混沌保密通讯的探索

摘要：利用蔡氏电路产生混沌信号，通过覆盖的方法对初始信号进行加密，将两混沌信号同步，利用减法器对混合信号进行解密，以达到保密通讯的效果。

关键词：混沌，保密，加法器，减法器

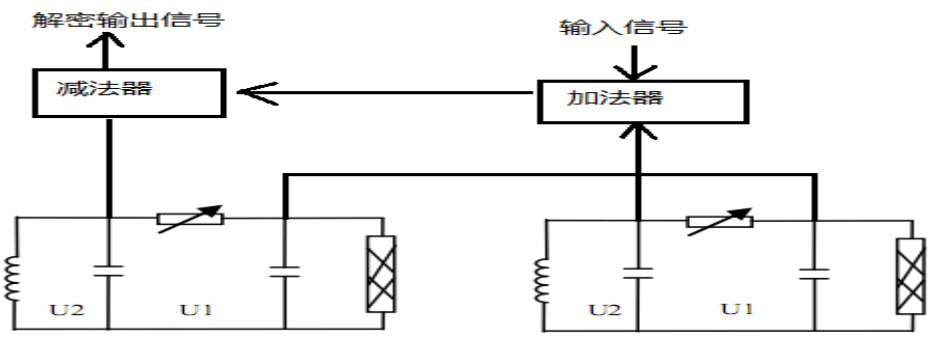
引言

近年来物理学家对混沌这一非线性物理问题进行了深入的讨论与研究。1990 年，美国海军实验室专家 Pecora 和 Carroll 提出了混沌同步概念及其驱动——响应方法。他们将系统分成两个子系统，即驱动子系统和响应子系统，先对响应子系统进行复制，然后用驱动子系统产生的信号驱动该复制的系统以实现同步。后来，通过进一步的研究，许多学者开始利用子系统之间的相互耦合来实现混沌同步，对混沌保密通讯等应用方面的研究也受到了更多的关注。本文将简要介绍混沌保密通讯的原理以及实现过程。

实验原理

混沌现象指的是一种确定的但不可预测的运动状态。它的外在表现和纯粹的随机运动很相似，即都不可预测。但和随机运动不同的是，混沌运动在动力学上是确定的，它的不可预测性是来源于运动的不稳定性。或者说混沌系统对无限小的初值变动和微扰也具于敏感性，无论多小的扰动在长时间以后，也会使系统彻底偏离原来的演化方向。

混沌保密通讯正是利用了混沌的这种不可预测性。首先通过一个混沌系统驱动另一个混沌系统，实现系统间的同步。然后利用加法器将混沌信号覆盖到需要保密的信号上，传输到目的地之后，再利用减法器将同步混沌信号减去，解密出初始信号，这就是一个简单的混沌保密过程。下图是一个示意图：



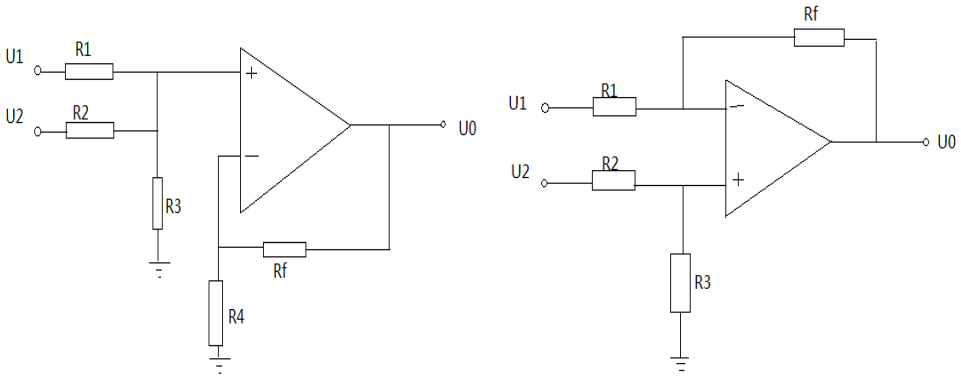
图中利用简单蔡氏电路产生混沌信号。

实验过程

搭建加法器和减法器：加法器和减法器由一个运算放大器和五若干电阻组成。说到运算放大器，就不得不介绍一下运放的虚短和虚断。因为理想运放的电压放大倍数很大，而运放工作在线性区，是一个线性放大电路，输出电压不超出线性范围（即有限值），所以，运算放大器同相输入端与反相输入端的电位十分接近相等。在运放供电电压为±15V 时，输出的最大值一般在 10～13Ⅴ。运放两输入端的电压差，在 1mV 以下，近似两输入端短路。这一特性称为虚短，这显然这不是真正的短路，只是分析电路时在允许误差范围之内的合理近似。

由于运放的输入电阻一般都在一百兆欧左右，流入运放同相输入端和反相输入端中的电流十分微小，比外电路中的电流小几个数量级，流入运放的电流往往可以忽略，这相当于运放的输入端开路，这一特性称为虚断。显然，运放的输入端不能真正开路。运用“虚短”、“虚断”这两个概念，在分析运放线性应用电路时，可以简化应用电路的分析过程。

下图是减法器和同相加法器的示意图：



利用运放虚短（$U_+ = U_-$）和虚断（$I_+ = I_- = 0$）的特性，就可以分析加减法器的输入与输出之间的关系了。

对于加法器

$$\frac{U_1 - U_+}{R_1} + \frac{U_2 - U_+}{R_2} = \frac{U_+}{R_3}$$

$$\frac{U_-}{R_4} = \frac{U_0 - U_-}{R_f}$$

$$U_0 = \frac{(R_4 + R_f)(U_1 R_2 R_3 + U_2 R_1 R_3)}{R_4(R_1 R_3 + R_2 R_3 + R_1 R_2)}$$

同理，对于减法器有

$$U_0 = \frac{U_2 R_3 (R_1 + R_f)}{R_1 (R_2 + R_3)} - \frac{U_1 R_f}{R_1}$$

实验里，我们的加法器中$R_1 = R_2 = R_3 = R_4 = \frac{1}{2} R_f = 83\text{k}\Omega$ ，减法器中$R_1 = R_2 = R_3 = R_f = 83\text{k}\Omega$ ，所以家发起的输出电压为

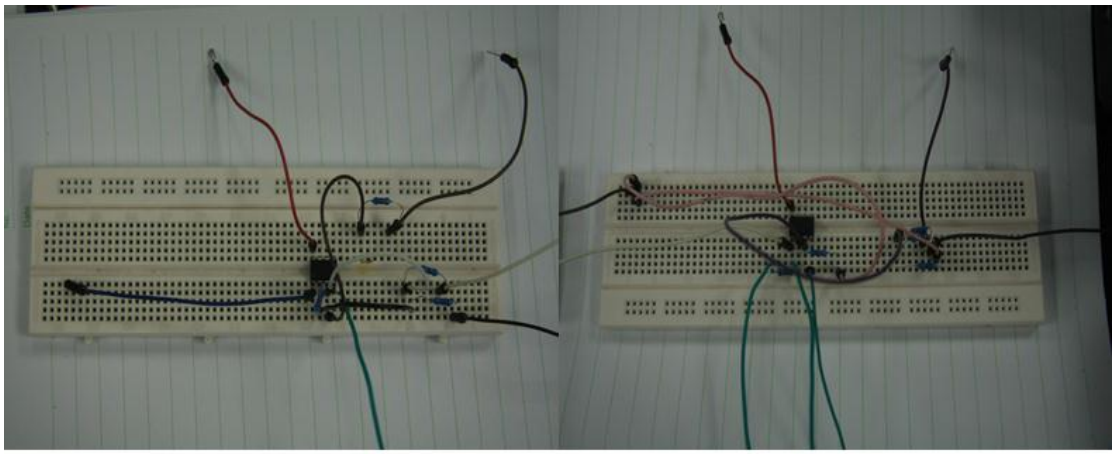
$$U_0 = U_1 + U_2$$

减法器的输出电压为

$$U_0 = U_2 - U_1$$

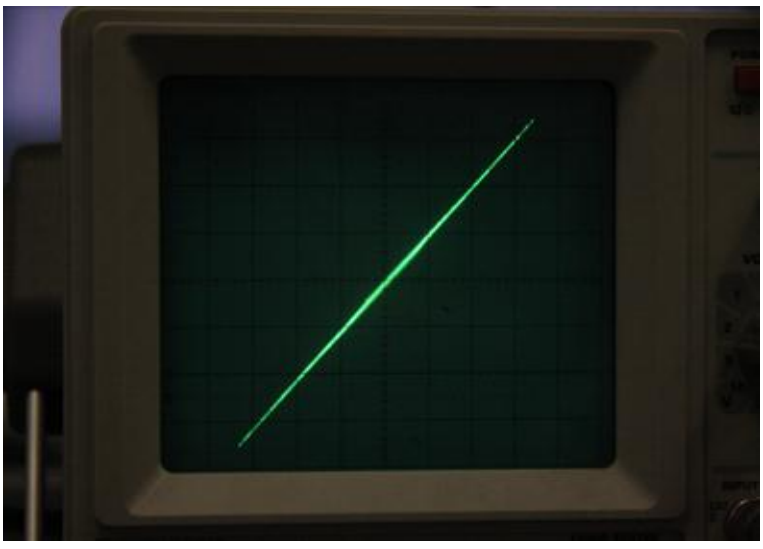
加减法器对输入电压没有放大或缩小效果。

下图是我们搭建的实物图：



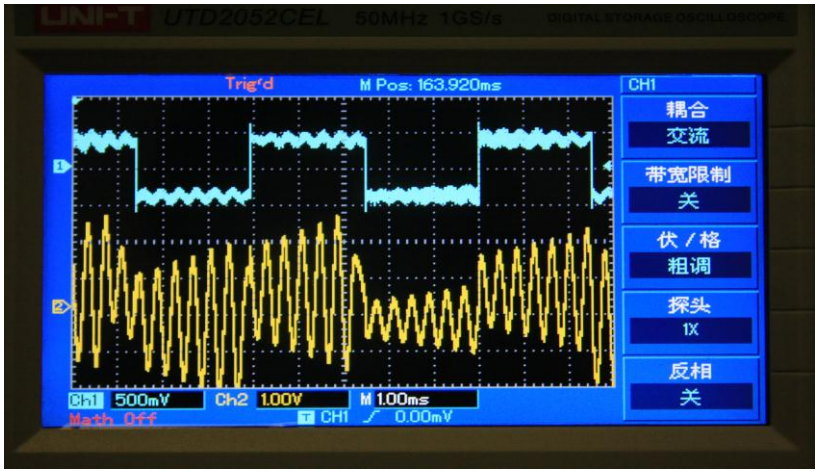
减法器　　加法器

将其接入电路中，并将运放工作电源接好，就可以用示波器观察输入输出信号，通过对示波器信号的观察，调节蔡氏电路参数，达到同步的效果。下图是我们观察到的同步信号李萨如图：



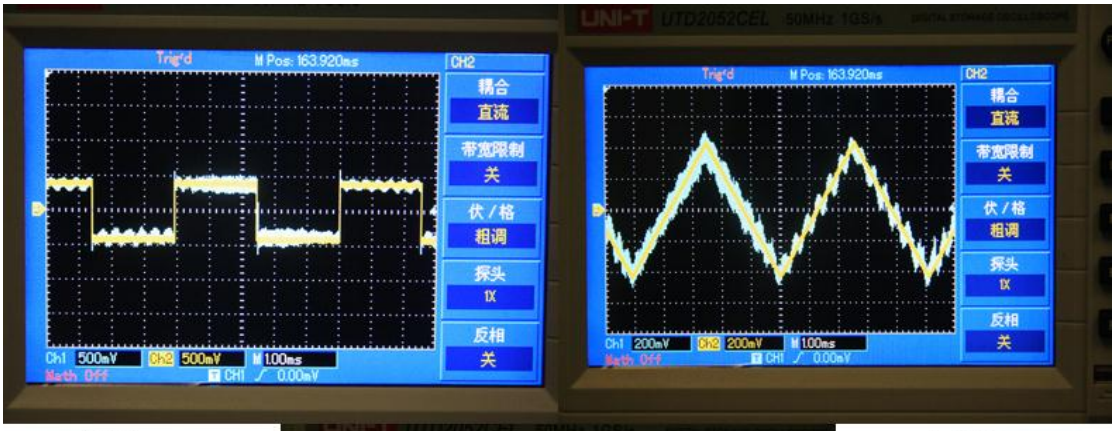
信号的调幅档位相同，相图成 45 度角，说明输入的两个信号同步很好。

下图是解密后的信号加密后的信号对比：



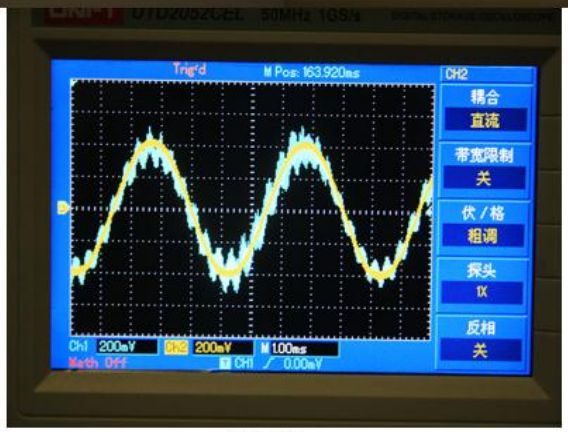
加密后已经完全看不出方波信号，加密效果较好。

然后分别对方波、三角波、正弦波进行实验，得到以下是保密前和解密后的信号对比：



方波

三角波



正弦波

从图像可以看出，整体上，还原度较高，细节上有一些缺陷，做加减法之后不完全相同，考虑到电阻的选取不一定准确，万用表测得的值精确度不够，同时线路上有些地方的相接使

用的夹子可能导致接触不良。使用更精确的电阻和电路应该可以得到更完美的结果。

小结

利用混沌覆盖的方法，经过加密后，原有信号对他人基本上不可预测，保密性较好。利用同步的方法解密信号，可以再次得到原来的输入信号，信号对己方可见。说明混沌通讯有保密的效果，可以进一步的开发利用。

致谢

感谢指导实验并热情提供帮助的乐永康老师以及搭档於逸骏同学。

参考文献

1、《近代物理实验补充讲义》复旦大学物理教学实验中心。

2、http://phylab.fudan.edu.cn，复旦物理实验中心保密通讯部分。

3、蔡氏混沌电路的单向耦合同步研究，蒋国平、王锁平。