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 (3): 271-274, DOI:

基于Multi-Power的批处理RSA算法的研究

李云飞[1], 柳青[2,3], 李彤[2,3], 郝林[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

Research of efficient variant of the Batch RSA based on Multi-Power

LI Yun-fei[1], LIU Qing[2,3], LI Tong[2,3], HAO Lin[1]

1. School of Information Science and Engineering, Yunnan University, Kunming 650091, China;
2. 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 (1063 KB) HTML (1 KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 提出一种改进的Batch RSA算法来提升Batch RSA算法的解密性能.该改进算法结合了批处理技术和Multi-Power RSA技术,在Batch RSA算法的指数计算阶段来提升Batch RSA算法的解密性能.实验结果和理论分析表明该改进算法使得Batch RSA算法的解密性能得到显著提升.

关键词： Batch RSA Multi-Power RSA 解密 加速

Abstract： This paper aims at speeding up Batch RSA decryption.An efficient variant of Batch RSA is proposed to improve the Batch RSA decryption performance.The improved Batch RSA variant speeds up decryption by combining the batch technique and multi-power RSA technique in the exponentiation phase .The experimental result and the theoretical values show that the speed of the decryption has been substantially improved.

Key words：

收稿日期: 2010-11-08;

通讯作者: 柳 青(1963-),男,云南人,教授,主要从事软件工程与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
- 郝林

引用本文:

李云飞,柳青,李彤等. 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, .

$author.xingMing_EN,$author.xingMing_EN,$author.xingMing_EN et al. Research of efficient variant of the Batch RSA based on Multi-Power[J]. , 2011, 33(3): 271-274, .

没有本文参考文献

[1] 李云飞 柳青 李彤 周保林 彭华 . 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 .

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