# 全国第三届DSP应用技术<br>第九届信号与信息处理

# 联合学术会议

# 论文集

中国电子学会DSP应用专家委员会
中国航空学会信号与信息处理专业分会 主编

北京航空航天大学出版社

# 全国第三届DSP应用技术 九届信号与信息处理 联合学术会议

# 论文集

中国电子学会DSP应用专家委员会
中国航空学会信号与信息处理专业分会 主编

北京航空航天大学出版社

## 内 容 简 介

本书为全国第三届 DSP 应用技术与第九届信号与信息处理联合学术会议论文集，反映了近年来国内在开发、设计、应用 DSP、FPGA、嵌入式技术及航空航天信号与信息处理等方面的最新科技成果。全书共 10 章，主要内容包括：DSP 在现代通信技术中的应用；DSP 在音频和视频信号处理中的应用；DSP 在测控系统技术中的应用；DSP 在图像处理领域中的应用；DSP 在雷达和水声信号处理中的应用；FPGA 的应用技术；嵌入式技术的设计及应用；DSP 的设计及接口技术；DSP 的应用及调试；航空航天信号处理技术。

本论文集内容丰富，具有开发、设计、应用的先进性、可行性、创新性及实用性，具有较高的学术参考价值，适合大专院校师生，科研院所、企事业单位的相关科技人员阅读和参考，也适宜科技情报室和图书馆收藏。

**图书在版编目(CIP)数据**

全国第三届 DSP 应用技术、第九届信号与信息处理联合学术会议论文集/中国电子学会 DSP 应用专家委员会，中国航空学会信号与信息处理专业分会主编．—北京：北京航空航天大学出版社，2005.9

ISBN 7-81077-727-0

Ⅰ．全… Ⅱ．①中…②中… Ⅲ．数字信号—信号处理—学术会议—文集 Ⅳ．TN911.72-53

中国版本图书馆 CIP 数据核字(2005)第 102389 号

**全国第三届 DSP 应用技术 第九届信号与信息处理 联合学术会议论文集**

中国电子学会 DSP 应用专家委员会
中国航空学会信号与信息处理专业分会 主编

责任编辑 冯 颖 高 路 芦潇静

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100083) 发行部电话：010-82317024 传真：010-82328026

http://www.buaapress.com.cn E-mail:bhpress@263.net

涿州市新华印刷有限公司印装 各地书店经销

开本：787×1 092 1/16 印张：28.25 字数：977 千字

2005 年 9 月第 1 版 2005 年 9 月第 1 次印刷

ISBN 7-81077-727-0 定价：90.00 元

# 单片机与嵌入式系统应用

www.dpj.com.cn

## 何立民教授主编

中央级科技期刊 月刊

北京航空航天大学出版社 承办

反映嵌入式系统先进技术
推动嵌入式应用全面发展

| | |
|---|---|
| 业界论坛 | 创新观念、技术评述、学术争论以及方向性、技术性指导 |
| 专题论述 | 单片机与嵌入式系统领域的热点技术、观念及综合分析 |
| 技术纵横 | 国内外先进技术的宏观纵览，全局资料分析、介绍和述评 |
| 新器件新技术 | 先进器件、先进技术及其在系统中的典型应用方法 |
| 应用天地 | 具有重要参考价值的科技成果与典型应用的技术交流 |
| 经验交流 | 嵌入式系统应用中的深入体验和开发经验交流 |
| 学习园地 | 介绍嵌入式系统新领域的基础知识 |
| 产业技术与信息 | 为嵌入式系统产业界提供技术与信息发布平台，推广厂家的最新成果 |
| 编读往来 | 嵌入式系统领域的科技活动报道及产业动态 |

专业期刊 着眼世界 应用为主
专家办刊 面向全国 读者第一

出版日期：每月1日出版
国际标准16开本形式出版
每期定价：8元 全年定价：96元
国内统一刊号：CN 11-4530/V
国际标准刊号：ISSN 1009-623X
邮发代号：2-765

诚挚欢迎业界人士向本刊投稿，欢迎广大读者订阅本刊

地址：北京市海淀区学院路37号《单片机与嵌入式系统应用》杂志社 邮编：100083
投稿专用邮箱：mcupress@263.net.cn 广告部专用邮箱：advmcu@263.net
电话：010-82338009（编辑部）82317029，82313656（广告部）82317043（网络部）
传真：010-82317043 网址：http://www.dpj.com.cn

# 全国第三届DSP应用技术<br>第九届信号与信息处理联合学术会议

2005年10月12日～17日

湖北·宜昌

**主管单位：** 中国电子学会
中国航空学会

**主办单位：** 中国电子学会DSP应用专家委员会
中国航空学会信号与信息处理专业分会

**支持单位：** 北京航空航天大学出版社
《单片机与嵌入式系统应用》杂志社

**顾问委员会：** 侯朝焕　毛二可　张彦仲　李启虎　郭桂蓉

**会议主席：** 张晓林

**副　主　席：**（按姓氏笔画排序）
丁国辉　龙　腾　李少洪　李哲英　赵荣椿

## 程序委员会

**主　　席：** 毛士艺

**副 主 席：**（按姓氏笔画排序）
王跃科　陈志昊　高梅国

**委　　员：**（按姓氏笔画排序）
马广云　万国龙　孙义明　刘云海　刘培志　刘　玫
许　超　何培宇　吴桂荣　张卫宁　张旭东　张　泽
杨东凯　林洪文　郑　红　侯榆青　赵歆波　袁嗣杰
徐伯夏　常　青　曾义芳　游林儒　曾　涛　翟正军

## 论文评审委员会

**主任委员：** 孟宪元

**副 主 任：**（按姓氏笔画排序）
马广云　刘志文　李传日　周继成　赵保军　曾义芳

## 会务委员会

**主任委员：** 曾义芳（兼大会秘书长）

**副 主 任：** 徐伯夏（兼大会副秘书长）
赵　勇（兼大会副秘书长）

# 中国电子学会DSP应用专家委员会委员名单

| | | | | |
|---|---|---|---|---|
| 张晓林 | 毛士艺 | 李少洪 | 万国龙 | 丑武胜 |
| 杨东凯 | 李传日 | 马广云 | 郑　红 | 李哲英 |
| 高梅国 | 赵保军 | 刘志文 | 曾　涛 | 曾义芳 |
| 孟宪元 | 张旭东 | 余道衡 | 许　超 | 周继成 |
| 何国键 | 李双田 | 毛武兴 | 刘培志 | 张文杰 |
| 景韶光 | 黄永杰 | 张伟明 | 梁志恒 | 高一文 |
| 赵　勇 | 王跃科 | 李　纲 | 刘济林 | 刘云海 |
| 何培宇 | 丁国辉 | 徐伯夏 | 李文元 | 刘瑞华 |
| 郑启生 | 廉保旺 | 樊养余 | 翟正军 | 侯榆青 |
| 袁嗣杰 | 张卫宁 | 王划一 | 王军宁 | 吴仁彪 |
| 侯春萍 | 游林儒 | 黄建军 | 张　泽 | 顾　红 |
| 刘　玫 | 刘　云 | 朱　明 | 曹建树 | |

# 第二届中国航空学会信号与信息处理专业分会名单

| | | | | |
|---|---|---|---|---|
| 张彦仲 | 张晓林 | 毛士艺 | 赵荣椿 | 丑武胜 |
| 陈志昊 | 霍　雯 | 龙　腾 | 曾义芳 | 郑启生 |
| 吴桂荣 | 孟宪元 | 余道衡 | 应怀樵 | 林洪文 |
| 王奎华 | 周　辉 | 常　青 | 陈正捷 | 赵歆波 |
| 金　钢 | 樊养余 | 黄勇杰 | 邓中卫 | 孙义明 |
| 张松林 | 陈加海 | 李耀民 | 孟卫华 | 丁勇正 |
| 甘俊英 | 杨日杰 | 姚宗信 | 周秀贞 | 韩金福 |
| 孟英谦 | 金心丽 | 韩培友 | 李　明 | 王　庆 |
| 崔蕴华 | 董永宏 | 赵　勇 | | |

# 前　言

DSP是专为适用高速、密集的数字信号处理运算而发展起来的。近年来，TI、AD等公司纷纷推出速度更高，功能更强的高端产品，以满足日益增长的高端需求。然而，对于低端应用，以及对价格和功能要求较高而对处理性能要求适中的产品，采用传统结构的DSP仍占据主导地位。现阶段，以单片或多片DSP以及可编程逻辑器件(FPGA、CPLD)等构成的可编程处理模块是高性能嵌入式系统以及高速实时信号处理系统的基本组成模块。随着半导体工艺的发展，片上系统(SoC)得到了广泛应用，并出现了基于FPGA和CPLD的可配置片上系统(CSoC)，这些均推动着嵌入式技术的进一步发展。

当前，DSP、FPGA、SoC以及嵌入式技术已广泛应用于通信、雷达、声纳、图像、测控、自动化、仪器仪表、消费电子及智能家电等领域，也即本次联合学术会议研讨和交流的四大主题。

中国电子学会DSP应用专家委员会于2003年10月正式成立；中国航空学会信号与信息处理专业分会于1997年10月正式成立。它们的成立时间虽然不长，但也组织了多届学术会议，举办了多期培训班，并取得了一定的成绩。这主要归功于上级学会的指导与鼓励，归功于委员会及分会成员们的帮助和支持，同时更要感谢社会各界专家、学者、科技工作者的认可和积极参与。

本次联合学术会议征文较晚，经过多方努力，正式录用106篇编入本论文集。全书共分10章，主要内容包括：DSP在现代通信技术中的应用(20篇)；DSP在音频和视频信号处理中的应用(16篇)；DSP在测控系统技术中的应用(11篇)；DSP在图像处理领域中的应用(13篇)；DSP在雷达和水声信号处理中的应用(12篇)；FPGA的应用技术(7篇)；嵌入式技术的设计及应用(4篇)；DSP的设计及接口技术(15篇)；DSP的使用及调试(4篇)；航空航天信号处理技术(4篇)。

本学术文集内容丰富，具有开发、设计、应用的先进性、可行性、创新性及实用性，具有较高的学术参考价值。适合大专院校师生，科研院所、企事业单位的相关科技人员阅读和参考，也适宜科技情报室和图书馆收藏。

特别要感谢北京航空航天大学出版社的领导和编辑们的帮助和支持，使得此论文集能够及时出版。

中国电子学会DSP应用专家委员会秘书长
中国航空学会信号与信息处理专业分会总干事　曾义芳

2005年8月于北京

# 目　录

## 第一篇　DSP 在现代通信技术中的应用


TD－SCDMA 移动终端加密的 DSP 实现 …… 罗刚华　郑建宏(2)
基于 DSP 的高动态直序扩频接收机的软硬件设计 …… 许　纹　李署坚　邵定蓉(6)
基于软件无线电思路的超小型高性能通用信号处理硬件平台设计 …… 李燕斌(10)
基于 ADSP－BF533 处理器的 GPS/GPRS 应用系统
…… 郑楚锋　赵汝聪　蒙　山　喻建平　谢维信(14)
应用 SOPC 技术的扩频接收机基带信号处理模块的研究
…… 李　勃　姚廷燕　杨东凯　张其善(18)
直序扩频通信中的一种同步方案设计 …… 郑惠荣　张晓林　张　超(22)
基于软件无线电技术的通用调制平台设计 …… 陈海小　周建峰(26)
H.264 中算术编码器电路设计 …… 许　超(30)
能用于 H.264 宏块预测模式决策的失真度量方法
…… 赖昌材　郝重阳　席迎来　葛晓晓(34)
TD－SCDMA 系统信道估计在 ZSP 的实现 …… 周　兰　申　敏　王　鹏(38)
天线阵列 CDMA 系统中的盲波束成型算法 …… 史　鹞　张旭东(43)
远距离射频识别系统 …… 濮剑锋　常　青　郑　铭(48)
基于 FPGA＋DSP＋PC 的软件无线电实验平台硬件设计
…… 杨　枫　寇艳红　张其善(51)
中频信号的数字下变频原理与应用 …… 江　山　陶青长　高梅国(55)
用 DSP 对确知码元的接收端进行无失真滤波器设计 …… 李　志　高　阳(59)
硬判决维特比译码在 TMS320C5410 上的实现
…… 毕存磊　常　青　李　健　金　科(62)
基于 VxWorks 操作系统的网管系统的设计与实现
…… 李红梅　刘文生　曾志民　周继成(65)
一种椭圆曲线加密智能卡设计 …… 林洪文　常　青　张其善(69)
串口总线时统技术研究的设想
…… 冯保红　李二鹏　冯保东　赵三军　冯　蔚　周　翔(73)
数字通信调制模式自动识别 …… 陈国杰　孙义明　闻　翔(77)


## 第二篇　DSP 在音频和视频信号处理中的应用


基于 DSP 的 G.729 语音编/解码器的设计与实现 …… 侯榆青　卢艳玲(84)
基于 TMS320C6701 EVM 板的房间冲激响应测试与 LabVIEW 中的实时显示
…… 潘　帆　何培宇　邓　方　吴景田(89)
基于 ZSP500 的 AMR 语音编码器实现 …… 王　鹏　郑建宏　周　兰(93)
基于 USB 存储的数据语音采集方案的设计与实现
…… 金　科　常　青　毕存磊　李　健(97)
基于 TMS320VC5501 的数字效果器的研究 …… 游林儒　景　博　唐都文(101)
基于 DSP 的视频交通信息检测系统通信软件设计 …… 张　曦　丁国辉(105)
基于两片 C64x 的视频跟踪器设计与实现 …… 万　军　赵保军　马志峰(109)

MPEG－4 视频解码器在 ADI BF533 上的实现 …… 贾 鹏 吴 强 孙光民(112)
汉语连读语音自适应端点检测 …… 范 京 刘惠华(116)
视频交通检测系统中背景建立算法的研究 …… 张 流(120)
啸叫抑制的 DSP 实现 …… 游林儒 唐郁文 景 博(124)
基于通用 DSP 的视频编码库优化研究 …… 吕鸿波 徐 慧 汪燮彬 刘云海(128)
基于 ADSP－BF561 车载多媒体系统
…… 王天元 赵汝聪 蒙 山 喻建平 谢维信(132)
基于 BLACKFIN561 的 H.264/AVC 视频编码的研究 … 祁云平 常 青 佟雨兵(137)
基于 TMS320C6713 DSP 的视频采集系统 …… 程齐明 郑 红(141)
基于 DSP 的可视电话系统设计 …… 张 骏 吴 强 刘明亮(146)

## 第三篇 DSP 在测控系统技术中的应用

基于 DSP 和 FPGA 的遥控指令测试平台设计和实现
…… 周 伟 门爱东 刘贺林 王 双 傅林春(151)
基于多 CPLD/FPGA 的多轴振动控制系统设计 …… 姚金勇 李传日 姜同敏(155)
TMS320C6701 在电离层探测系统中的应用 …… 时 雨 赵正予 杨国斌(163)
用软件解调 PCM－DQPSK 遥测信号的方法研究 …… 安志琦 袁嗣杰(166)
两输入单输出模糊控制器的数字实现 …… 田鸿堂 王进军(170)
多点振动控制算法在 μC/OS－II 中的双缓冲实现 …… 石士进 李传日(174)
全极点滑动窗在软件解调中的应用 …… 章兰英 侯孝民 袁嗣杰 陈进军(178)
多轴振动控制系统中基于 CPLD 的多模式多通道同步采样系统设计
…… 姚金勇 李传日 姜同敏(181)
TMS320C6201 在某光电装置中的应用 …… 邹斌阳 闫 琳 周月梅(186)
某型机载导弹机上检测箱智能检测电源电路的设计
…… 张志虎 汪东林 贾红光 王天玉(189)
基于 PCI 总线与 DSP 的振动控制系统数据通信及 CPLD 实现
…… 张新运 李传日 姚金勇(191)

## 第四篇 DSP 在图像处理领域中的应用

微波成像系统中高速数据采集系统的设计与实现 …… 李 剑 黄智刚 万国龙(198)
数码相机教学系统设计 …… 杨 威 李哲英(202)
基于图像区域概率分类的室外场景理解方法
…… 张 敏 刘培志 陈志昊 徐英新 王晋华 刘 莹(206)
一种基于边缘检测的图像降斑方法 …… 朱立民(210)
一种基于视觉特性的运动估计匹配准则 …… 邹晓春 赵歆波(214)
基于多片 C64x 的红外实时处理机的硬件设计与实现 …… 李 宏 李 伟 王 俊(217)
基于 TMS320VC5510DSK 和 FPC1010 指纹传感器子卡的自动指纹识别系统
…… 高志奇 张 泽(221)
一种基于图像的近场－远场 RCS 转换技术 …… 黄 莹 许小剑(226)
基于 DSPC6201 和 CPLD 的高速图像采集系统设计 …… 谭金利 赵保军(230)
基于 TMS320C6711DSK 实现 CCD 图像显示 …… 李临生 何延昭 陈东源(233)
基于 FPGA＋双 DSP 光电跟踪系统设计 …… 吴 莲 史彩成(236)
基于 JSP 技术的远程智能维护系统 …… 张江波 常 青(240)
基于双 DSP 的图像实时跟踪测量系统研究 …… 王军宁 刘英彬 李 辉(242)

## 第五篇 DSP在雷达和水声信号处理中的应用

基于ADSP-TS201S的高速并行信号处理机的设计 …… 张永杰 李少洪(247)
基于StarFabric互连的8-TMS320C6416并行信号处理板的设计与实现
…… 刘国满 郑 坤 李 岳 高梅国(251)
Radon-Wigner分布在线性调频雷达信号分选中的应用 …… 赵 阳 王月忠(257)
基于DDS技术的雷达中频信号源的设计 …… 郭 洪 李 阳 曾 涛(261)
海上舰船目标的多路径仿真 …… 崔 凯 许小剑 毛士艺(264)
用于机动目标跟踪的交互式多模型粒子滤波算法 …… 刘迎娜 曾 涛(268)
采用FPGA实现聚束SAR成像算法的研究 …… 王文菁 孙进平 袁运能(271)
基于Spartan-3的雷达定时通信模块设计 …… 杨兆勇 曾大治(276)
基于某型雷达目标模拟器的DSP异步串行通信设计 …… 欧 燕 梁 沂 薛明华(281)
海面目标电视跟踪技术研究 …… 崔 健 陈远知(285)
基于双DSP的激光测距机信号处理系统 …… 张云龙 赵保军(289)
基于VxWorks的窄带中频雷达回波信号产生器的实现
…… 曹 宁 马银松 汪 飞 胡建荣(292)

## 第六篇 FPGA的应用技术

FPGA实现嵌入式系统 …… 孟宪元(299)
IC总线的FPGA实现以及实例说明 …… 张 帆 王 琦 龙 腾(303)
基于FPGA的短时傅里叶变换递推算法 …… 羌胜莉 袁嗣杰(308)
基于FPGA的多接口存储器实现 …… 李 蒙 王 俊 齐秀凤 李 宏(313)
基于TMS320C3X系列DSP浮点运算方法的研究及其FPGA实现 …… 李红军(317)
一种高速滤波器结构的硬件实现 …… 文开霞 李哲英(323)
扩频接收机匹配滤波器的设计及其FPGA实现
…… 李 健 常 青 毕存磊 金 科(328)

## 第七篇 嵌入式技术的设计及应用

电子设备接入Internet的嵌入式Web服务器设计 …… 郝英华 李晓光 李哲英(332)
基于S3C2410的嵌入式智能飞镖游戏计分系统设计 …… 夏永存 席丙俊 金 锋(336)
DSP+FPGA体系结构实现最小二乘递推算法 …… 姜娇蕊(339)
嵌入式μPSD3254在数控标记系统中的应用 …… 李 斌 刘 玫 张卫宁(343)

## 第八篇 DSP的设计及接口技术

DSP设计中的DFG方法 …… 陈 鸽 李哲英 李维敏(348)
一种可编程数字信号处理器的设计与实现
…… 沈 钰 何 虎 张延军 杨 旭 谭洪贺 孙义和(353)
DSP系统中的USB海量存储 …… 陈婷婷 李哲英(357)
浅谈DSP系统中的电磁兼容性 …… 孙 宏(361)
基于Motorola 56800系列DSP的虚拟机的移植和通用用户接口的设计
…… 王云柱 丁国辉(365)
Flash与DSP间的接口设计与实现 …… 曾梁英 肖海凤 邵定蓉 王小康(369)
基于CPLD的航电总线ARINC 429接口板设计与实现 ……
…… 吴晓洁 翟正军 丁 楠 羊天德(372)
基于TMS320C6201/6701的硬件平台设计 …… 于龙沾(379)
协处理结构巡航弹载计算机设计 …… 陈远知(382)

TI C6416 与主机之间 PCI 通信的实现 …… 周建锋 陈海小 刘作学(386)
MATLAB 实现主机和 DSP 实时数据交换 …… 吴昌成(389)
基于 PMC 模块的多 DSP 并行计算机系统设计
…… 苏兰冬 张金龙 赵俊良 王定湖(394)
板上网络互联与交换结构多 DSP 系统模块设计 …… 王跃科 明德祥 随卫平(396)
基于 TMS320C6713 的 DSP 基础硬件程序设计 …… 王 娜 郑 红(401)
基于 DSP 的智能 429 总线接口板硬件设计与实现 …… 韩 冲 翟正军 羊天德(405)

## 第九篇 DSP 的应用及调试

TMS320F206 使用经验及技巧 …… 刘 畅(411)
DSP 在航空、航天生物医学中的应用概况 …… 李 娟 由 衷 王 翔(416)
基于 TMS320LF2407 DSP 中断程序的调试研究 …… 周治国 侯建刚(419)
ADSP－21062 在脉间步进频体制信号处理机中的开发与调试 …… 韩相秋(422)

## 第十篇 航空航天信号处理技术

航空航天中冲击过负荷问题 …… 吴桂荣(428)
复杂系统人机功能信息分配模型的建立及应用 …… 曲战胜 周前祥 周诗华(432)
运动吸氧排氮预防高空减压气泡和减压病的研究
彭远开 贵锦学 虞学军 国耀宇 王 亮 肇 海 常绍勇 全海曦(435)
基于 MAP 过程的斑点抑制算法分析 …… 于越华 李 颖(439)

# 第一篇

# DSP在现代通信技术中的应用

# TD-SCDMA 移动终端加密的 DSP 实现

罗刚华　郑建宏

重庆邮电学院移动通信重点实验室，重庆，400065

**摘　要**　本文介绍了一种采用密钥长度为 128 bits，分组长度为 64 bits，内核为 KASUMI 的 f8 算法的数据加密算法，并利用 TMS320C5510 器件实现了该算法。由于该加密算法提供了可靠的安全性和可达 2 Mb/s 的加密速度，使其在移动终端中有着十分广阔的应用前景。

**关键词**　安全性，加密，KASUMI 算法，f8 算法

## 1　引　言

第二代(2G)及 2.5G 移动通信系统是当前正在广泛应用的移动通信系统，它以 GSM/GPRS 网络为代表。第三代移动通信系统(3G)是当前通信领域研究开发的热点。在 3G 系统中，除话音业务外，电子商务、电子贸易、网络服务等新型业务将成为 3G 的重要业务的发展点。若信息在网络中没有任何保护地传输，不仅容易被窃听，而且容易被修改，这些攻击将直接影响用户的利益，同时未经授权业务的接入也将影响运营商的利益。而密码技术是保护信息安全的有效方法，传统的加密体制存在密钥交换、密钥传递等问题，应用于网络通信存在诸多不便。公钥密码体制不要求通信双方事先传递密钥，因而公钥密码体制更适于网络的保密通信。

3G 系统的安全体制是建立在 2G 基础上的。GSM 及其他 2G 系统已证明，必须继续采用稳健的安全元素；3G 系统还将改进 2G 的安全弱点，最终提供全新的安全性能和业务。由于篇幅的限制，本文只讨论移动终端数据加密的算法描述、算法分析及 DSP 实现过程。

## 2　算法描述

保密功能是通过 MS(移动台)和 SRNC(服务无线控制器)间专用信道的加密函数 f8 实现的。若构成无线承载的 RLC(无线链路控制)层采用非透明模式，则数据加密在 RLC 层实施；若 RLC 层采用透明模式，则数据加密在 MAC(管理)层实施。f8 属于同步序列密码，图 1 显示了使用 f8 加/解密明文/密文的方法。它的输入参数包括：CK、时间相关的计数器 COUNT－C(32 bits)、无线信道标识 BEARER (5 bits)、方向比特 DIRECTION(1 bit)及密钥流分组长度标识 LENGTH。基于这些输入，f8 输出密钥流分组。CK 是在 AKA(可信密钥协定)过程中产生的 128 bits 加密密钥，由 MS 和对应的 SRNC 同时拥有。

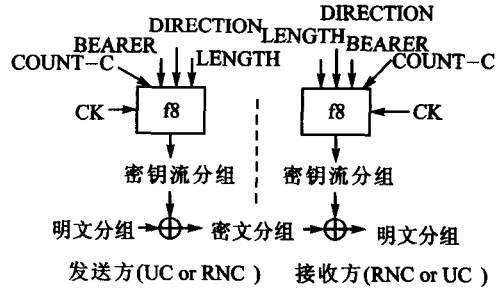


**图 1　无线链路上用户与信令数据的加/解密**

## 3　算法分析

为了满足 3G 安全性增强的要求和达到最大 2 Mb/s 的数据加密速度，分组密码必须采用 128 bits 的密钥长度(密钥空间：$3.4\times10^{38}$)以抵抗穷举攻击，分组长度可为 64 bits 或 128 bits。如内核分组密码可采用 3GPP 已标准化的 KASUMI(64 bits 分组)、AES、Twofish(128 bits 分组)等。为了实现全球漫游功能，本文关于数据加密实现部分采用 64 bits 分组的 KASUMI 内核算法。

### 3.1　简　介

保密性算法 f8 是一种用流密码对长度为 1～20 000 bits 的数据块进行加/解密的加密算法。

## 3.2　输入/输出参数

表1　输入参数

| 参　数 | 大小/bits | 说　明 |
|---|---|---|
| COUNT | 32 | 输入结构 COUNT[0]…COUNT[31] |
| BEARER | 5 | 信使身份 BEARER[0]…BEARER[4] |
| DIRECTION | 1 | 传输方向 DIRECTION[0] |
| CK | 128 | 密钥 CK[0]…CK[127] |
| LENGTH | 18[1] | 加/解密比特流长度(1～20 000) |
| IBS | 1～20 000 | 输入比特流 IBS[0]…IBS[LENGTH－1] |

表2　输出参数

| 参　数 | 大小/bits | 说　明 |
|---|---|---|
| OBS | 1～20 000 | 输出比特流 OBS[0]…OBS[LENGTH－1] |

## 3.3　初始化

本节将介绍怎样在密钥流产生器产生密钥前初始化关键变量。设置64 bits的A寄存器为COUNT || BEARER || DIRECTION || 0…0(共26个"0"),例如:A=COUNT[0]…COUNT[31] BEARER[0]…BEARER[4] DIRECTION[0] 0…0(共26个"0");设置计数器BLKCNT=0;设置密钥修改器KM为0x5…5(共32个"5");设置 $KSB_0=0$;寄存器A进行如下处理 $A=KASUMI[A]_{CK\oplus KM}$。

## 3.4　密钥流

一旦密钥流产生器按照上述方式初始化,它就作好了产生密钥流的准备(下面以KASUMI内核为例)。长度为1～20 000 bits的明文/密文将被加/解密,同时密码流产生器产生以64 bits长为单位的密码流。根据LENGTH指示的所有比特数来确定0～63之间最不重要的比特,其将被忽略。由此可知,BLOCKS=⌈LENGTH/64⌉。例如,LENGTH = 128,则BLOCKS= 2;LENGTH= 129,则BLOCKS= 3。为了产生密码流块(KSB),做如下处理:对每一个整数 $n(1\leqslant n\leqslant BLOCKS)$,定义 $KSB_n=KASUMI[A\oplus BLKCNT\oplus KSB_{n-1}]_{CK}$,其中BLKCNT=$n-1$。密码流的个别比特从 $KSB_1$ 到 $KSB_{BLOCKS}$ 中轮流提取,最重要的比特先提取,提取处理为:对 $n=1$ 到BLOCKS,$i=0,1,2,\cdots,63$,$KS[((n-1)*64)+i]=KSB_n[i]$。如图2所示。

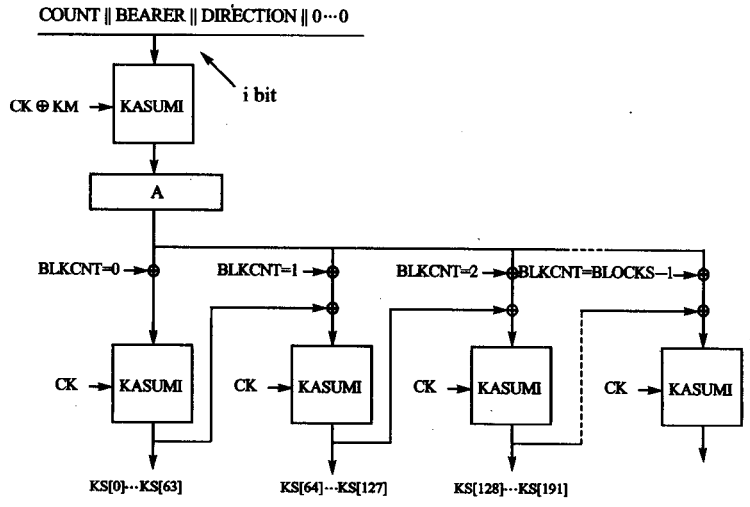


图2　f8密钥流产生器

### 3.5 加/解密

加密和解密处理方式一样，通过输入数据(IBS)与产生的密钥流(KS)进行“异或”算术操作。对每一个整数 $i(0 \leqslant i \leqslant \text{LENGTH}-1)$ OBS[$i$] = IBS[$i$]⊕KS[$i$]，如图 1 所示。

## 4 DSP 实现流程设计

### 4.1 TMS320C5510 DSP 简介

数字信号处理(Digital Signal Process，简称 DSP)是利用专用或通用数字信号处理芯片，通过数字计算的方法对信号进行处理，具有精确，灵活，抗干扰能力强，可靠性好，体积小，易于大规模集成等优点。TMS320C5510 DSP 是美国德州仪器公司推出的一款高性能、低功耗芯片，其速度可达 400～800 MIPS，广泛应用于移动通信、智能家用电器、个人多媒体数字助理等领域。它具有丰富的总线结构及 40 bits 的算术逻辑单元、40 bits 的移位器，支持 32 bits 运算，支持 DMA，支持多层嵌套循环，功耗可降至 0.25 mW，是 3G 终端产品的理想选择。C55X 可以使用 C 语言和汇编语言混合编程，主程序或控制类的程序采用 C 语言编写，便于控制；而各个基本的具体算法模块则采用汇编语言编写，执行效率要高些。C 编译器(C Compiler)将 C 源代码编译为 C55X 所用的汇编源程序，而汇编器(Assembler)将汇编源程序翻译为 COFF(Common Object File Format)格式的机器语言，链接器将 COFF 目标文件重定位到一个可执行的 COFF 目标模块中，生成可执行文件。最后，我们将所得到的可执行文件加载到 C55X 芯片上，便可在芯片上实现程序功能。有关 TI TMS320 C5510 芯片的使用情况可参见文献[6]。

### 4.2 DSP 实现流程

移动终端数据加密的 DSP 实现，从图 1 可知，其关键在于获得加/解密密钥。而从图 2 的密钥生成器框图可以看出，获得加/解密密钥的关键在于 KASUMI 内核，而 KASUMI 算法是一个 8 轮的 feistel 结构，由 FL 和 FO 两个单元函数构成轮函数，故可以在 DSP 实现时将 KASUMI 作为一个模块，按照图 1 所示设计其 DSP 实现的流程如下：

① 初始化 KM 和 A，并计算 CK⊕KM；

② 将明文分成 64 bits 的组，不足 64 bits 的块进行 0 填充使之为 64 bits；

③ 调用 KASUMI 模块，并将其输出作为种子输入参数；

④ 将块号和种子输入进行“异或”操作，并将其输出和 CK 作为 KASUMI 的输入，再次调用 KASUMI 模块得到 64 bits 的密钥流；

⑤ 重复第 4 步⌈lengths/64⌉次得到所有的密钥流；

⑥ 用得到的密钥流与明文“异或”操作，得到密文。

### 4.3 DSP 实现的资源开销

由图 2 知，假设数据加密明文长度为 64 bits，此情况下完成数据加密开销的 MIPS 最大。当 MIPS 开销在 DSP 能力范围内时，数据加密用软件无线电实现是可行的。MIPS 开销根据 TD-SCDMA 移动通信系统最大数据传输速率(2 Mb/s)计算。根据最大传输速率，完成 64 bits 的数据加密时间是 0.030 517 578 125 ms。同时，针对 TI 公司的 C5510 DSP 的指令特点，在一个执行周期内，可以完成一个 32 bits 的“异或”、“与”、“或”及移位等运算。从 KASUMI 的 8 级迭代算法可以看出，需要应用 8 次 FL 函数和 8 次 FO 函数，而每个 FO 函数需要应用 3 次 FI 函数，一个 FI 函数需要应用 2 次 S9 和 2 次 S7。理论上完成一次 S7 或者 S9 函数的运算需要 160 cycles，但是采用应用查表法只需要 3 cycles，而完成一个 FL 函数的运算需要 6 cysles，因此，理论上完成一次 KASUMI 运算需要 $6\times8+[(3\times2+3\times2+6)\times3+6]\times8+4+8=540$ cycles；所以，获得 64 bits 的加密密钥理论上需要 1 133 cycles。经过实际 DSP 代码测试，完成 64 bits 数据加密的实际开销 1 359 cycles，即 (1 359/0.030 517 578 125)=44.551 MIPS。而实际 TI 公司的 C5510 DSP 的 MIPS 最高可达 200 MIPS，所以从 MIPS 开销来看，用 C5510 DSP 实现数据加密是可行的。

## 5 总 结

随着“3G 热”的不断升温，通信的安全性也越来越为人们所关注。任何一种加密算法不可能实现绝对的安全，安全只是相对的。在相对安全的加密算法中，人们讨论较多的是公钥体制。其中，f8 加密算法是一种标准

化的安全性能良好的算法，它的安全性完全由算法的严密来保证，因此，推广 f8 加密算法的 DSP 实现是很有现实意义的。

## 参考文献


1 3GPP TS 35.201: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification

2 3GPP TS 35.202: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification

3 3GPP TS 33.103: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Intrgration guidelines

4 3GPP TS 33.102 version 3.2.0: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture

5 李小文，李贵勇，陈贤亮，等．TD-SCDMA 第三代移动通信系统、信令及实现．北京：人民邮电出版社，2003

6 申敏，邓矣兵，郑建宏，等．DSP 原理及其在移动通信中的应用．北京：人民邮电出版社，2001


# Realization of Data Encryption on DSP in TD-SCDMA System


**Luo Ganghua** **Zheng Jianhong**

Key Lab of Mobile Communication Technology of CQUPT, Chongqing, 400065, P. R. China



**Abstract** This discourse introduced a kind of data encrypting arithmetic which adopts the key's length as 128 bitses, the grouping length as 64 bitses and whose kernel is kASUMI. Then it utilizes the TMS320C5510 apparatus to implement this arithmetic. As it providing the dependable security and can reach the encryping speed to 2 Mbs/s, it has very wider applied foreground in mobile telecommunication.



**Key Words** Security, Encrypt, KASUMI Arithmetic, f8 Arithmetic