计算机工程　2010 36 (06): 131-132　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

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