2024年主要工作总结与展望

徐瑞阳

2025 年 1 月 15 日

2024 年概览

1 月 ～ 4 月

- 华为研究项目 ("切片代码仿真验证技术", PI, 2023-24)

5 月 ～ 6 月

- 完成本科毕业设计，成功毕业

6 月 ～ 10 月

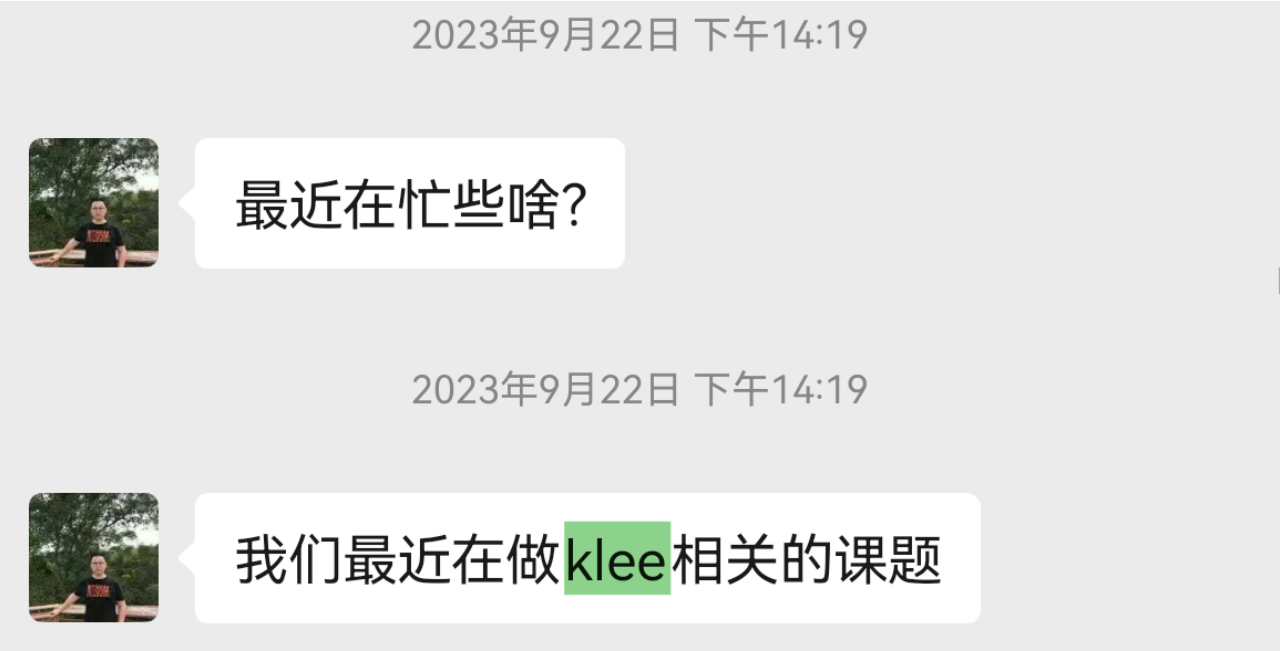
- 投稿论文，被拒再投
- IFSE: Taming Closed-box Functions in Symbolic Execution via Fuzz Solving

10 月 ～ 12 月

- 调研课题

项目到底做了什么？

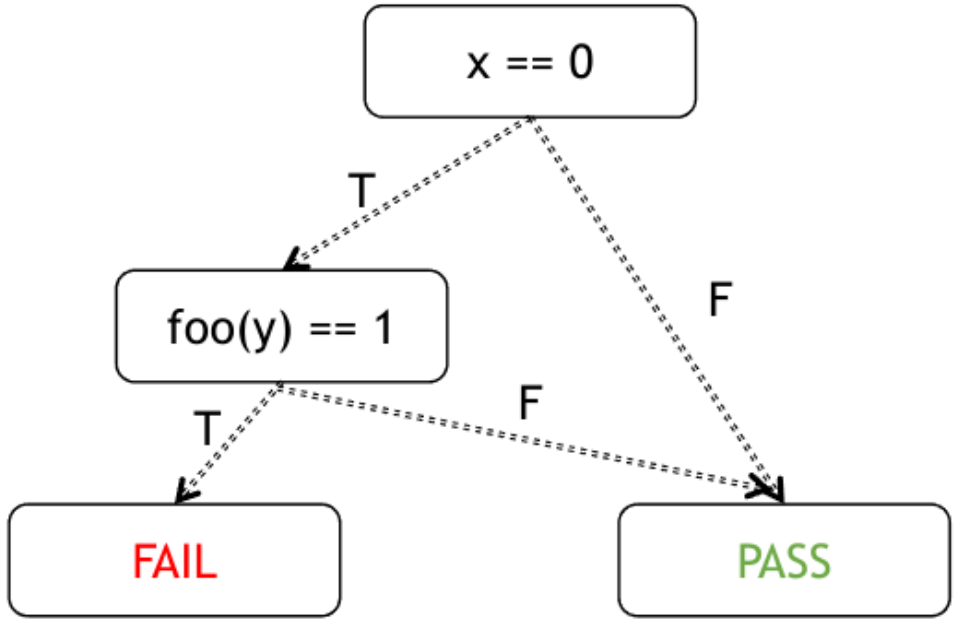
这得从符号执行引擎 klee 说起



符号执行

符号执行 (Symbolic Execution) 是一种软件分析技术，使用符号变量代替具体值作为输入, 并通过生成路径约束条件来判断这些条件是否可满足, 以确定路径的可行性

```
1 int foo(int r) { return r;}
2
3 if (x == 0) {
4   if (foo(y) == 1) {
5     assert(0 && "Bug");
6   }
7 }
8 printf("PASS");
```



例如, 上述通向 Bug 的路径约束为 *{x == 0 && foo(y) == 1}*

如果能够求解出该约束（如 *x = 0, y = 1*），则代表探索到了通向 Bug 的路径

具体化机制 (*concretization*)

> 如果调用函数源码未知（*第三方库，内联汇编或者系统调用等，* 统称为**闭盒函数**）

- 随机准备一些参数
- 与闭盒函数一并丢给 JIT 编译器动态执行
- 获取具体的返回值继续进行符号执行

由于返回值是具体值，后续用到路径判断的话会严重缩减符号执行的状态搜索空间

既然闭盒函数不能静态推理，但可以动态执行，**能否大规模地去调用闭盒函数，每次变异参数的值来试探返回值，直到可以弥补丢失的状态搜索空间**（借助 fuzzing 的思想）
接下来就是在klee系统上实现，并写一个基于 fuzzing 的符合 SMT 规范的求解器

实现

2024年3月20日
又寄了，还是那个问题。

2024年3月18日
跑...寄了，刚刚那个问题是“快 30...

2024年3月18日
跑了快30min，寄了

2024年3月18日
又寄了

2024年3月30日
刚从医院回来，有点累

2024年3月29日
你有急事吗？我今天有点累

2024年3月27日
我现在有点累

2024年3月23日
去睡了[捂脸]累的我心脏砰砰跳

2024年3月23日
...天真要累昏了，看vscode行号都经常看错。

2024年3月21日
昨天太累了，而且飞机晚点，有点急，不好意思

2024年3月20日
...解释这种trivial的事情搞得我快累死了

2024年3月18日
我现在比较累，休息下

2024年4月25日
...跑的时候依然挂了 REColossus 是 18.78

2024年4月25日
但是现在挂的非常快，3min 就挂了

2024年4月25日
挂了，[图片]

2024年4月25日
关闭 stdout 测试 yes 还是挂了，还是因为 lar...

2024年4月24日
原版 klee 跑 sort 很快就挂了 datalayout

2024年4月23日
昨天记录的是 30min 挂了

2024年4月22日
现在跑完了36个，挂了4个(其中有三个是没修...

2024年4月21日
...了： basename 又挂了，挂在添加 false dd...

2024年4月21日
...这边测完，这边总共测 41 个 挂了 7 个

2024年4月21日
...复了），7 个挂了，4个 Unknown（还没跑...

2024年4月21日
总共挂了几个

5 ~ 6 月

- 准备本科毕业论文
- 回母校吉大参加毕设答辩

7～8月

有充足的时间去思考事情，同时读了许多书

- Plato. *The Republic.* Translated by Allan Bloom. New York: Basic Books, 1968.
- Plato. *The Republic.* Translated by Benjamin Jowett. Oxford: Clarendon Press, 1871.
- Plato. *The Apology of Socrates*. Translated by Fei Wu. Huaxia Publishing House, 2017
- Fei Wu. *A Commentary on The Apology of Socrates*. Huaxia Publishing House. 2017
- Allan Bloom. *An Interpretation Essay on The Republic* New York: Basic Books, 1968
- Mill, John Stuart. *On Liberty. The Commercial Press*
- Mill, John Stuart. *Utilitarianism. The Commercial Press*
- … …

10 ~ 12 月

平静且正常的研究生生活

- 整理之前项目和研究的经历，写论文投稿
- 按部就班上课，和同学们处好关系
- 徒步健身旅游爬山等


刻苦训练
vivo X200 Pro | ZEISS
2025.01.02 18:59

10 ~ 12 月 (Cont'd)

两件不太平静的事情

1. 滴水湖院区的开启

> 滴水湖院区远离政治和经济中心的边缘地质，给予大家**沉静思考，深刻追问**的契机

2. 硕转博的申请 💪

祝愿

愿大家在新的一年里，能够勇敢地面对生活：

- 能够无论何时何地保持对生活的热爱，对生活充满激情，
- 能够无论处于快乐或还是苦恼，或处于欲望还是及恐惧中，保持自己的信念

最后祝愿大家每一天过得充实，回顾自己的经历时候
能够诚实地面对自己，能够经得起审视，能够说自己活得真实

谢谢！