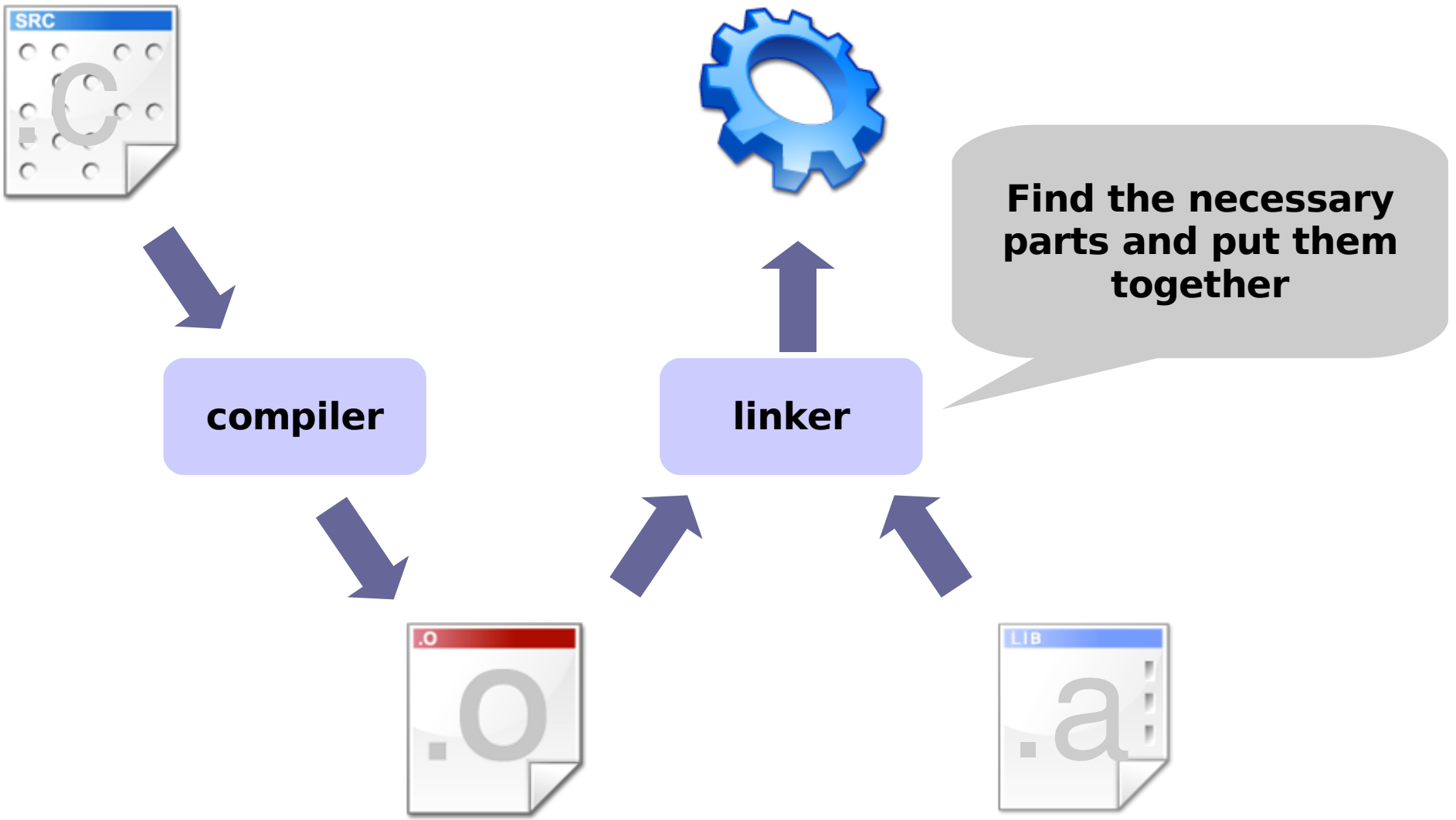



Diablo: a reliable, retargetable and extensible link-time rewriting framework

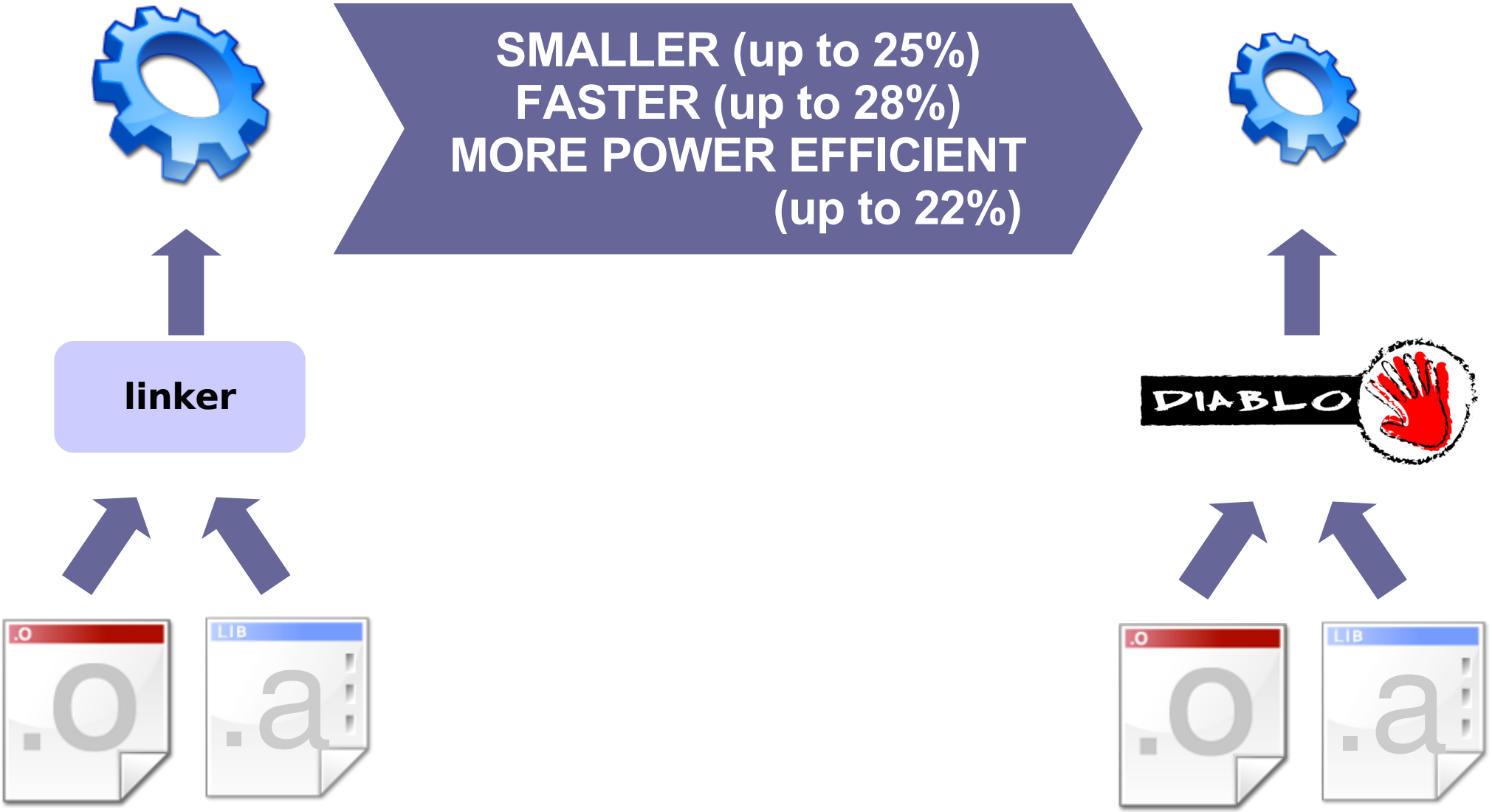
Ludo Van Put, Dominique Chanet, Bruno De Bus,
Bjorn De Sutter and Koen De Bosschere

ISSPIT'05 – Athens, Greece
19/12/05

Contemporary linkers hardly optimize programs...



...although it's very useful.

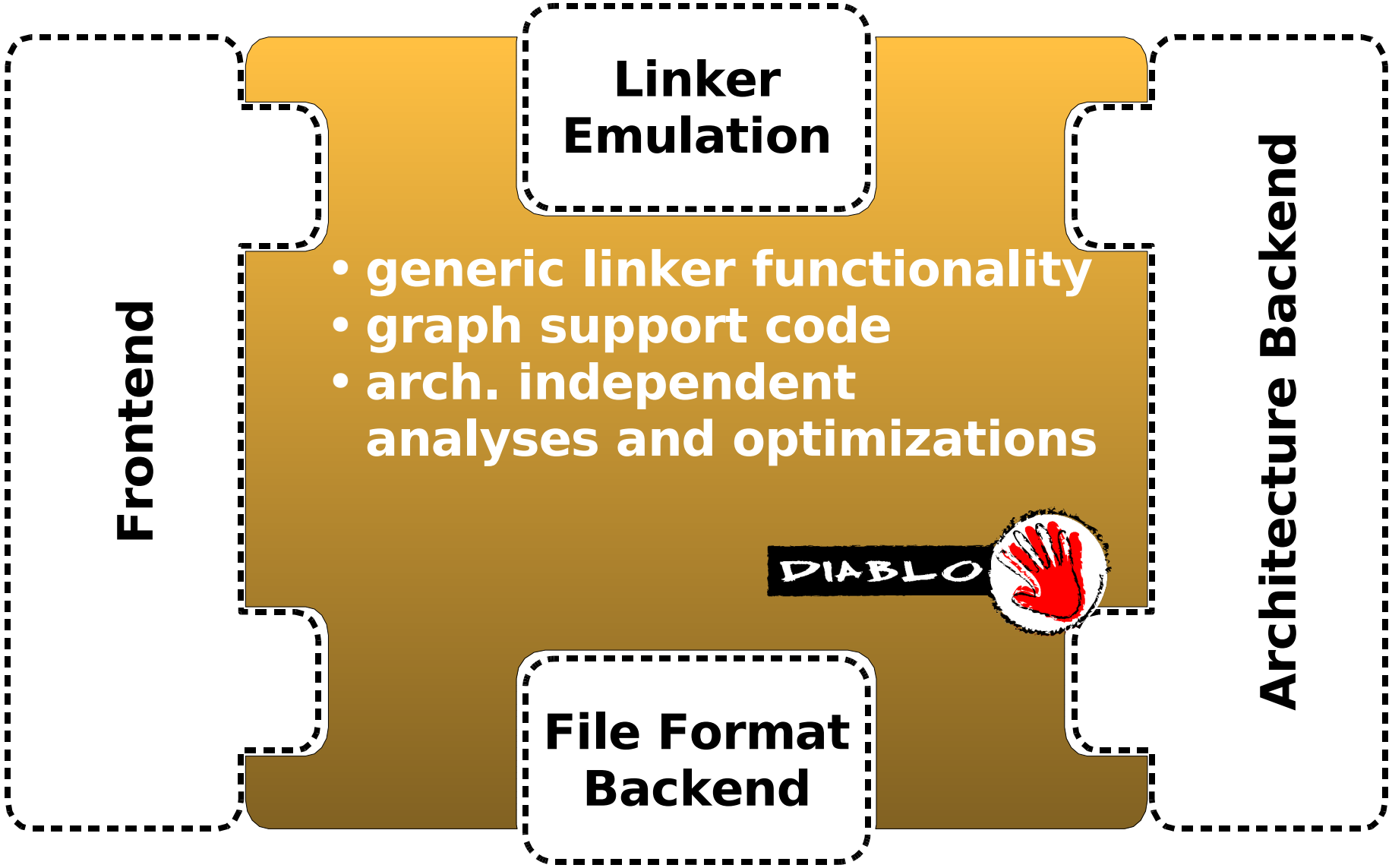


Link-time rewriting framework: safe, ...

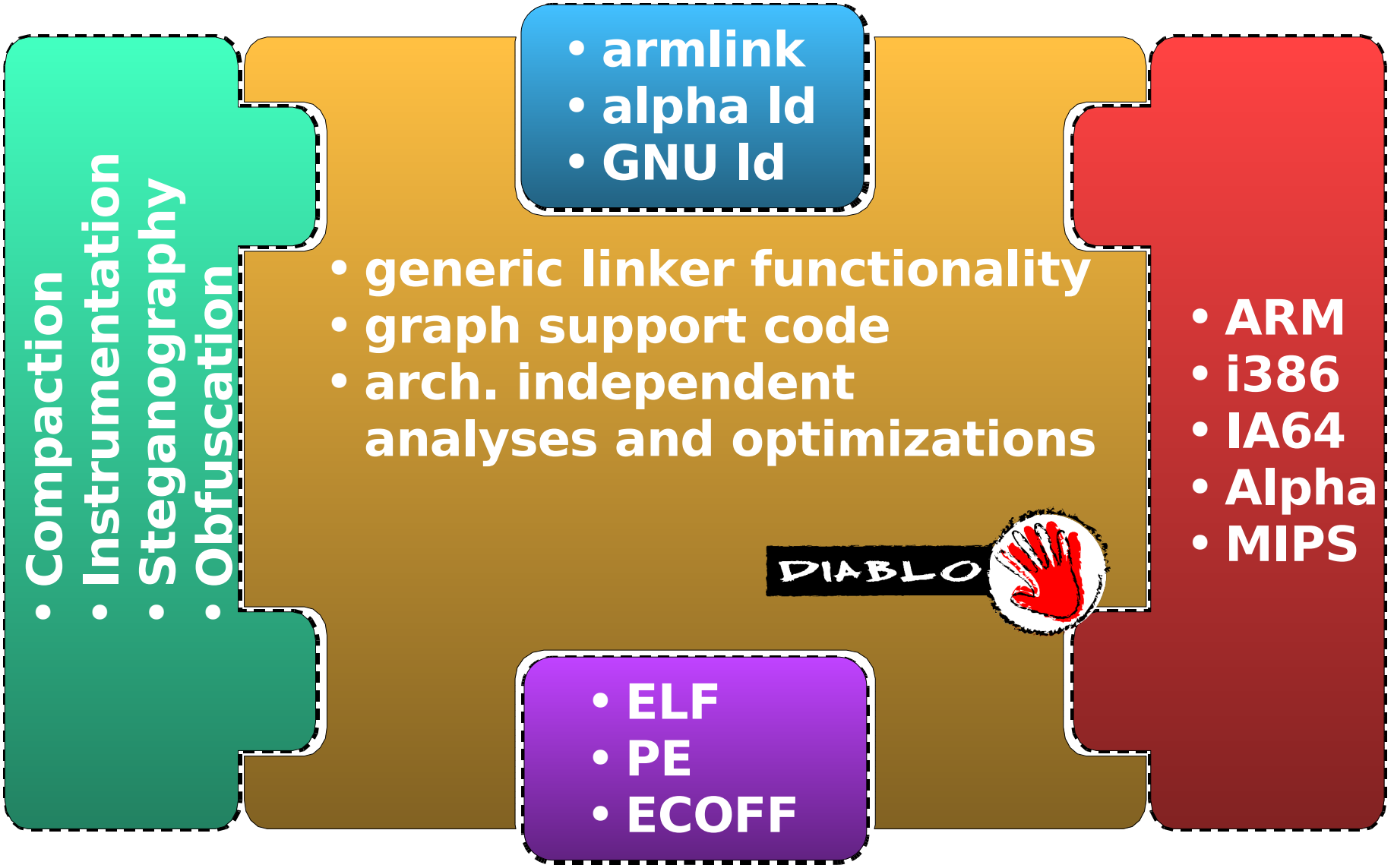
Use all available information:

- **linker (relocations,symbols,...)**
- **ABI/calling conventions**
- **pattern detection**
- **conservative fallback mechanism**

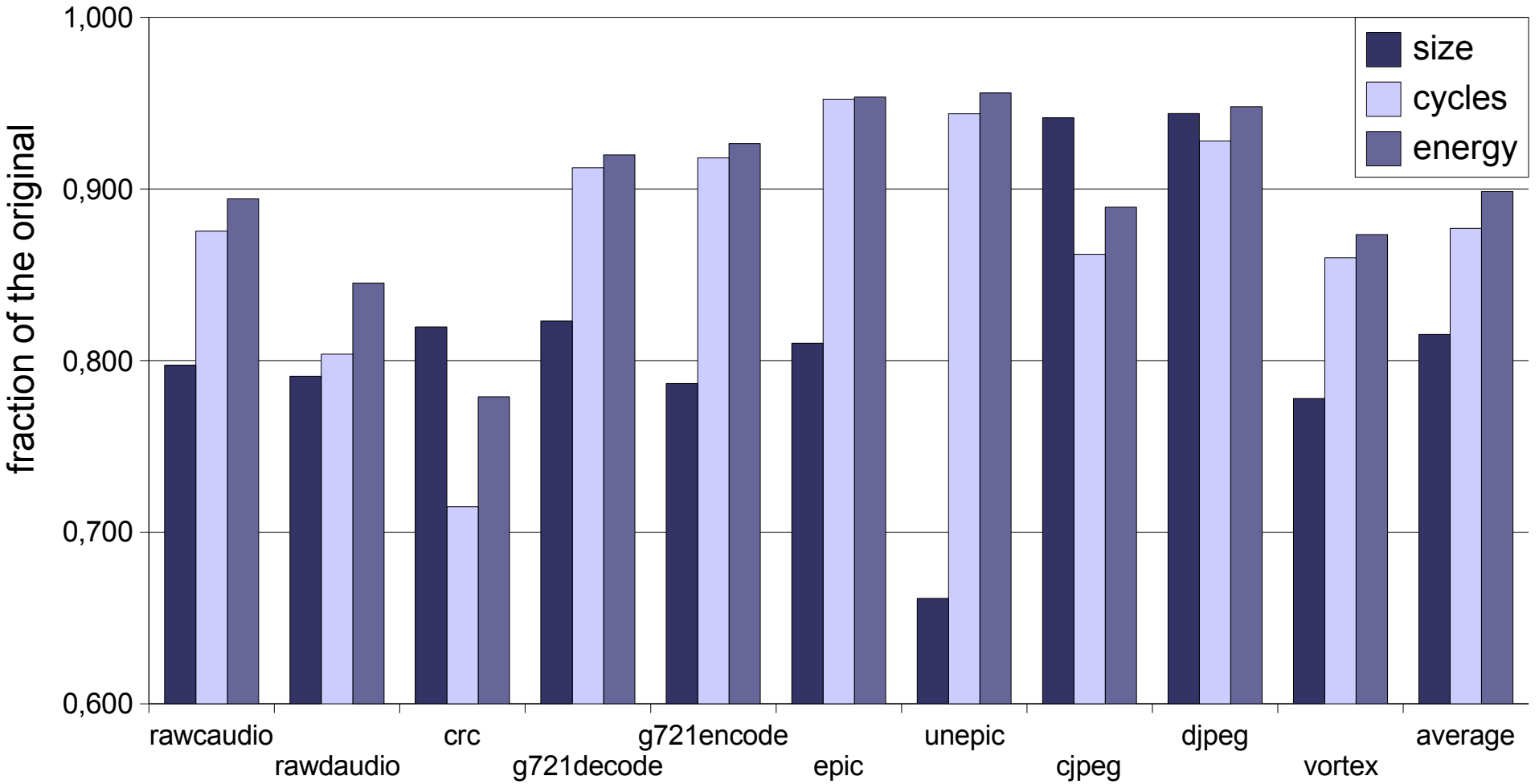
... extensible & retargetable



Extensible & retargetable



Significant compaction



ARM RVCT2.1 compiler for StrongARM platform

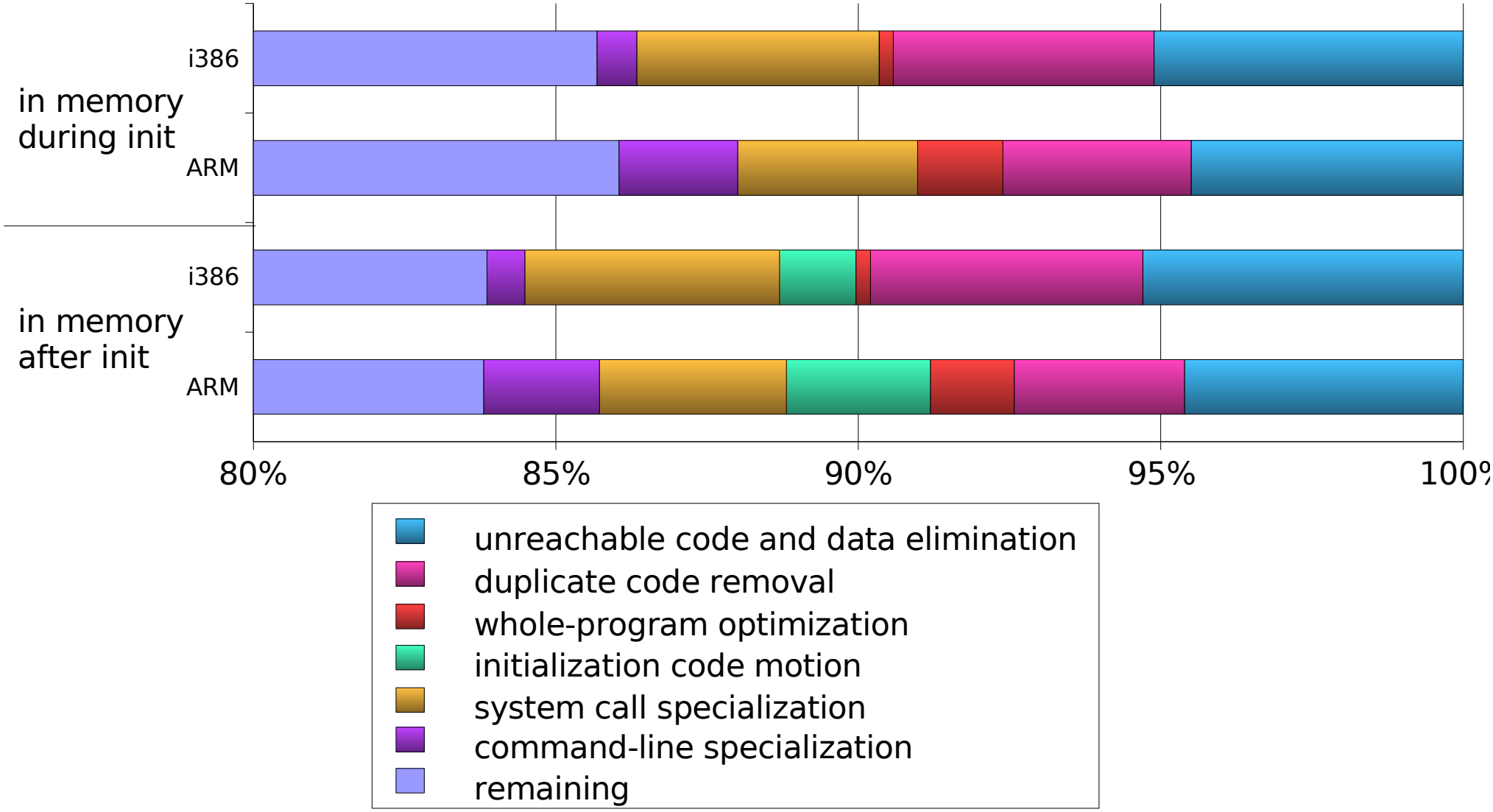
Kernel specialization

+ Free
+ No vendor lock-in
+ Full control over source
  and fast time to market

+ Kernel size

150kiB – 800kiB ↔ 25kiB – 60kiB

16% kernel size reduction



Research platform, many applications:

instrumentation (FIT)

obfuscation (LOCO)

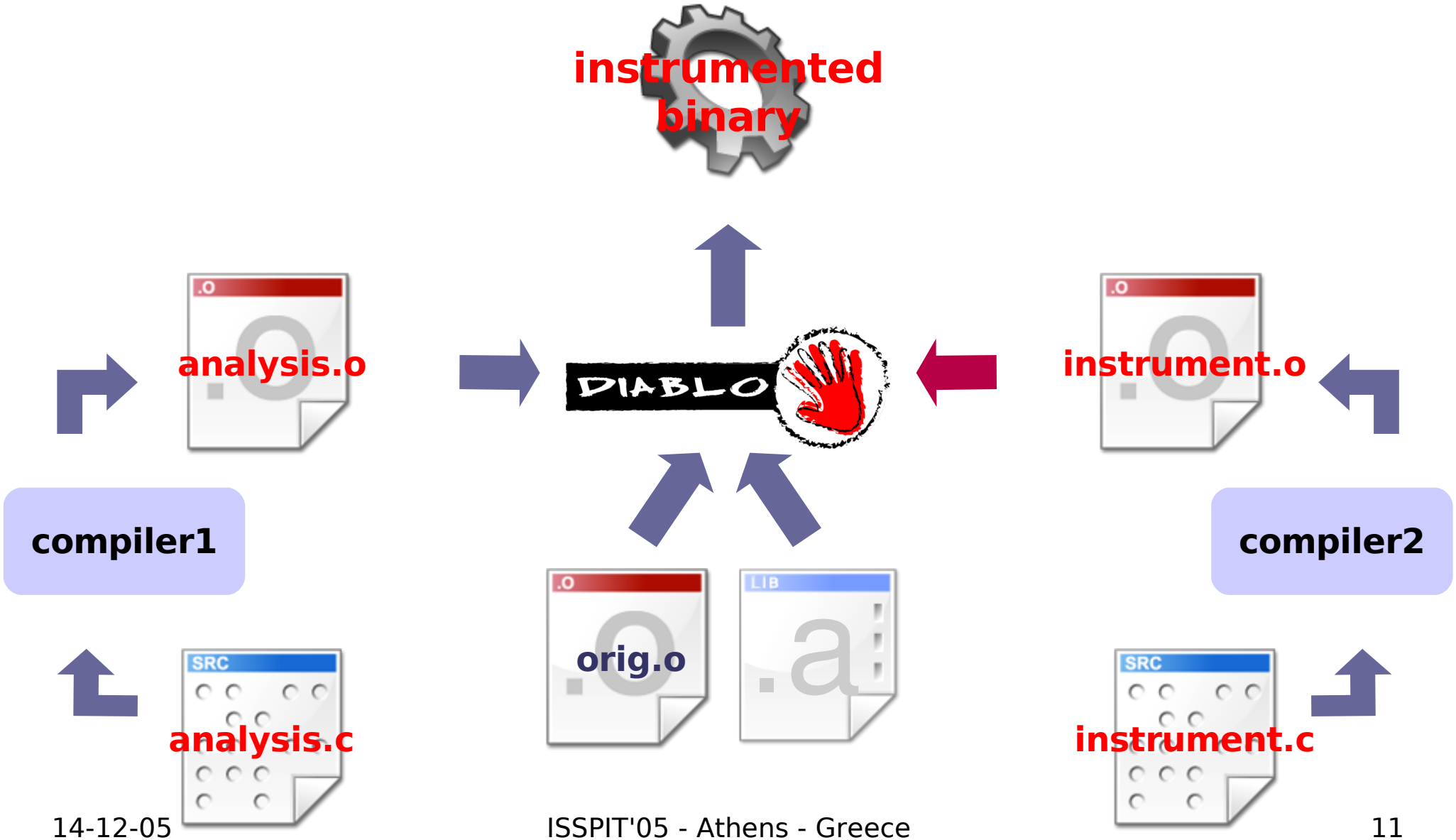
steganography (STILO)

program visualization & analysis (LANCET)

watermarking

program surgery (LANCET)

Generate custom instrumentors



http://www.elis.ugent.be/diablo

google: diablo linker

Link-time rewriting