

安全技术

可重构散列函数密码芯片的设计与实现

李 淼, 徐金甫, 戴紫彬, 杨晓辉

(解放军信息工程大学电子技术学院, 郑州 450004)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 根据不同环境对安全散列算法安全强度的不同要求, 采用可重构体系结构的思想和方法, 设计一种可重构的散列函数密码芯片。实验结果表明, 在Altera Stratix II系列现场可编程门阵列上, SHA-1, SHA-224/256, SHA-384/512的吞吐率分别可达到727.853 Mb/s, 909.816 Mb/s和1.456 Gb/s。

关键词 [可重构密码芯片](#); [安全散列算法](#); [现场可编程门阵列](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: [李 淼](#); [徐金甫](#); [戴紫彬](#); [杨晓辉](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (88KB)
- ▶ [\[HTML全文\]](#) (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“可重构密码芯片; 安全散列算法; 现场可编程门阵列”的 相关文章](#)
- ▶ [本文作者相关文章](#)