
How to provide proof that software is bug-free? Verified compilation to the rescue

Sandrine Blazy*¹

¹IRISA – Université de Rennes – France

Résumé

Deductive verification provides very strong guarantees that software is bug-free. Since the verification is usually done at the source level, the compiler becomes a weak link in the production of software. Verifying the compiler itself provides guarantees that no errors are introduced during compilation. This talk will illustrate this approach through CompCert, the first fully verified compiler for C that is actually usable on real source code and that produces decent target code on real-world architectures. More generally, this approach opens the way to the verification of software tools involved in the production and verification of software.

*Intervenant