的长度和电平分别相同。因此, 以游程为单位接收伪随机码, 当接收到的游程数为偶数 $2r$ 时(r 是一个周期所含有的游程个数), 就必

然会出现前 r 个游程和后 r 个游程完全匹配的情况, 在这种情况下, 这 r 个游程代表的就是接收到的伪随机码序列。可见, 如果将这 r 个游程的信息储存下来就完成了识别的任务。

从上面的分析中可以看到, 要获得伪随机码序列的信息有两个步骤要走, 第一, 接收两个周期或两个周期以上长度的序列的信息 0 路的多少, 以及系统支持的最高工作时钟等参数都将受到 FPGA 器件的限制。在器件允许的前提下, 系统设计的原则是采用尽量高的采样时钟和容量尽可能大的 RAM, 因为这样可以识别速度更高和长度更长的伪随机码序列。

图 6 给出了以一定工作时钟频率和基于 FPGA 的一种伪随机码序列的识别方法。图 6 中, 虚线框内是由 FPGA 来实现的。整个系统的核心是个有一定长度和每一单元有一定比特容量的 RAM。整个电路的规模, 包括 RAM 的大小, 游程计数器的容量, 比较电路的多少, 以及系统支持的最高工作时钟等参数都将受到 FPGA 器件的限制。在器件允许的前提下, 系统设计的原则是采用尽量高的采样时钟和容量尽可能大的 RAM, 因为这样可以识别速度更高和长度更长的伪随机码序列。

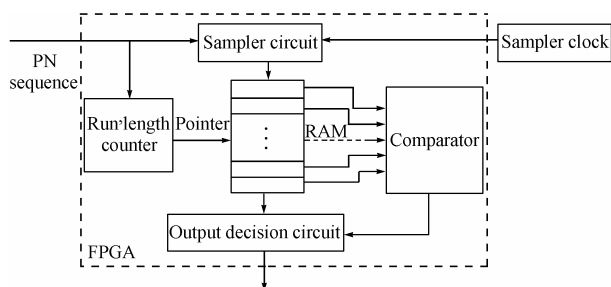


图 6 伪码序列识别电路原理框图

Fig.6 Block diagram of recognition circuit of pseudo-random code sequence

3.2.2 重构 图 6 中的输出判决电路的输入信号是整个 RAM 的数据和比较电路提供的控制信号。判决电路根据控制信号选择哪些 RAM 单元中的数据应该作为输出, 并且将其不断地循环输出。当一个周期的所有游程全部发射完毕之后, 就从第 1 个游程开始重新发射, 发射过程就是如此周而复始地进行。

然而作为干扰方, 对方引信的本地伪随机码序列的预延迟时间 τ 是未知的, 要想成功干扰掉引信, 识别后的伪随机码序列必须有一个适当的延迟。实际中, 我们这样做: 把存储的一个周期内的伪随机码序列按照一定的规律顺次延迟一段时间, 每次延迟一段时间后都连续送几个周期的伪随机码序列到调制电路, 调制后发射。

3.3 调制电路

经识别重构后的伪随机码序列和原引信的伪随机码序列大致一致, 用它调制同频同相的本地载波再去干扰该伪随机码调制引信, 就容易干扰掉。因为识别重构后的伪随机码序列与对方引信预延迟的本地伪随机码序列相关性好, 相关输出大于比较电平, 可以使敌方引信早炸, 达到成功干扰的目的。

利用现有的集成电路 $0/\pi$ 调相器(芯片 1)、极性变换器(芯片 2)、传输线变压器和简单的外围电路, 就可以实现伪随机码调制电路的硬件实现, 电路框图如图 7 所示。

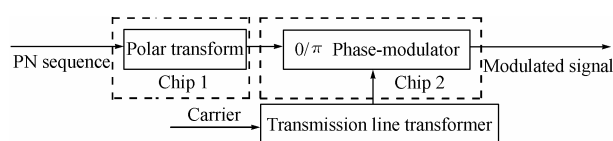


图 7 伪随机码调制电路框图

Fig.7 Block diagram of pseudo-random code phase-modulation circuit

图 7 中 $0/\pi$ 调相器(芯片 1)要求输入的调制信号高电平为 1.2V, 低电平为 0.7V, 而识别重构后输出的伪随机码序列信号一般为 TTL 电平, 不符合其输入电平的要求, 所以要对输入信号进行一次电平变换, 才能把整形延迟后的伪随机码序列送到 $0/\pi$ 调相器中去, 这里用极性变换器(芯片 2)来完成电平变换。另外 $0/\pi$ 调相器(芯片 1)要求输入的载波信号为平衡输入, 这样就需要一个传输线变压器来完成不平衡到平衡的转换。图 8 给出了通过频谱仪观测到的伪随机码调制信号的实际频谱。

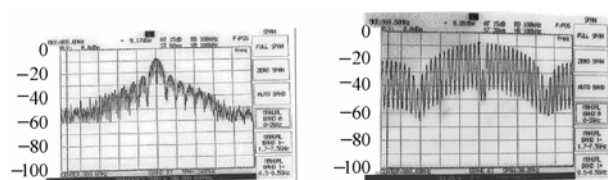


图 8 伪随机码调制信号实际频谱

Fig.8 The spectrum of pseudo-random code phase-modulation signal

由图 8 可以看出: (1)从载波抑制上看, 调制波形的载波抑制为 15dBm 以上, 达到设计要求。(2)信号输出幅度在 -10dBm 左右, 而实际要求在 0dBm 左右, 可以通过加一级放大器得到。

4 结束语

瞄准式欺骗性干扰是对伪随机码调制引信的有效干扰方式之一, 本文重点分析了其硬件电路的实现, 从各部分电路的试验结果来看, 本设计原理正确, 方案可行。同时整个系统调试正常, 达到了预先要求的干扰效果。

参考文献

- [1] 张居正. 伪随机码调制引信原理与设计[J]. 制导与引信, 2000, 21(3): 1-7.
- [2] 李世银等. 2PSK 非相干解调原理研究[J]. 中国矿业大学学报, 2003, 31(3): 315-318.
- [3] 王钢, 刘毅鹏. BPSK 载波同步技术的研究[J]. 通信技术, 2003, (1): 21-23.

胡泽宾: 男, 1980 年生, 硕博连读生. 从事无线电引信干扰与抗干扰技术、信号调制解调方面的研究。

赵惠昌: 男, 1958 年生, 教授, 博士生导师. 主要从事无线电引信系统、无线电引信干扰与抗干扰技术研究. 近 5 年来, 在各类刊物、学会上独立或合作发表论文近 50 篇。