MEI/MiEI UC de Laboratório de Engenharia Informática

Verificação Relacional para o Frama-C

Contexto:
A verificação relacional de programas é uma extensão à Lógia de Hoare que permite raciocinar sobre pares de programas (e.g. para estabelecer a sua equivalência). Trata-se de um formalismo que foi recentemente explorado com muito sucesso na formalização de provas de segurança de primitivas criptográfica, dando origem ao sistema EasyCrypt.

Objectivo:
Com este projeto pretende-se demonstar a utilizada e viabilidade de se estender um sistema genérico de verificação de programas escritos na linguagem C, com um mecanismo que suporte a verificação relacional de programas.

Projeto:
O projecto consiste em desenvolver um plugin para o sistema Frama-C que permita algum tipo de suporte à verificação relacional de programas, por via da tradução e interligação ao sistema EasyCrypt. Note-se que a dimensão do projecto obriga a focar num protótipo *proof-of-concept*, em que identifica uma utilização típica do raciocínio relacional ao nível do código fonte (e.g. equivalência entre duas definições de função), e mostrar como esse problema pode beneficiar de uma tradução para o sistema EasyCrypt.

A área científica deste projecto é a confluência dos Métodos Formais e a Criptografia (mas com um peso muito forte da primeira).

Acompanhamento:
Este projeto será acompanhado por José Carlos Bacelar (jba@di.uminho.pt), Jorge Sousa Pinto (jsp@di.uminho.pt) e por membros do grupo de Criptografia do HASLAB que fazem uso do sistema EasyCrypt nos seus projectos de investigação.