混沌理论在密码中的应用

北京电子科技学院赵耿

汇报提纲

一、 项目背景和总体思路

二、研究技术水平和创新点

三、社会效益和推动科技进步

四、近期和后续研究工作

一、项目背景和总体思路

项目背景

总体思路

计算机网络技术的飞速发展和广泛应用，使得密码理论与技术有了空前的繁荣。

一、项目的立项背景和总体思路

项目背景

总体思路

与此同时，密码攻击方法和手段也在同步发展，这促使人们不断寻求新设计方法的基础上，还得进一步探索发展新的密码理论与技术，近年来对量子密码、生物密码等等的研究热潮就是最好的例证。

一、项目的立项背景和总体思路

项目背景

总体思路

混沌密码：由于混沌自身的优良特性，在军事战争、国家安全、通信对抗等方面都具有潜在的重要应用价值，因此，混沌密码正受到各国军事及安全部门的高度重视。

一、项目的立项背景和总体思路

项目背景

总体思路

自从90年美国海军实验室的Pecora—Carrol发现电路中的混沌自同步以来，利用混沌来实现秘密通信已成为近年来竞争最为激烈的混沌应用研究领域。

一、项目的立项背景和总体思路

项目背景

美国陆军实验室、麻省理工学院、马里兰大学、华盛顿洲立大学、休斯顿大学、俄罗斯科协无线工程电子学会及莫斯科物理技术研究所、英国甘地夫威尔斯大学及新汉普郡大学、德国哥丁根大学、意大利Di Lescce大学、瑞士联邦技术研究所等等均有许多科学家竞相参与竞争，各自加紧研究新的混沌密码系统，有效的信号处理等技术。因此混沌密码通信技术已被列入美国国防研究计划，正在加紧秘密研究之中。

总体思路

一、项目的立项背景和总体思路

项目背景

总体思路

因此, 从1998年起到2001年我们开始做前期准备工作, 学习有关理论和知识.

2001年开始在北京电子科技学院科研基金的支助下, 正式开始了立项研究. 并先后获得10项国家自然科学基金的中办、总参预研项目 的资助.

一、项目的立项背景和总体思路

项目背景

总体思路

混沌由确定性动力系统产生，具有有界性、非周期性、对初始条件的极端敏感依赖性，而这几种性质正是密码所要求的。混沌具有有界性，这意味着混沌是可控的，而且也是可观测和可实现的；混沌具有非周期性，这表明它具有宽的频带和类噪声的特点，基于此，正好用其掩盖所要传送的通信信息，使这些信息看起来像是宽带的噪声一样难于提取；对初始条件的敏感依赖性说明混沌信号具有长期不可预测性。

一、项目的立项背景和总体思路

项目背景

总体思路

由于对初始条件的极端敏感，任意小的初始条件的变化都会导致一组完全不同的混沌密码，因此，一个混沌动力学方程所代表的密码序列有无限多个，密码序列的长度从理论上来说是无限长，而且便于控制和操作，从而混沌密码可以成为一种新的、性能良好的密码资源，以代替和补充传统的密码技术，作为加密数据的密码或密码的密码和噪声源等。

一、项目的立项背景和总体思路

立项背景

总体思路

另外，可随意通过增加混沌的维数使其具有多个李亚普诺夫指数，也可通过多个混沌动力学方程的不同组合改变其奇怪吸引子来改变混沌密码的复杂度，提供从商密到核密的不同级别密码。再者，连续流混沌也提供了可能的一种物理噪声源。

一、项目的立项背景和总体思路

项目背景

混沌密码研究的主要困难问题在于：第一，混沌同步的困难性；第二，混沌算法的复杂度分析；第三，混沌密码的编码方法；第四，混沌噪声源的研究。

总体思路

因此，本项目的研究目标是：在理论方面，对混沌的同步、混沌算法复杂度分析、密码编码方法，混沌噪声源等进行深入研究；在应用方面，研制混沌同步，密码，噪声源三类原理试验样机。从而为混沌密码用于密码通信做好理论研究和实际应用准备。

二、研究技术水平和创新点

研究水平

技术水平

创新点

该项目属密码前沿理论中的混沌密码理论研究范畴，项目组努力按照现代密码学的思想建立起混沌密码学的理论。该项目研究难度大，在该领域，国内尚无单位做如此全面、系统、长期的研究工作，且取得了丰硕的成果。项目组成员获得国家专利五项，受理国防发明专利一项；发表较高水平论文202篇，其中，发表SCI和EI检索的论文103篇；出版专著1部；研究成果和综合研究能力达到国际同类先进水平。

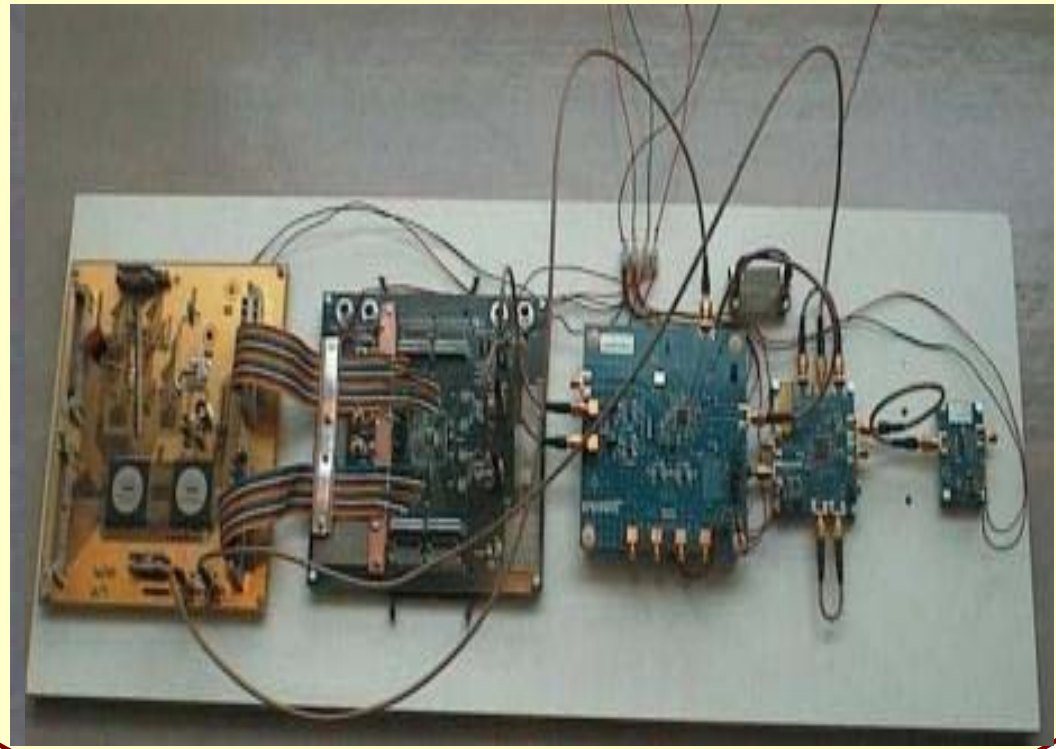
二、研究技术水平和创新点

研究水平

技术水平

创新点

1　国内完成混沌同步密码通信样机



二、研究技术水平和创新点

研究水平

技术水平

创新点

1　完成真正意义上的混沌同步密码通信样机和试验

- 环形缓存自然丢失加解密同步技术
- 数字流混沌产生器实现技术
- 时钟间隔脉冲驱动同步技术