数字移动通信系统保密技术

关 键 词：移动通信系统　保密通信　数字通信

所属年份：2005	成果类型：应用技术
所处阶段：	成果体现形式：
知识产权形式：	项目合作方式：
成果完成单位：西安电子科技大学	

成果摘要：

一、成果内容简介、关键技术、技术经济指标：1.攻关任务研究用于用户身份认证和通信保密、符合GSM建议的3个关键算法A3、A8、A5，完成选型设计及A5算法的C25芯片实现。2.主要技术指标及考核目标：(1)用户身份认证和加密密钥生成算法A3、A8：①实现算法的环境或资源为带(8信)CPU的智能卡；②实现二算法A3、A8的时限为500ms；③算法的安全性。以上指标可采取模拟方式证明。(2)通用数据加密算法A5：①实现算法的环境或资源为TMS320C25数字信号处理器；②要求算法的数据加密速率达到114b/0.5ma，相当于228kb/s；③算法的安全性；④用TMS320C25数字信号处理器实现通用数据加密算法A5。3.成果内容简介及关键技术：GSM建议03.20对GSM系统中采用的3个关键密码算法A3、A8、A5给出了统一的规范，但并不给出具体的算法。该专题组独立地完成了3个关键算法A3、A8、A5的选型设计及A5算法的C25芯片实现，结果表明，所提出的选型设计方案是先进、可行的。(1)在身份认证与加密密钥生成算法设计中，论证选用了目前国际公认最安全的一种“并行DM-HaSh函数”框架，用于生成32b用户签字应答和64b会话密钥。(2)课题组自行设计了分组密码HDSS，使算法A3/A8在SIM卡的环境下得以高速实现。(3)在通用数据加密算法A5的设计中，设计了OFB模式的帧加密框架。论证提供了2种供该框架使用的基本分组密码模块。采用数字信号处理器DSPIMS320C25对上述通用数据加密方案进行了软硬件模拟，实现了在0.5毫秒内加密一帧数据(114b)的协议指标。对使用IDEA作基本分组密码模块的上述OFB模式的算法A5进行了安全性分析；结果表明，在已知的密码攻击方法下，所设计的通用数据加密算法A5是安全的。二、经济、社会、环境效益及控广应用前景：该专题主要成果除了可用于设计(持合GSM建议的数字移动通信系统的)SIM卡之外，也适用于一般CPU卡(智能卡)及8位单片机，因而具有较大的应用价值和潜在的经济效益。三、成果转化的可行性：专题组自行设计的分组密码HDSS可以支持按以下方式实现中国GSM制式的数字移动通信系统的身份认证模块(SIM)的生产：①在近期实现自行设计、国外集成的SIM；②待中国具备了CPU卡芯片生产技术后，实现自行设计、生产SIM卡。可以生产通用的CPU卡(智能卡)，它们在“三金工程”等安全保密领域有重要作用。

成果完成人：何大可;王新梅;徐胜波

完整信息

推荐成果

· 空间飞行器SPACEWIRE高速数据...　04-23
· Adhoc网络中的QoS保证(Wirel...　04-23
· 基于正交多载波传输的高速无...　04-23
· 光因特网体系结构与管理技术　04-23

行业资讯

QH3792S腔式双工器
数字微波传输关键设备研制
2.4G无线接入系统设备
VSAT卫星通信系统
码分多址卫星数据通信地球站
WSD-1卫星数据通信单收站
1560点对多点微波通信系统
M2000 6GHz 155Mb/s SDH微波...
2×155Mbit/s SDH微波通信系统
M1000型2×34Mb/s数字微波接...

成果交流