Micro-architecture simulation for verified security and performance

Vashti Galpin

School of Informatics
University of Edinburgh
Current research: modelling micro-architecture for security and performance

• Motivation
Spectre-type transient execution vulnerabilities occur at micro-architecture level and detailed reasoning is needed to understand the vulnerabilities and mitigations.

• Solution
Formal modelling of micro-architecture using a statistical approach to understand performance and security properties.
Verifying performance impacts of micro-architecture vulnerability mitigations

• **Approach**

  Stochastic modelling with CARMA allows for component-based approach using code profiling.

• **Output**

  Estimates of performance and likelihood of security properties.
Future research: micro-architecture simulation for verified security and performance

• **Objectives**

Generalise the approach to develop efficient and lightweight simulation of micro-architectural behaviour based on composition of micro-architectural elements that will allow the trade-off of security and performance.

• **Collaboration**

**EPSRC** Digital Security by Design call: closing date 7 January 2020