MEI/MiEI UC de Laboratório de Engenharia Informática

Correcção de Circuitos Booleanos

Contexto:
Muitos protocolos criptográficos, em especial na área da *Secure Multi-Party Computation (SMC)*, exprimem as funcionalidades pretendidas por intermédio de Circuitos Booleanos. A adopção de um modelo computacional de tão baixo nível obriga normalmente a recorrer a ferramentas de conversão que, a partir de descrições de funcionalidades de mais alto nível (e.g. programa C), produzam os circuitos Booleanos correspondentes.

Objectivo:
Com este projeto pretende-se formalizar a tradução de um circuito booleano que faz uso de "portas" de alto nível (e.g. adição de 32bit) em circuitos booleanos elementares (i.e. que só fazem uso de portar `xor` e `and`).

Projeto:
O projecto, a ser desenvolvido no sistema de prova assistida Coq (http://coq.inria.fr), consiste na formalização de circuitos booleanos e na demonstração de equivalência circuitos que recorrem a "portas" de alto nível (e.g. aritmética 32bit) e circuitos que só recorrem a portas elementares (`xor` e `and` binárias).
Note que, mesmo se a área de aplicação é a criptografia e SMC, o projecto acaba por situar muito mais na área da Verificação Formal e utilização de demonstradores de teoremas.

Acompanhamento:
Este projeto será acompanhado por José Carlos Bacelar (jba@di.uminho.pt) e Maria João Frade (mjf@di.uminho.pt). É ainda previsível que possa vir a ser integrado em projectos mais abrangente que se encontram a ser desenvolvidos no grupo de Criptografia do HASLAB.