

项目编号: G2007011

# 东南大学

## 国家大学生创新性实验计划项目认定书

项目名称: 移动终端信息安全传输技术研究

项目负责人: 逯丞 学号: ( 04005315 )

身份证号: ( 620502198705012055 )

电话: 13951671258

E-mail: marslovesvenus@163.com

项目参加者: 郭晓乔 (学号: 04004325, 身份证号 120101198510014038)

张橙 (学号: 04004013, 身份证号 320926198610210413)

黄梓宏 (学号: 04005338, 身份证号 320282198704036818)

刘慧慧 (学号: 04005304, 身份证号 410184198705069020)

项目指导教师 1: 胡爱群 (所属院系: 信息科学与工程学院)

电话: 13809003195

E-mail: aqhu@seu.edu.cn

项目指导教师 2: 陈立全 (所属院系: 信息科学与工程学院)

电话: 13813852253

E-mail: lqchen@seu.edu.cn

项目迄止时间: 2007 年 11 月 ~ 2008 年 11 月

东南大学教务处

## 一、项目内容简介

本项目对移动通信手机终端的安全传输技术进行研究,提出保障移动终端信息安全的传输技术,并进行原型验证。主要解决手机的语音,短信息和数据业务的安全传输问题。提出的多业务统一安全手机的安全通信技术,能够实现手机用户间端到端的语音、短信息的安全通信。

在手机端到端通信过程中,短信息和语音传输一般是在移动终端的底层协议传送,与手机的硬件和操作系统较为紧密。在智能手机的结构中,如基于 Intel Xscale PXA255 硬件和 Windows CE 操作系统的智能手机中,短信息和语音通信可以通过专门的驱动和应用程序来完成。通过调用 Windows CE 系统上的 API 接口函数,使用专门的安全短信息传输软件和安全语音通信软件实现短信息和语音的端到端之间的安全传输。

在智能手机中实现图 1 所示的安全通信技术来保证手机端到端安全。在操作系统的安全函数库基础上,可以实现语音,短信息甚至其它数据业务的安全传送。

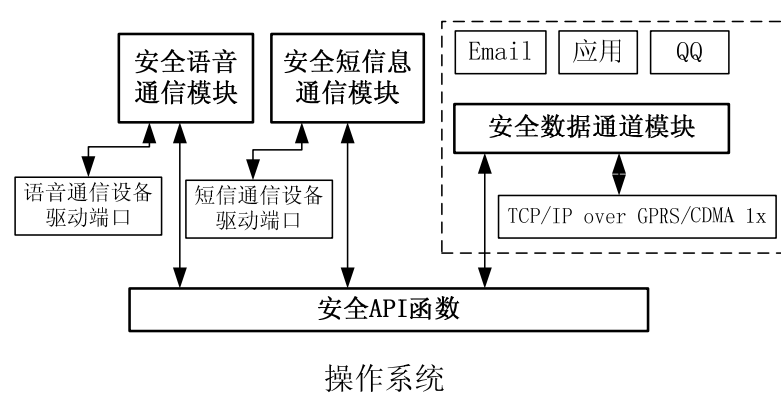


图 1 手机终端上的实现模型

研究内容主要分为以下三大部分:

### 1) 安全语音传送

安全语音传送过程可以通过在智能手机上编制专门安全语音通信软件来完成。在 Windows CE 操作系统中,加密语音的传输可以通过电路交换数据 CSD 链路或者 GPRS IP 通道来实现,只要对这个安全加密端口进行操作就可以实现语音的传送过程。我们通过编制专门的安全语音软件,调用操作系统的安全 API 函数,实现端到端的加密语音传送。

### 2) 安全短信息传送

同样,安全短信息传送过程也是通过编制在智能手机上的专门安全短信息通信软件来完成。在 Windows CE 操作系统中,短信息传送硬件模块已经映射成一个驱动的设备,如 TAPI 设备端口,只要对这个端口进行操作就可以实现短信息的发送和接收过程。通过编制专门的安全短信息软件,调用操作系统的安全 API 函数,来实现端到端的加密短信息传送。

### 3) 安全加密函数实现

基于操作系统上安全 CSP 调用模式，完成语音 RC4 加密算法的调用，短信息加密通过调用 3DES 加密算法来实现。

#### 目的意义：

已有的移动通信系统（包括 GSM, CDMA 和 3G 系统）本身的安全机制和措施都存在缺陷，难以保证手机端到端的安全。因此，本项目提出并实现的发送手机信源加密到接收手机信源解密的端到端安全传输方法，有效保证移动信息在整个传输过程的安全传输。

目前国内外的研究较多集中在移动通信本身的安全机制和算法方面，由于语音在到达基站侧时，会变成 PCM 码流进行透明传输，所以需要端到端的安全语音传输技术来保证移动信息端到端的安全。解决这个移动信息安全问题具有重要的社会意义和良好的经济效益。

#### 具体目标：

预期完成一个可实现的手机安全通信技术方案，对方案中的各软件模块进行深入研究，并提出相应的解决方法和实现方案；

在智能手机的基础上，编制出安全的语音通信软件；

在智能手机的基础上，编制出安全短信息通信软件；

搭建完成手机到手机之间端到端的安全通信接入的原型验证系统。

#### 实现的系统满足以下技术指标：

支持 GPRS 或 CDMA 1x 移动网络；

安全算法支持对称加密算法；

移动终端类型支持智能手机或 PDA 手机等；

移动终端操作系统支持 Windows CE 或 Windows Mobile；

加密后语音质量好、延迟低；

加密短信息支持最大字数：140 字节。

## 二、研究技术路线

本课题主要提出并研究移动终端手机安全通信技术的可实现方案，并实现一个简化的用于测试验证所提出方案的模拟实验原型系统。对方案中的各系统模块、软件模块、安全算法机制等关键问题进行深入研究，提出相应的解决方法和实现方案。编制实现安全语音通信软件模块和安全短信息发送接收软件模块。

首先针对端到端手机安全通道技术的框架进行分块深入研究。其中包括了对移动通信网络体系、移动网络安全机制、安全算法和移动终端构成等进行分析和研究，提出移动信息端到端的安全传输技术和方案。

在本项目研究的过程中，我们根据实验室的条件搭建了如图 2 的原型系统。可以模拟、测试并验证手机到手机之间端到端的安全通信接入的所有过程。

移动终端选用基于 Windows CE 操作系统的智能手机，如多普达 818 (GPRS) 或大显 CU928 (CDMA 1x)。需要在移动终端的 Windows CE 操作系统上实现安全函数编程调用，同时实现安全的语音，短信息程序等。

手机移动网络是指移动运营商的移动网络，能进行快速数据接入。如中国移动的 GPRS 网络和中国联通的 CDMA 1x 网络。

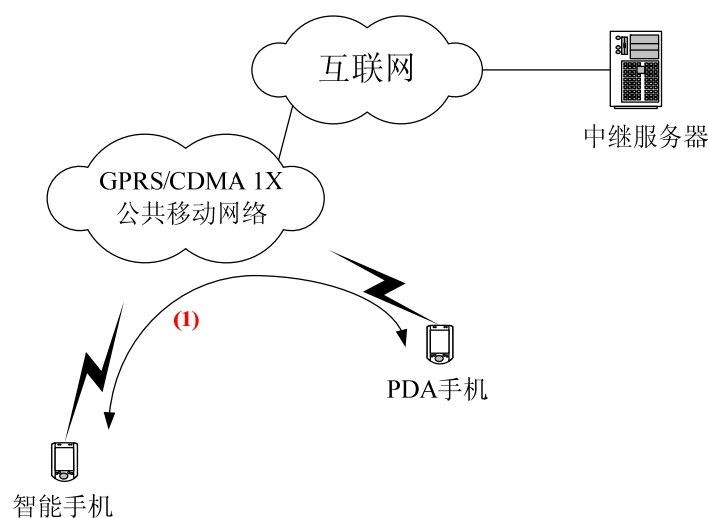


图 2 简化的原型系统框图

### (1) 移动语音安全传输

在移动端到端语音安全方面，主要按照以下图形进行实现，传输的方面可以采用 GPRS 传输，也可以采用 CSD 通道来进行传输。

#### 1)、语音采集和播放

通过 waveform audio API 函数对音频输入输出设备的控制来实现语音的采集和播放。其中包括打开输入输出设备，分配音频数据块，播放音频文件，为音频数据分配内存，关闭音频输出设备等。

#### 2)、CELP 编解码

考虑到在 Windows CE 上实现，PDA 的 CPU 是 Intel 公司的 PXA272 定点 CPU，所以需要将 CELP 算法采用定点编程的程序来实现。

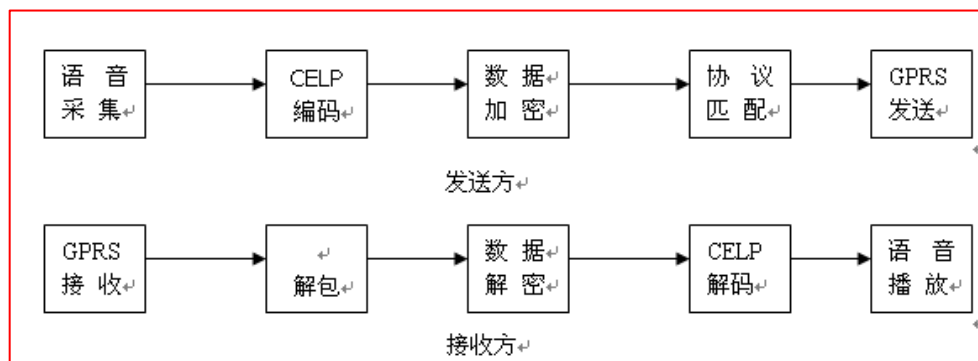


图 3 加密语音传输框图

### 3)、加解密

采用对称加密算法来实现。

### 4)、GPRS 上的 Socket 连接

侧重选择在 GPRS 通道上建立端到端的语音安全传输：

a) CSD 编程底层开发在接收语音时，TAPI 函数不能独占信息，而我们实验的手机原有的电话程序则一直占用着接纳呼叫信息，所以必须采用 RIL 函数方式才能实现，而 RIL 模式是 microsoft 的专利技术，涉及到多方面的问题，技术复杂度较高。所以我们选择采用 GPRS 通道来传输端到端的安全语音信息。

b) 使用 GPRS 通道也是适应未来数据域技术和业务发展的趋势。现在 WiMAX 技术成为了新的 3G 标准，基于数据域上传语音是一个必须解决的问题。

c) GPRS 通道的优势是，GPRS 可以包月计费，没有漫游费。

### 5)、地址分配和端到端穿越

通过 CMNET 方式拨号上 GPRS 的智能手机获得 GPRS 网关分配的 IP 地址为 10. X. X. X 的内网 IP 地址。

当在屏蔽 GPRS 直接点到点通信的地方，或者需要跨区 GPRS 端到端安全通信的地方，则需要建立一个公网上的中继服务器来进行数据的中转发送。需要安全通话的两个终端通过这一中继服务器来完成语音信号的到达。这里面存在一个 IP 地址 NAT 穿越的过程。

## (2) 移动短信息安全传输

短信息的发送模式主要有 BLOCK 模式、基于 AT 指令集 PDU 和 TEXT 模式两种(详见 GSM 07.05 文档)。PDU 模式已逐渐取代 BLOCK 模式，后者逐渐淡出通常的使用方式，在 Pocket PC 的 Windows CE 上采用的就是 PDU 模式。而且针对字符与汉字，也采用不同的编码格式，如对汉字采用的 140 个 8 bit，而汉字的 UNICODE 编码格式占用 2 个 Bytes(16bit)，即一条短信最多发送 70 个汉字，对于字符，即 ASCII 值为 0~127，一条短信最多发送 140 个左右字符。

短信的发送，所采取的是有微软提供的 TAPI 中的有关 SMS 操作的函数。TAPI 实际上是对 AT 指令集的封装。

短信息的接收过程可以分为两种方式，一种是不用 inbox 作为短信接收工具；另一种是用 inbox 作为接收工具。其在程序上的不同为前者需要对进程进行编程，而后者则用到了另一 API 函数 MAPI, 并且需要修改注册表。

### (3) 安全算法实现

语音和短信息加密的算法预计采用 RC4 和 3DES 算法来完成。

#### 可行性分析:

本项目研究的移动终端信息安全传输技术需要解决以下的关键难点问题:

1) 语音 CELP 定点压缩算法的实现, 通过参考国外的浮点 CELP 算法的源代码, 进行定点变化, 实现 4.8Kbps 的定点 CELP 在 Windows CE 上的实现。

2) 语音录制和回放的实现, 在 Windows CE 下面, 实现语音的连续采集和压缩, 还有连续回放, 需要实现乒乓模式的缓冲机制, 同时缓冲的大小选择根据网络带宽来调整。

3) IP 地址穿越问题, 当采用 GPRS 实现移动信息端到端安全的时候, 涉及到 IP 地址的分配和 IP 地址寻址的问题, 通过 NAT 的机制完成 IP 地址的寻址。

本项目侧重研究的移动信息安全传输技术, 有着强大应用开发环境和实验环境支撑。现在的移动通信网络发展迅速, 网络覆盖良好, 为本项目的开展和应用提供了基础, 同时, 现在移动信息安全仍是热门话题, 这为本项目成果的推广应用提供需求。

本项目将在东南大学信息安全研究中心胡爱群教授和陈立全等老师的指导下完成。东大信息安全研究中心一直以来从事移动信息安全技术的研究, 承担的 863 计划, 242 基金, 115 基金等多项移动信息安全监管、移动信息端到端安全的项目, 这些丰富的项目经验将为本项目的顺利开展和完成提供有效支撑保障。

#### 三、项目预期成果形式及数量

■ 文献资料综述	1 份;	□ 调研报告	份;
■ 研究或设计方案	1 份;	□ 图纸	套;
□ 实验记录	份;	■ 论文	1 篇;
■ 实物: 名称 <u>移动终端信息安全传输原型系统</u> 主要技术指标 <u></u>			
■ 软件	1 件;	■ 心得体会	5 份;
■ 展板(电子稿) ★	1 幅;	■ 其它	专利 1 项

四、项目进度安排 起止时间 <input checked="" type="checkbox"/> 一年期：本年 11 月至第二年 11 月 <input type="checkbox"/> 半年期：本年 5 月至 12 月	项目内容及时间安排		项目内容及时间安排		
	<input checked="" type="checkbox"/> (文献查阅) 2007. 11~2008. 2		<input checked="" type="checkbox"/> (研制开发) 2008. 6~2008. 9		
	<input type="checkbox"/> (社会调查)		<input checked="" type="checkbox"/> (撰写论文或研究报告) 2008. 10		
	<input checked="" type="checkbox"/> (方案设计) 2008. 3		<input checked="" type="checkbox"/> (结题和答辩) 2008. 11		
	<input checked="" type="checkbox"/> (实验研究) 2008. 4~2008. 5		<input type="checkbox"/> (成果推广或论文发表)		
	<input type="checkbox"/> (数据处理)		<input type="checkbox"/> (其它)		
五、经费用途	科目	金额(元)	科目	金额(元)	备注
	材料(试剂)费	7000	论文版面费	1000	
	加工费	4000	市内公交	1000	
	工具费	1000	上机上网费	500	
	专利申请费	2000	试验(实验)费	1500	
	资料费	2000			
			合 计	20000	
六、指导教师意见：  <p style="text-align: center;">技术方案可行，经费预算基本合理，希望协调好小组学生按进度开展工作</p> <p style="text-align: right;">签字    胡爱群                  2007 年 12 月 15 日</p>					
七、院系“研学指导小组”意见：  <p style="text-align: center;">课题目标明确，前期工作充分，方案详细可行，特色突出，同意立项</p> <p style="text-align: right;">组长签字    孟桥                  2007 年 12 月 15 日</p>					
八、学校主管部门意见：  <p style="text-align: center;">同意该项目立项为国家级大学生创新训练项目，批准经费 20000 元。</p> <p style="text-align: right;">负责人签章                          年    月    日</p>					

★展板的电子稿用 photoshop 软件,按(900mm×1200mm)尺寸绘制