

当前位置: 科技频道首页 >> 军民两用 >> 光机电 >> 大数模幂乘密码算法处理器

请输入查询关键词

科技频道

搜索

## 大数模幂乘密码算法处理器

关键词: **芯片 密码 模幂 算法 处理器 模乘 网络安全**

所属年份: 2002

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: 深圳市中兴集成电路设计有限责任公司

成果摘要:

产品功能及应用领域: 该产品具有网络安全、安全电子交换、公开密钥体系、VPN服务器(IPSec)、安全套接层(SSL)、数字签名算法、Diffie-Hellman密钥生成、椭圆曲线密码、技术特点: 执行大数的模幂、模乘运算; RSA1024bit速度为50Kbps; 最大模数2048bit; I/O口与TTL兼容; 电源: +3.3V; 最大功耗: 1W。与国内外同类产品比较: 国内先进水平, 暂无自主开发的1024bit, 填补国内空白。达到国际中上等水平。综合功能的加密卡已得到广泛应用。项目成熟程度: 产品样机。市场分析简要说明: CPU芯片和DSP芯片是电信产品中的核心部件, 几乎在电信产品的每一个印制板上都会找到这两类芯片, 因此CPU芯片的市场需求是与电信产品的发展紧密相关的。目前国内和国际电信市场都在快速发展, CPU芯片的市场需求是很大的。国内未有同类产品, 通讯类产品的中档或中档以下的CPU应用都可以完全替代进口, 市场份额一年之内可以达到20%, 争取第二年达到40%。新增总投资: 1278万元。新增销售收入: 3800万元。产品主要技术性能指标: 使用了快速模幂运算芯片及快速算法。具备高速的密码运算能力, 对1024比特RSA的加密(对应于验证)和解密(对应于签名)的速度估算为: 加密速度130Kbps, 相当于每秒可验证签名130次, 签名50Kbps, 相当于每秒可签名50次。

成果完成人:

[完整信息](#)

### 行业资讯

- 塔北地区高精度卫星遥感数据处理
- 综合遥感技术在公路深部地质...
- 轻型高稳定度干涉成像光谱仪
- 智能化多用途无人机对地观测技术
- 稳态大视场偏振干涉成像光谱仪
- 2001年土地利用动态遥感监测
- 新疆特克斯河恰甫其海综合利...
- 用气象卫星资料反演蒸散
- 天水陇南滑坡泥石流遥感分析
- 综合机载红外遥感测量系统及...

### 成果交流

### 推荐成果

- 容错控制系统综合可信性分析... 04-23
- 基于MEMS的微型高度计和微型... 04-23
- 基于MEMS的载体测控系统及其... 04-23
- 微机械惯性仪表 04-23
- 自适应预估控制在大型分散控... 04-23
- 300MW燃煤机组非线性动态模型... 04-23
- 先进控制策略在大型火电机组... 04-23
- 自动检测系统化技术的研究与应用 04-23
- 机械产品可靠性分析--故障模... 04-23

Google提供的广告

