MEI/MiEI UC de Laboratório de Engenharia Informática

Implementação Certificada e Eficiente do SHA3

Contexto:

A implementação de algoritmos criptográficos é particularmente desafiante porque combina a necessidade de maximizar a eficiência com a de garantir a correcção e segurança da implementação. Esses dois requisitos eram até à muito pouco tempo incompatíveis, porque a procura da máxima eficiência obrigava a recorrer a linguagens de programação de muito baixo nível (tipicamente assembly), quando as metodologias/ ferramentas de verificação só se adequavam a linguagens de alto nível. Recentemente surgiram no entanto propostas que permitem reconciliar esses dois mundos, como as ferramentas que serão exploradas no âmbito deste projecto.

Objectivo:

Com este projeto pretende-se realizar o estudo de implementações do algoritmo SHA3 por forma a garantir o melhores níveis de eficiência (para diferentes arquitecturas/ variantes de processadores), sem abdicar de uma argumentação sólida referente às respectivas garantias de correcção e segurança.

Projeto:

O projecto, a ser desenvolvido com recurso ao compilador certificado Jasmin (https://github.com/jasmin-lang/jasmin) e ao sistema de prova assistida EasyCrypt (https://www.easycrypt.info/trac/), consiste na transformação incremental de uma implementação de referência do algoritmo SHA3 (conforme o standard respectivo), até atingir versões que tirem partido das facilidades oferecidas pelas arquitecturas/processadores modernos, tais como instruções assembly específicas (e.g. simd, etc.). Cada um dos incrementos adoptados deverá ser acompanhado por um argumento que ateste a preservação da correcção no processo.

Acompanhamento:

Este projeto será acompanhado por José Carlos Bacelar (jba@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.