云南大学学报（自然科学版）
JOURNAL OF YUNNAN UNIVERSITY(NATURAL SCIENCES)
中文核心期刊
中国科技核心期刊

云南大学学报(自然科学版) » 2011, Vol. 33 » Issue (1): 22-26 DOI:

基于多核的批处理RSA的并行加速方法

李云飞[1], 柳青[2,3], 李彤[2,3], 周保林[1], 彭华[1]

1. 云南大学 信息学院,云南 昆明 650091;
2. 云南大学 软件学院,云南 昆明 650091;
3. 云南省软件工程重点实验室,云南 昆明 650091

Parallel accelerated method of batch RSA based on multi-core processor

LI Yun-fei[1], LIU Qing[2,3], LI Tong[2,3], ZHOU Bao-lin[1], PENG Hua[1]

1. School of Information Science and Engineering,Yunnan University,Kunming 650091,China;
2. National Pilot School of Software,Yunnan University,Kunming 650091,China;
3. Key Laboratory in Software Engineering of Yunnan Province,Kunming 650091,China

- 摘要
- 参考文献
- 相关文章

全文: PDF (646 KB) HTML (1 KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 为了改善RSA算法解密和签名的性能,Fiat提出了batch RSA算法,但效果并不显著.针对现有计算机多核的特点,对batch RSA算法进行并行优化,使其在解密和签名时的速度得到大幅度提升,实验表明并行优化后平均加速比可达到4.75.

关键词： batch RSA 加速 并行 多核

Abstract： Fiat had put forward the batch RSA to speed up the decryption and signing,but it wasn't very effecient.Considering the multi-core feature of present computers,this paper focused on the parallel optimization of batch RSA in order to further speed up decryption and signing.Experiments finally showed that the speedup can reach a factor of 4.75.

Key words：

收稿日期: 2010-03-23;

通讯作者: 柳 青(1963-),男,云南人,教授,主要从事软件工程、信息安全方面的研究.

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 李云飞
- 柳青
- 李彤
- 周保林
- 彭华

引用本文:

李云飞,柳青,李彤等. 基于多核的批处理RSA的并行加速方法[J]. 云南大学学报(自然科学版), 2011, 33(1): 22-26 .

$author.xingMing_EN,$author.xingMing_EN,$author.xingMing_EN et al. Parallel accelerated method of batch RSA based on multi-core processor[J]. , 2011, 33(1): 22-26 .

没有本文参考文献

[1] 李云飞 柳青 李彤 郝林 . 基于Multi-Power的批处理RSA算法的研究[J]. 云南大学学报(自然科学版), 2011, 33(3): 271-274, .

[2] 陈英涛 戴宏 唐翰犀. 8位600MS/s CMOS超高速并行模数转换器的仿真分析与设计[J]. 云南大学学报(自然科学版), 2010, 32(3): 267-272, .

[3] 付志涛 李彤. 软件并行开发过程体系结构设计与应用[J]. 云南大学学报(自然科学版), 2009, 31(4): 341-345 .

编辑出版：云南大学学报编辑部 (昆明市翠湖北路2号, 650091)
电话：0871-5033829(传真) 5031498 5031662 E-mail: yndxxb@ynu.edu.cn yndxxb@163.com