Group Meeting - 7

Members: Yong Li, Depeng Liu, Weizhi Feng, Xie Li, Shizhen Yu, Yutian Zhu, Zongxin Liu

2021 年 6 月 30 日

差分隐私

这俩周:

- 中期答辩;
- Aplas 期刊：其他部分初步完成；由于 MDP 算法仅是充分的，Stream 例子的 pan-privacy 分析可能有点问题，需加以解释和根据实验情况确定。
- 在调研几个部分：预估通过学习算法学得 DP 模型可行性、实际代码中的 DP 部署及验证、APPLE 的差分隐私验证、隐私参数的选取等。
- 用 SageMath 做带有绝对值的连续噪声的带参定积分，分段积分是可计算的，解决简单连续机制如 Laplace 的验证；复杂机制刻画输入输出关系方面困难一些，需尝试。

计划:

- Aplas 期刊：计划完成
- 调研部分：报告讨论一下调研情况，再具体分析后续工作。

内存安全工具开发

上周目标和进展情况：

- 将变量类型统一为字节变量并进行求解：完成
- 加入对数组和结构体的支持：基本完成，能够支持基本的结构体的处理，但在链表等复杂数据结构上还需要例子来改进
- 多个基本块的符号执行：加入了获得展开循环的所有执行路径的功能，还未将符号执行整合。

TODOs：

- 代码的重构
- 对已处理的例子进行收集，逐步构建出 benchmark
- 调整编译选项获取结构体等信息
- 对 `memcpy()`,`memset()` 的语义进行调研
- 讨论过程间符号执行怎么做，函数调用图和 CFG 的结合。

下周目标：对多个基本块的符号执行，找更多的例子运行，

内存安全工具开发

文献阅读:

李勰:

[1] Thomas Ströder et al. Proving Termination and Memory Safety for Programs with Pointer Arithmetic. IJCAR'14. (**完成**)

[2] Deciding Memory Safety for Single-Pass Heap-Manipulating Programs. POPL'20. (**计划**)

宗鑫:

[1] Proteus: Computing Disjunctive Loop Summary via Path Dependency Analysis. FSE'16

冯维直

进展：

- 阅读 rank-based 和 slice-based 算法做 unambiguous Büchi automata 取补的 GandALF '20 文章，在李老师的指导下基于 spot 库实现 slice-based 的算法.
- 结合 NCSB 算法的 TACAS 文章读 seminator 和 spot 中实现 semi-deterministic Büchi automata 取补的代码.
- 基于 seminator 和 spot 提供的自动机库和接口等实现了 unambiguous Büchi automata 取补的 slice-based 的算法，运行结果有些问题，需要继续调试.

计划：

- Slice-based 算法正确实现成功运行，进行实验，和李老师讨论，在 GandALF '20 文章基础上写实验部分的章节.