

产品、研发、测试

## 静态二进制翻译中间接过程调用恢复技术研究

丁松阳 赵荣彩

河南财经学院计算机科学系 中国科学院计算技术研究所

收稿日期 2006-2-23 修回日期 网络版发布日期 2007-2-14 接受日期

**摘要** 间接过程调用的恢复问题是静态二进制翻译中的难点之一。针对使用c后端的静态二进制翻译框架, 提出并实现间接过程调用恢复方法, 该方法结合代码间隙分析, 在后端c代码生成过程中插入映射源过程地址到目标机过程地址的代码。相对于使用解释器的方法, 该方法具有实现简洁、在目标机上运行速度更快的优点。

**关键词** [静态二进制翻译](#) [间接过程调用](#) [解释器](#) [代码间隙](#)

分类号

## The Recovery of Indirect Procedure Call for Static Binary Translation

### Abstract

The recovery of indirect procedure call is a difficult problem in static binary translation. For the static binary translation of using c language as backend, this paper put forward a technique of analyzing the gap code and plugging codes into the target programs that searching the target procedure address basing on the source procedure address. This method can be implemented effectively. It has the advantage of code running faster in the target.

**Key words** [Static binary translation](#) [Indirect procedure call](#) [Interpreter](#) [Code gap](#)

DOI:

通讯作者 丁松阳 [dingsongyang@yahoo.com.cn](mailto:dingsongyang@yahoo.com.cn)

### 扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(0KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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](#)

▶ [复制索引](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“静态二进制翻译”的相关文章](#)

▶ [本文作者相关文章](#)

· [丁松阳 赵荣彩](#)