

软件技术与数据库

基于数据流分析的寄存器参数恢复方法

方霞, 尹青, 蒋烈辉, 黄海, 何红旗

(解放军信息工程大学信息工程学院, 郑州 450002)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对在反编译IA32体系结构可执行程序过程中涉及的寄存器参数恢复问题, 基于IA32适用的ABI约定, 分析寄存器参数的特征, 借鉴数据流分析中到达-定义分析及使用-定义链等经典方法, 利用寄存器定义和使用等信息, 提出一种寄存器参数的识别、处理及实参恢复的方法。

关键词 [反编译](#); [寄存器参数](#); [参数恢复](#); [数据流分析](#)

分类号 [TP311.12](#)

DOI:

通讯作者:

作者个人主页: [方霞](#); [尹青](#); [蒋烈辉](#); [黄海](#); [何红旗](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (129KB)

▶ [\[HTML全文\]](#) (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“反编译; 寄存器参数; 参数恢复; 数据流分析”的相关文章](#)

▶ [本文作者相关文章](#)