混沌理论在密码中的应用

北京电子科技学院赵耿

二、研究技术水平和创新点

研究水平

技术水平

创新点

2　国内完成在PSTN网络上的混沌密码样机和试验

二、研究技术水平和创新点

研究水平

技术水平

创新点

2 国内完成在PSTN网络上的基于混沌分组密码样机和试验

- 连续流混沌产生器的实现技术
- 离散点混沌产生器的实现技术
- 混沌噪声源作为密钥产生源技术
- 广义一次一算法的分组密码设计和实现

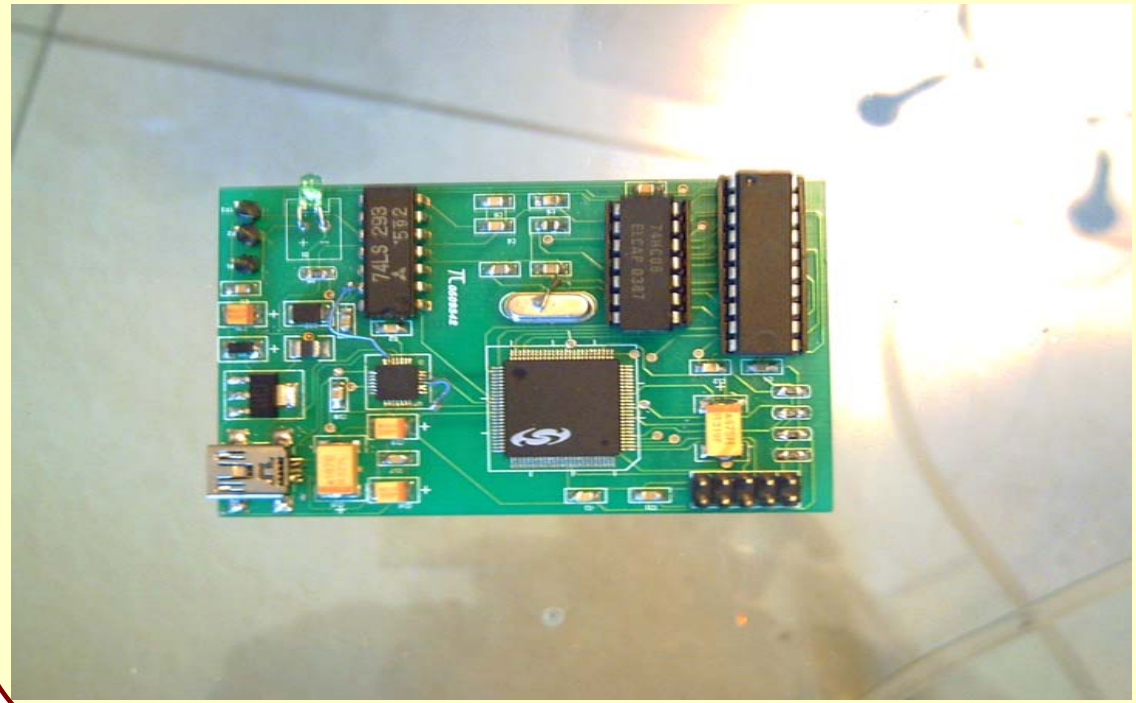
二、研究技术水平和创新点

研究水平

技术水平

创新点

3　国内首个混沌噪声源原理样机和试验



二、研究技术水平和创新点

研究水平

技术水平

创新点

3 国内首个混沌噪声源原理样机和试验

- m序列扰动提速技术
- 集成电路模拟非线性器件技术

二、研究技术水平和创新点

研究水平

技术水平

创新点

（1）建立起国内第一个较为系统的混沌密码理论体系。从混沌电子学、混沌复杂性、混沌产生器，混沌同步密码通信，混沌密码算法理论到混沌噪声源都作了较为详尽的研究，全面和系统的研究，其本身就是一个创新。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（2）按混沌种类和实现方式归类和分别定义了不同类型和不同方式的混沌通信和混沌产生器。提出了连续流、数字流、离散点混沌产生器的理论。定义了模—模，模—数—模，数—数混沌密码通信的概念。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（3）提出并建立了模—数—模混沌密码通信中的时钟间隔脉冲驱动同步理论。并在样机中予以实现验证。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（4）提出并建立了数一数密码通信中的环形缓存自然丢失加解密同步算法。并应用于商密SHS06数字电话密码机。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（5）设计并实现了一个电路混沌噪声源，并在理论上作了验证和混沌链路密码机中予以实现验证，并已准备集成化。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（6）初步建立了混沌密码的编码理论，并在此基础上，提出了的“广义一次一算法”的设计思想，并在实验样机和实验电路中实现和仿真验证。

二、研究技术水平和创新点

研究水平

技术水平

创新点

（7）定义了C（Ch aos）序列的概念，并在文件加密系统为蓝本编制了仿真程序来验证，作为序列密码的一种设计方式，并在商密SHS06数字电话密码机中的系统密钥管理中得到使用。

三、社会效益和推动科技进步

社会效益

科技进步

商密SHS06密码机

三、社会效益和推动科技进步

社会效益

科技进步

四、近期和后续研究工作

理论研究

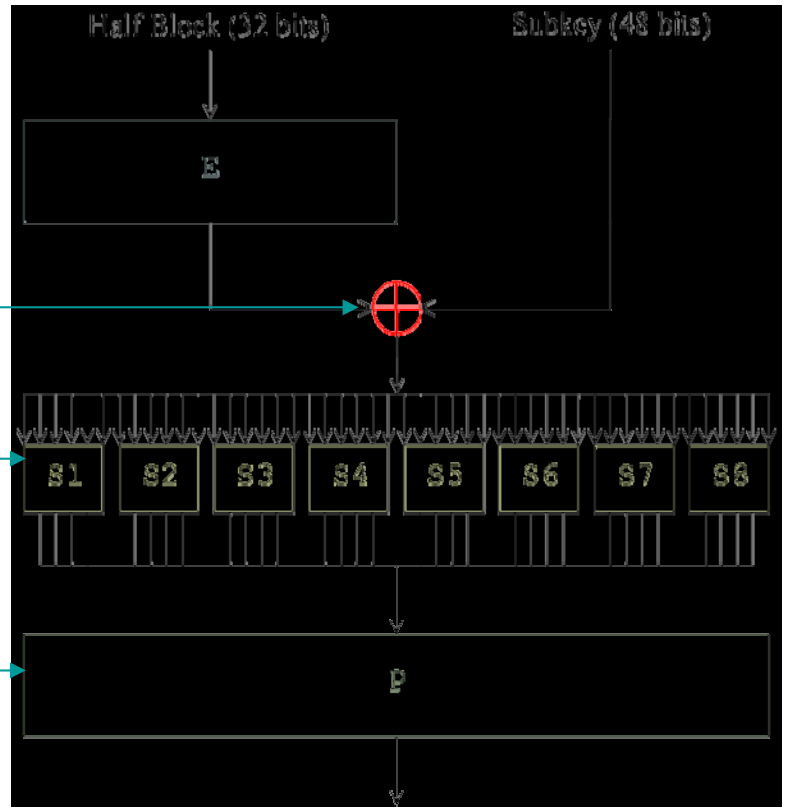
1.混沌密码与常规密码的比较性研究

应用研究

混沌密码与传统密码的比较

混沌映射

（性能指标
的对比，
比如
密钥空间，
混沌生成S盒
的非线性，
差分均匀性，
P盒的扩散性，
加密速度，）



用混沌生成的密码学部件究竟好不好，快不快，是否安全，是否可实现，性能怎么样？