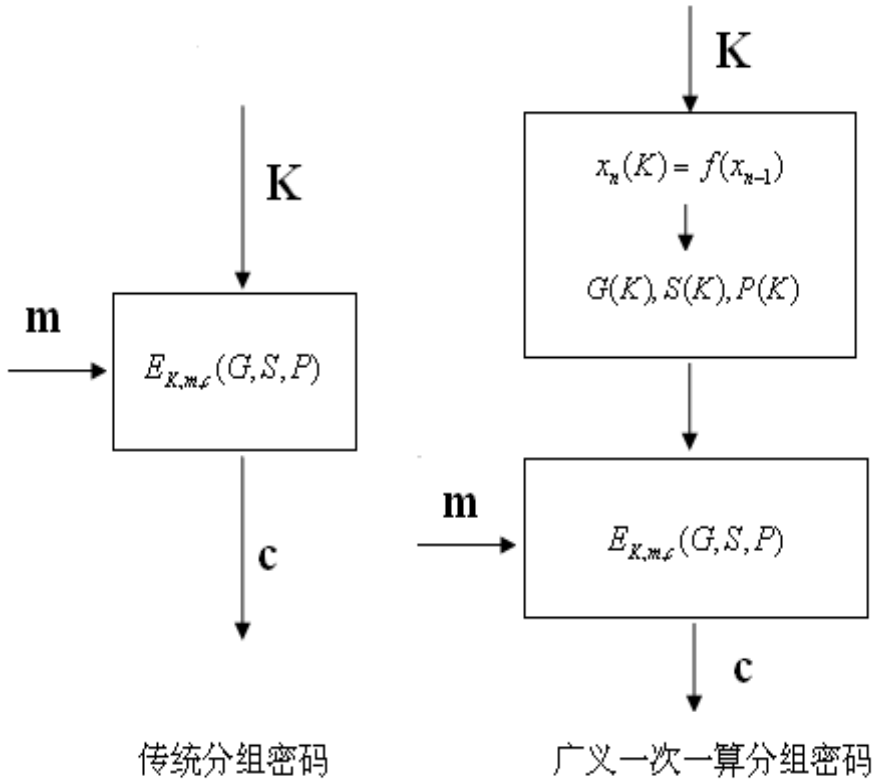
混沌密码与传统密码的比较



四、近期和后续研究工作

理论研究

2.基于混沌的公钥密码算法研究

应用研究

基于混沌的公钥密码算法研究

	特点	优点	缺点	应用
对称密码体制	加密密钥与解密密钥相同。对称密码体制的保密性主要取决于密钥的保密性，与算法的保密性无关	加密速度快 安全强度高	密钥的管理与分配的安全性很难保障	主要用于加密数据、消息认证
非对称密码体制	加密密钥与解密密钥不同，一个密钥公开，用于加密；另一个密钥保密，用于解密。加密运算和解密运算分离。	通信双方无须事先交换密钥就可以建立保密通信。解决了密钥分配的问题。	运算速度相比对称密码算法来说很慢	主要用于数字签名、秘密共享、认证功能、密钥管理以及保密通信

基于混沌的公钥密码算法研究

利用Chebyshev映射的的半群特性和混沌特性，以数学上离散对数求解的难题作为安全保证，以ElGamal公钥密码算法为蓝本，提出基于Chebyshev映射的类ElGamal公钥密码算法　和Hash算法.

四、近期和后续研究工作

理论研究

应用研究

1. 混沌噪声源集成电路研制

1 混沌噪声源集成电路研制

- 混沌对初始条件和参数的极端敏感性以及混沌模拟电路难于精确控制和预测的原因，使其同时也特别适用于作为噪声源芯片，电路元器件参数的离散性使其不可能作出输出一致的噪声源。研究一种可集成的混沌噪声源电路。研究出一种基于混沌的高速噪声源，用作各种密码机的会话密钥发生器.
- 为保证噪声源的随机性，通常源电路应采用模拟电路，为了实现高速性，通常采用数字电路，本课题将研究模拟数字集成的噪声源集成电路，研究集成的混沌高速噪声源电路芯片。
- 用混沌设计高速噪声源是可能的，但如何设计能降低集成成本，从而又使外部器件最少，还能在单一低电源电压下高速工作。

四、近期和后续研究工作

理论研究

应用研究

2 基于快速混沌密码加密的会议视频系统

四、近期和后续研究工作

理论研究

应用研究

3. 单芯片语音密码机的研制

3 单芯片语音密码机的研制

- **1)**高保真度语音压缩和编解码问题研究
- 语音压缩编码在单芯片话密机的研制中占有及其重要的地位，语音压缩编码既决定了整个话密机的通话质量，又能尽可能降低数据的传输量。而话密机中现用的语音压缩编码大都是通用型的，没有特别的针对性。该课题先实现几种国际标准的语音压缩编码，然后根据需要，优化其代码，并对其进行改进，以达到既有良好的压缩率代码执行效率，又使之具有较高的实用性。研究分析现有语音压缩编码标准；优化DSP中的语音压缩编码，使之符合传输的要求；改进现有的语音压缩编码标准，使之符合单一芯片语音密码机的应用环境。

3 单芯片语音密码机的研制

- **2）低误码率调制解调算法及接口研究**
- 主要研究内容包括：研究单一芯片语音密码机的调制解调特性；对现有广泛使用的几种调制解调标准协议分析，作重研究V.22,V.22bis,V.32,V.32bis,V.34以及具有纠错压缩技术的V.42和V.42bis；研究现有的自适应技术和各自的性能和研究现有的均衡技术。通过研究和实验做出改进，使其适合于单一芯片语音密码机的低误码率应用环境，完成调制解调模块算法及接口的研究和实验。

3 单芯片语音密码机的研制

- **3）高安全性单芯片密码算法及同步的研究**
- 已公开的分组密码算法不是安全度不高，就是仅适合在专门密码芯片上实现的算法，在单一DSP芯片全双工多任务情况下，必然要求高安全性和高速的统一，而二者往往又是矛盾的双方，因此研究安全高速的密码算法（包括密码同步算法）是一个重点研究内容。

3 单芯片语音密码机的研制

- **4）密码机的体系结构及实现方法研究**
- 研究拥有何种速率，拥有何种接口环境的DSP芯片，以及外围接口电路才能满足单一DSP芯片语音密码机的要求也是研究的一个方面。

3 单芯片语音密码机的研制

- **5）单一DSP芯片下的多任务调度算法研究**
- 对于单一芯片语音密码机而言，其重点和创新点是要将声码器、加解密算法、调制解调器三部分一体化。DSP在整个系统中除了扮演微处理器的角色之外，还兼有控制器的功能，DSP对外部数据采集的操作是整个系统的一部分，为了更有效使用DSP资源，考虑多任务的调度和切换，因此单芯片语音密码机中三部分之间通信链路的建立以及各个任务调度也是一个重点研究内容。

3 单芯片语音密码机的研制

- **6）通信双方建链时的密钥头和安全通信协议研究**
- 仅有安全度高的密码算法并不能保证整个系统的安全，密钥传递和安全通信协议是信息安全的另一重要保障体系，本课题也将研究和实现在单一芯片下的语音密码机的密钥头传递和安全通信协议。

谢谢大家！