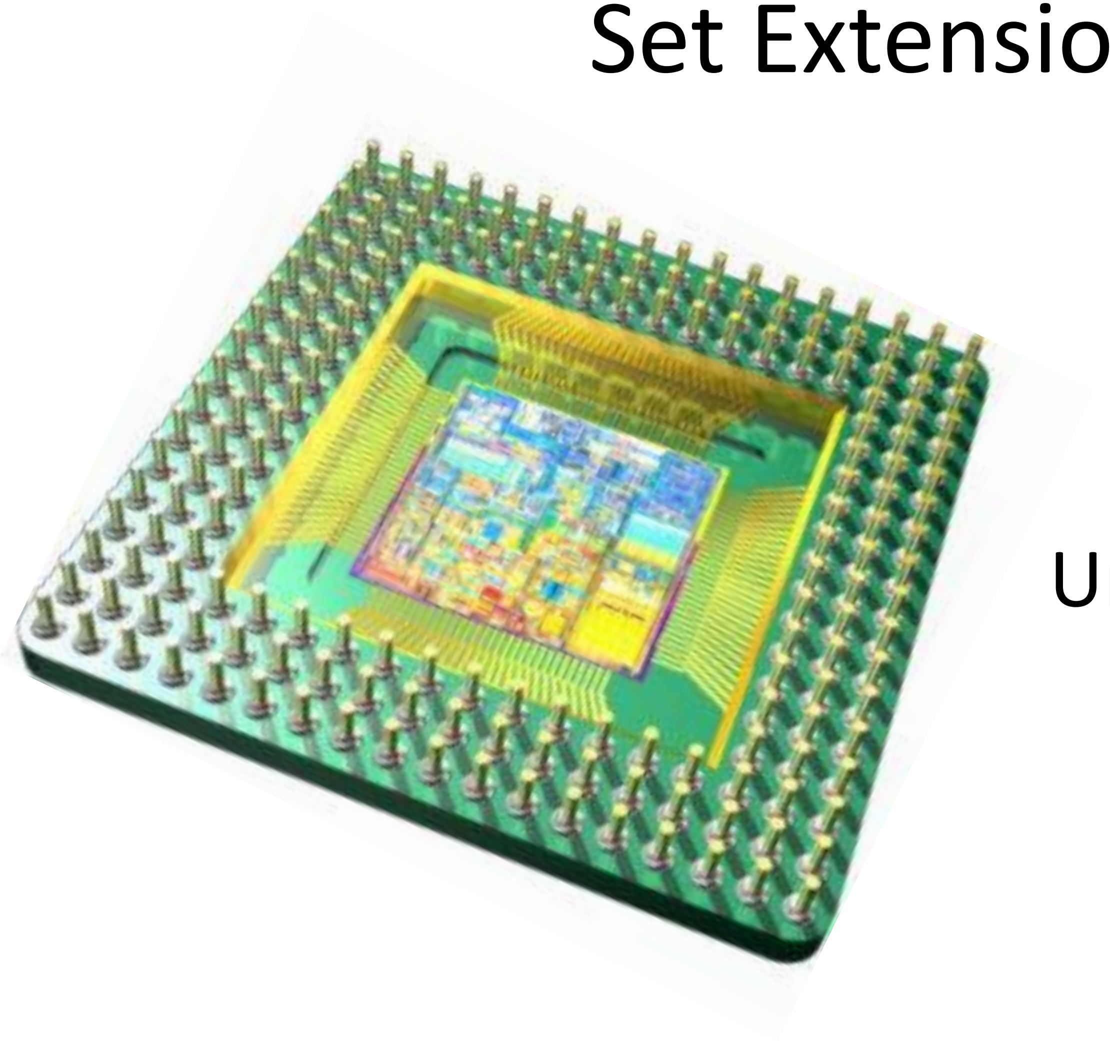
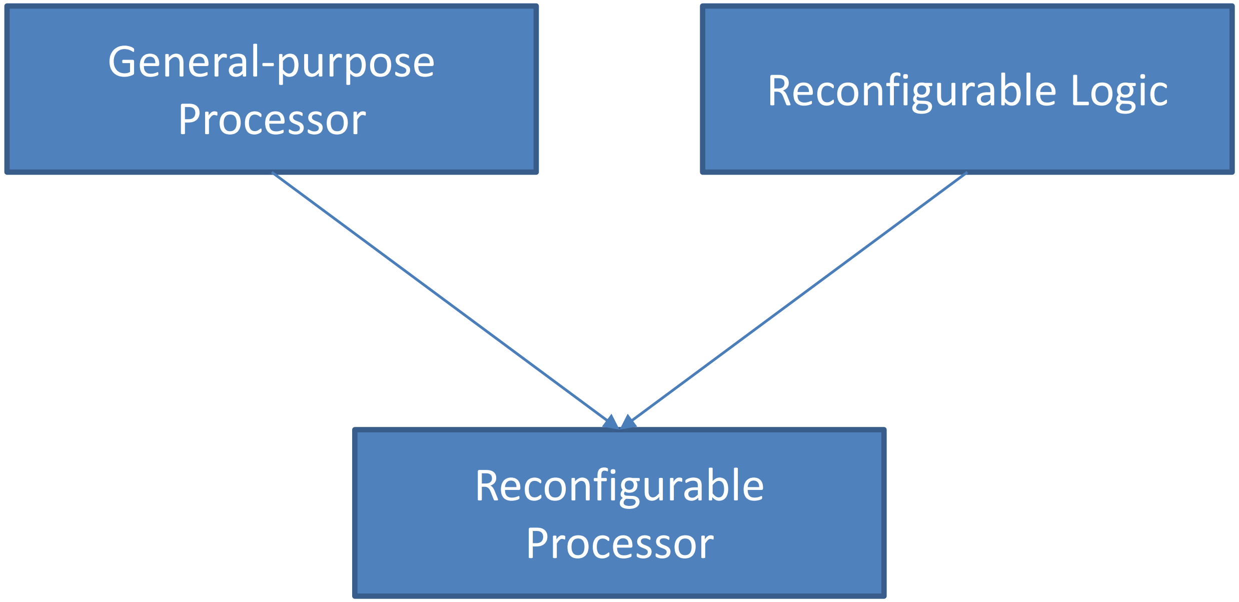
An Exploration of Mechanisms for Dynamic Cryptographic Instruction Set Extension



Philipp Grabher
University of Bristol

WEP

Instruction Set Extensions in Practice



General-purpose Processor

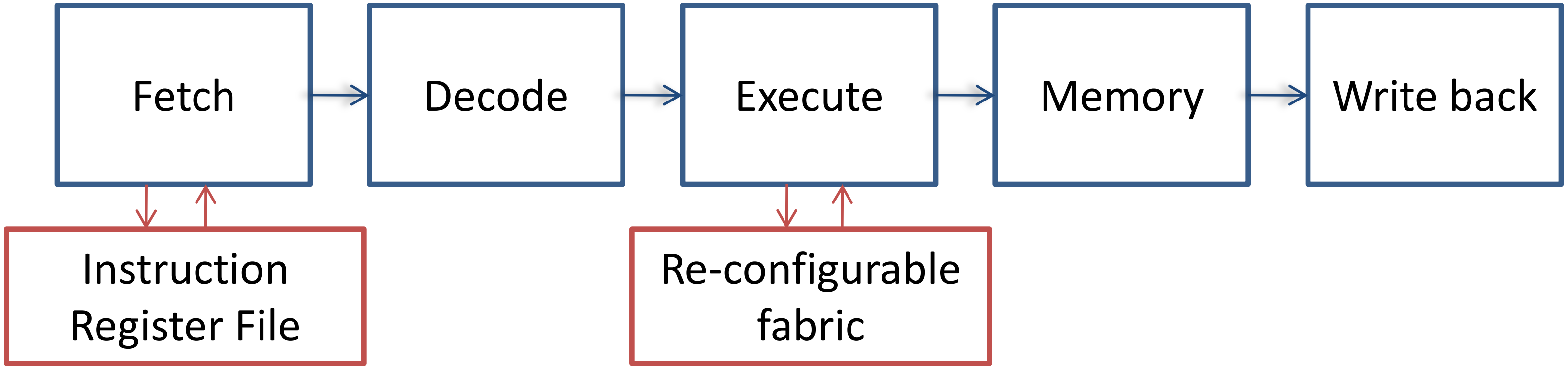
Reconfigurable Logic

Reconfigurable Processor

Main Contributions

- Implementation of Reconfigurable Processor
- Evaluation with Cryptographic Primitives
- Security Analysis

Prototype


Fetch
Decode
Execute
Memory
Write back
Instruction Register File
Re-configurable fabric

Programming Interface of Re-configurable Fabric

- GPR[dst] = f(GPR[src1], GPR[src2], imm)

Performance Improvement

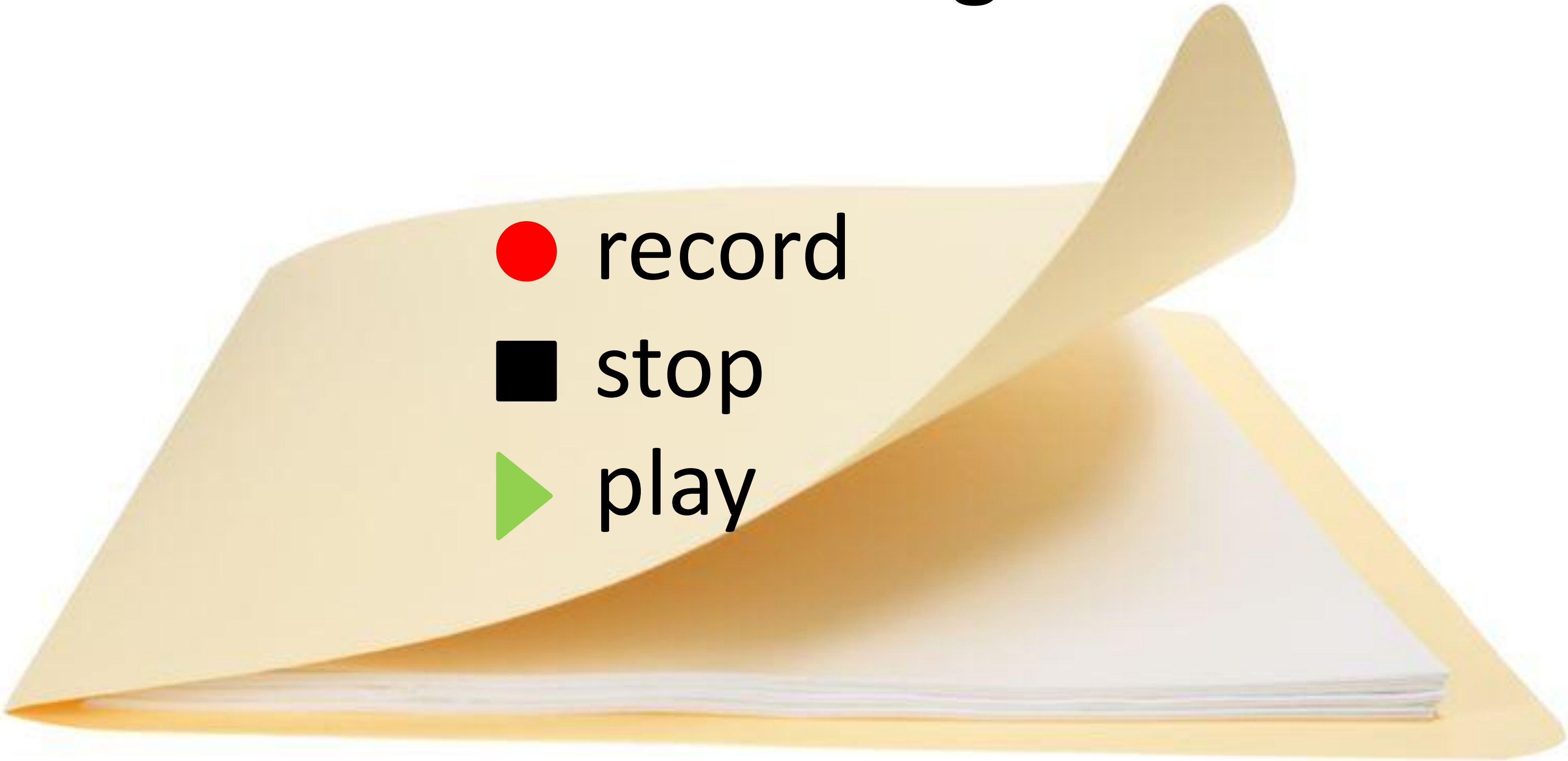
1.2x - 37x

Memory Footprint Reduction

20% - 93%

Reconfiguration Speed as Bottleneck

Programming Interface of the Instruction Register File



- ● record
- ■ stop
- ▶ play

Reduction in Memory Fetches

2x – 8x

Trusted Configuration

State “read out”

Information Leakage

Fault Injection