Emulacja 8086 używając nowoczesnego jezyka C++

Patryk Kaniewski

March 15, 2021

1 Cel

Zbudowanie biblioteki do emulacji 8086 w C++17, a nastepnie zbudowanie na jej podstawie emulatora 8086 ktory mozna byłoby wykonywać proste programy DOS.

2 Motywacja

8086 jest jednoczesnie dostyć prostą architektura (ograniczona liczba instrukcji w porównaniu do nowoczesnego x86 z dużą liczbą rozszerzeń) i posiada tylko realmode

3 Używane technologie

- C++17
- GCC
- cmake
- tinyasm
- ncurses

4 Spis czynnosci

- disasembler 8086

- zbudowanie toolchaina (uzywajac nasm i bash) do latwego assemblowania i uruchamiania kodu 8086
- zbudowanie systemu debugowania (register dump, memory dump, single step)
- interpretacja instrukcji 8086
- implementacja wywolan systemowych DOS/BIOS
- implementacja instrukcji zmiennoprzecinkowych 8087
- wolf3d

5 Spis tresci

6 Referencje

6.1 SoK: All You Ever Wanted to Know About x86/x64 Binary Disassembly But Were Afraid to Ask

`https://arxiv.org/abs/2007.14266`

6.2 Verifying x86 Instruction Implementations

https://arxiv.org/abs/1912.10285

6.3 The INTEL® 8087 numeric data processor

https://dl.acm.org/doi/10.1145/1500518.1500674

6.4 Design and Implementation Techniques of the 8086 C Decompiling System

https://apps.dtic.mil/sti/citations/ADA294633

6.5 Formal Specification of the x86 Instruction Set Architecture

https://publikationen.sulb.uni-saarland.de/handle/20.500.11880/26394