IceBear: A Fine-Grained Incremental Scheduler for C/C++ Static Analyzers

肖瑜，马旭桐，李知霖，严俊

FSE Companion 25, 2025 年 6 月 23 - 28 日

联系方式：严俊 yanjun@otcaix.iscas.ac.cn

科研背景与挑战（Background & Challenges）

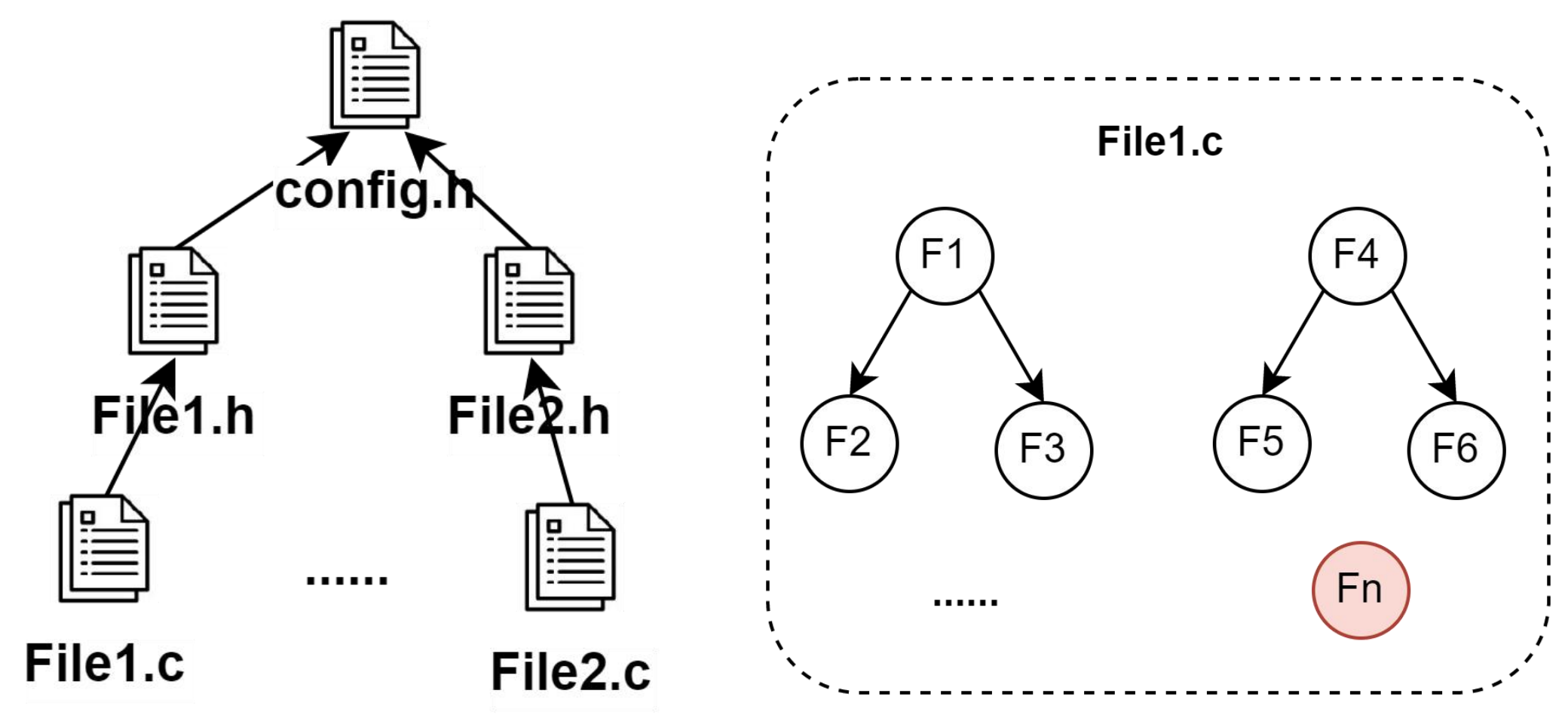
静态分析是保障C/C++软件质量的关键技术。在快速迭代的开发现实中，开发者频繁修改代码，需要分析工具快速反馈新引入的缺陷。现有分析工具的调度器（如CodeChecker），仅支持文件级的增量调度，研究表明大多数修改可能仅涉及少量函数，**文件级增量调度粒度仍然过粗**。IceBear实现**函数级别**的细粒度增量静态分析调度，大大提高了多款分析工具在真实应用场景下的分析效率。

IceBear框架概览（IceBear Framework）

IceBear是一个为C/C++静态分析器（支持CSA, Clang-tidy, Cppcheck等）设计的调度框架，旨在通过精确定位代码变更及其影响范围，减少冗余分析并过滤无关报告 。

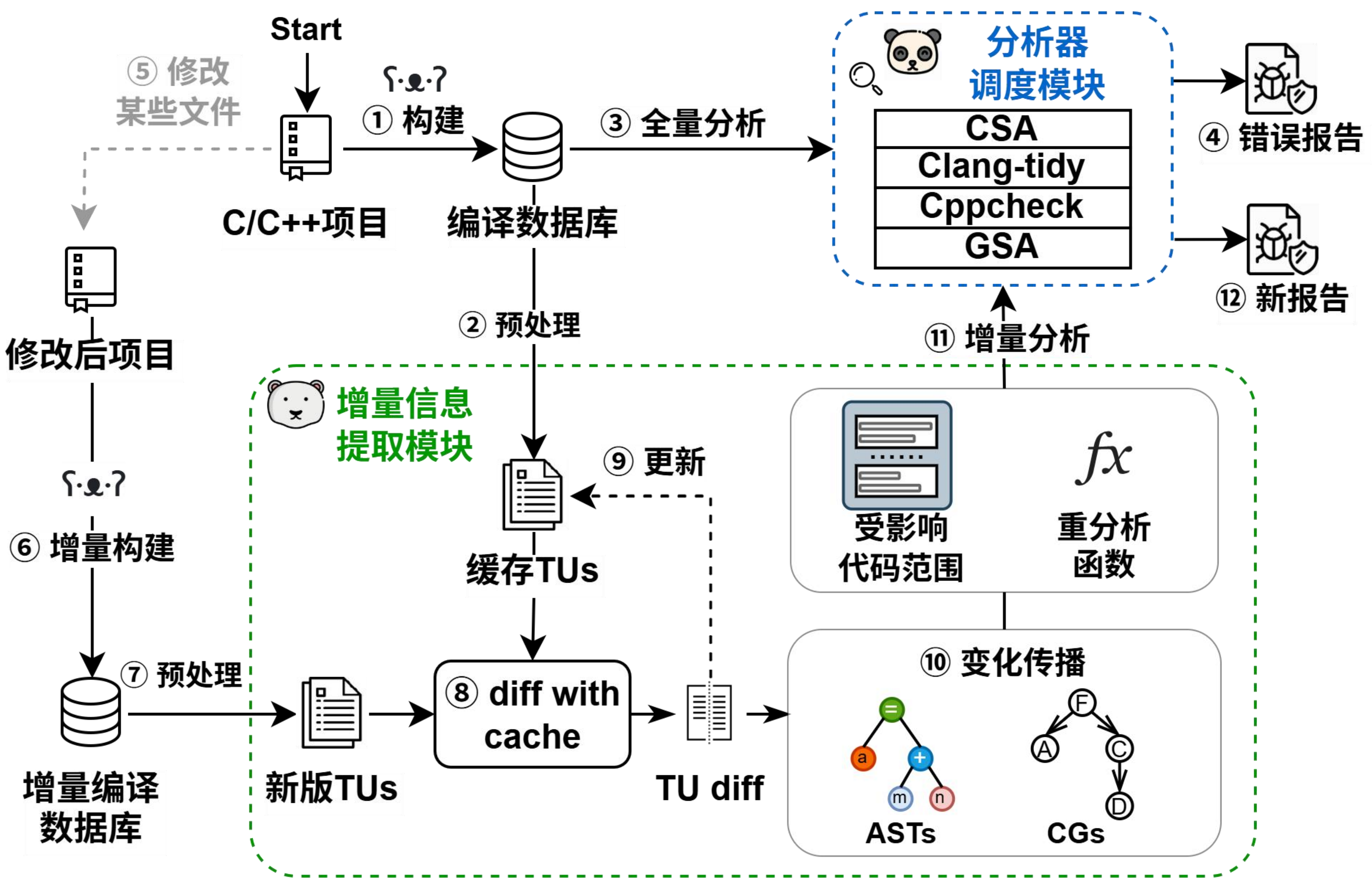
增量信息提取模块

- 精确的翻译单元级差异分析
- 细粒度的函数级变更传播



分析器调度模块

- 多种分析工具函数级增量调度
- 变更无关报告过滤



实验评估（Evaluation & Results）

选取8个C/C++流行开源项目，每个项目选择5个版本，以第一个版本为基础，后续执行增量分析，并统计增量分析时间以及产生报告数量。

Project	CSA		Clang-Tidy		Cppcheck	
	T_{IncB}	T_{IB}	T_{IncB}	T_{IB}	T_{IncB}	T_{IB}
protobuf	1,568.2	322.0	552.5	308.7	32.8	17.9
tesseract	394.5	158.2	249.1	191.8	216.6	174.4
vim	110.4	16.3	3.4	3.4	465.4	253.9
redis	146.5	44.6	5.5	5.4	244.9	11.0
openssl	358.2	12.7	91.9	23.9	492.8	218.3
FFmpeg	407.9	9.1	28.6	16.3	571.1	33.9
bitcoin	648.9	338.1	456.5	394.3	6.6	3.8
grpc	328.2	135.1	395.1	380.0	14.3	11.0
Total	3,962.6	1,036.0	1,782.8	1,323.7	2,044.6	724.1
Reduction		73.86%		25.75%		64.58%

Project	CSA		Clang-Tidy		Cppcheck	
	R_{IncB}	R_{IB}	R_{IncB}	R_{IB}	R_{IncB}	R_{IB}
protobuf	224	28	10,326	761	25	10
tesseract	397	187	2,347	294	951	767
vim	124	6	351	7	131	107
redis	268	71	892	64	8	2
openssl	1,261	2	8,588	27	605	49
FFmpeg	728	9	6,229	61	729	410
bitcoin	83	39	2,220	134	64	64
grpc	56	6	3,977	9	0	0
Total	3,141	348	34,930	1357	2,513	1,409
Reduction		88.92%		96.12%		43.93%

研究的意义与应用（Significance & Application）

在多个大型真实开源软件上的实验表明，相较于传统的基于增量构建的增量调度策略，IceBear能够减少**60.4%**分析时间，过滤**92.3%**的无关报告。并且IceBear已成功支持4种C/C++静态分析工具，展现了IceBear较强的可扩展性。