

## 安全技术

### 公钥密码系统中的硬件二元域求逆模块

宋灏龙, 梁华国, 单国华

(合肥工业大学计算机与信息学院, 合肥 230009)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 针对二元域上基本运算求逆操作的复杂性问题, 将软件应用中效率较高的求逆算法移植到现场可编程门阵列中, 利用其分步特点获取较低延迟, 并采用度数和乘法的规律性对执行周期进行缩减, 以较小的硬件开销增量换取较大的性能提高。仿真实验结果表明, 该模块能够适用于多个二元域及软件求逆。

**关键词** [二元域](#); [公钥密码体制](#); [求逆](#); [现场可编程门阵列](#)

分类号 [N945](#)

**DOI:**

通讯作者:

作者个人主页: [宋灏龙](#); [梁华国](#); [单国华](#)

## 扩展功能

### 本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(155KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

### 服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

### 相关信息

- ▶ [本刊中 包含“二元域; 公钥密码体制; 求逆; 现场可编程门阵列”的 相关文章](#)
- ▶ [本文作者相关文章](#)