

王潮, 时向勇, 牛志华. 基于Montgomery曲线改进ECDSA算法的研究[J]. 通信学报, 2010, (1):9~13

基于Montgomery曲线改进ECDSA算法的研究

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[王潮](#)

[时向勇](#)

[牛志华](#)

摘要点击次数: 443

全文下载次数: 286

中文摘要:

提出了一种基于Montgomery曲线改进ECDSA算法, 并重点改进异步步点乘问题。改进的ECDSA具有更快的计算速度并能有效的抵御时间攻击和能量攻击, 将验证签名与产生签名时间之比从2倍降低到约1.2倍, 减少约40%, 算法对提高椭圆曲线密码的实现效率有一定意义。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

[关闭](#)

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/881 电子邮件: xuebao@ptpress.com.cn

技术支持: 北京勤云科技发展有限公司