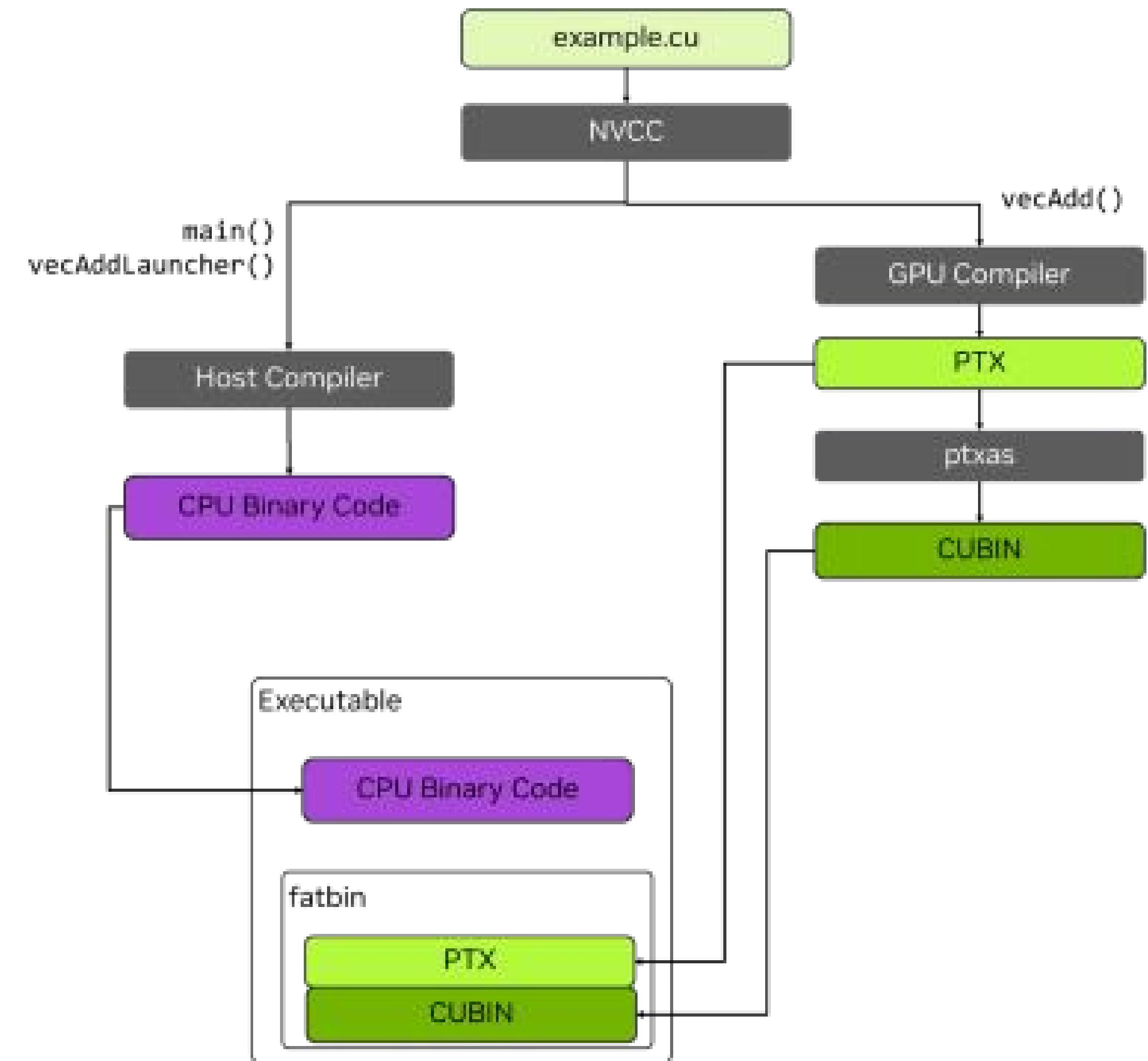


숨겨진 GPU ISA 보안 분석환경 구축

컴퓨터공학과 홍지환

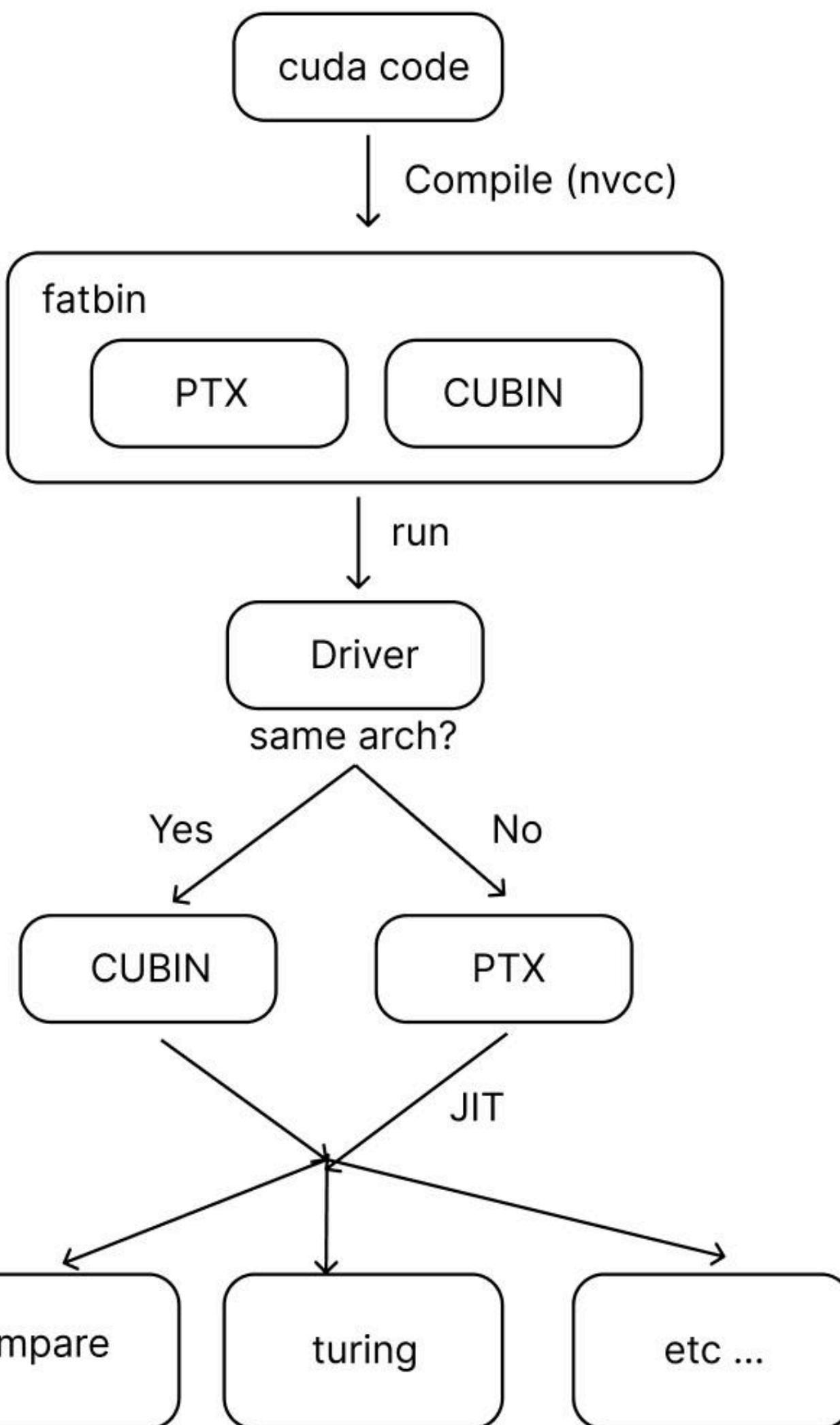
cuda 코드 컴파일 구조

1. cuda 코드 작성
2. 컴파일러로 컴파일 (nvcc)
3. nvcc가 cpu코드와 gpu코드 분리
4. gpu코드는 ptx 및 cubin으로 컴파일

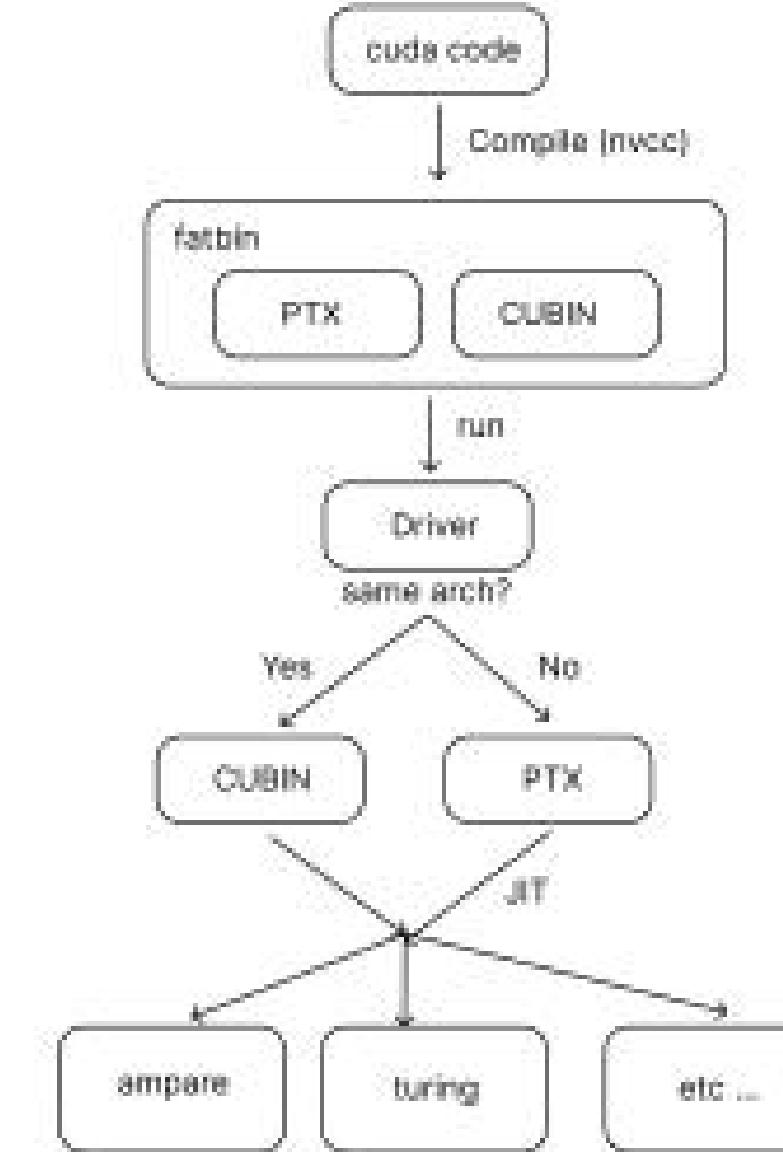
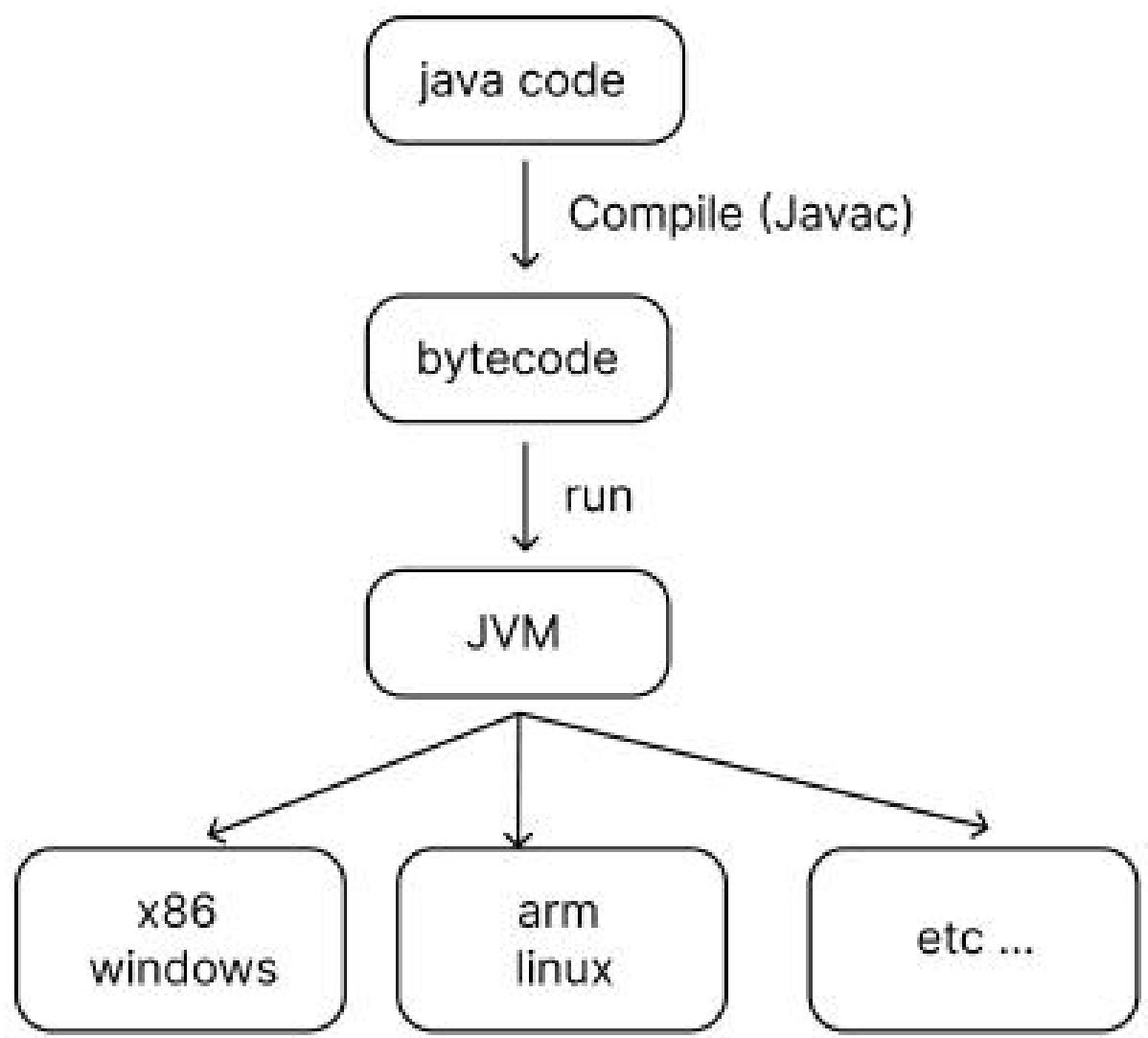


cuda 코드 컴파일 구조

- PTX: 중간 코드
- CUBIN: 특정 아키텍쳐의 바이너리



Java vs Cuda



Java

JVM을 이용하여 각 환경에 맞게 동작

CUDA

Driver를 통해 각 환경에 맞게 동작

숨겨진 ISA 찾기

cubin 변경

- 간단한 CUDA 코드 작성
- 컴파일 후 binary 수정

숨겨진 ISA 찾기

Open Source 활용

- 큰 규모의 오픈소스 이용
- disassembler 이용하여 해석되지 않는 부분 확인

Reference

<https://www.pnfsoftware.com/blog/reversing-nvidia-cuda-sass-code/>

https://docs.nvidia.com/gameworks/content/developertools/desktop/ptx_sass_assembly_debugging.htm

<https://developer.nvidia.com/blog/understanding-ptx-the-assembly-language-of-cuda-gpu-computing/>