Lightweight On-Chip Decoder Design for Information Hiding in Compiled Programs

The Future of Computer Security

Malcolm Taylor

Faculty Advisors

Dr. Min Wu

Dr. Gang Qu

MERIT 2007 FAIR

Emergence of Hardware Security

- Attackers becoming smarter and more aggressive
- Software security solutions are commonly defeated
- Shift towards hardware based computer security implementations
- One solution is a high performance trusted processor
  - Involves manipulation of compiled binaries
  - Employs hardware/software co-design
  - Information hiding based (lossless encoding)

Data Hiding Process

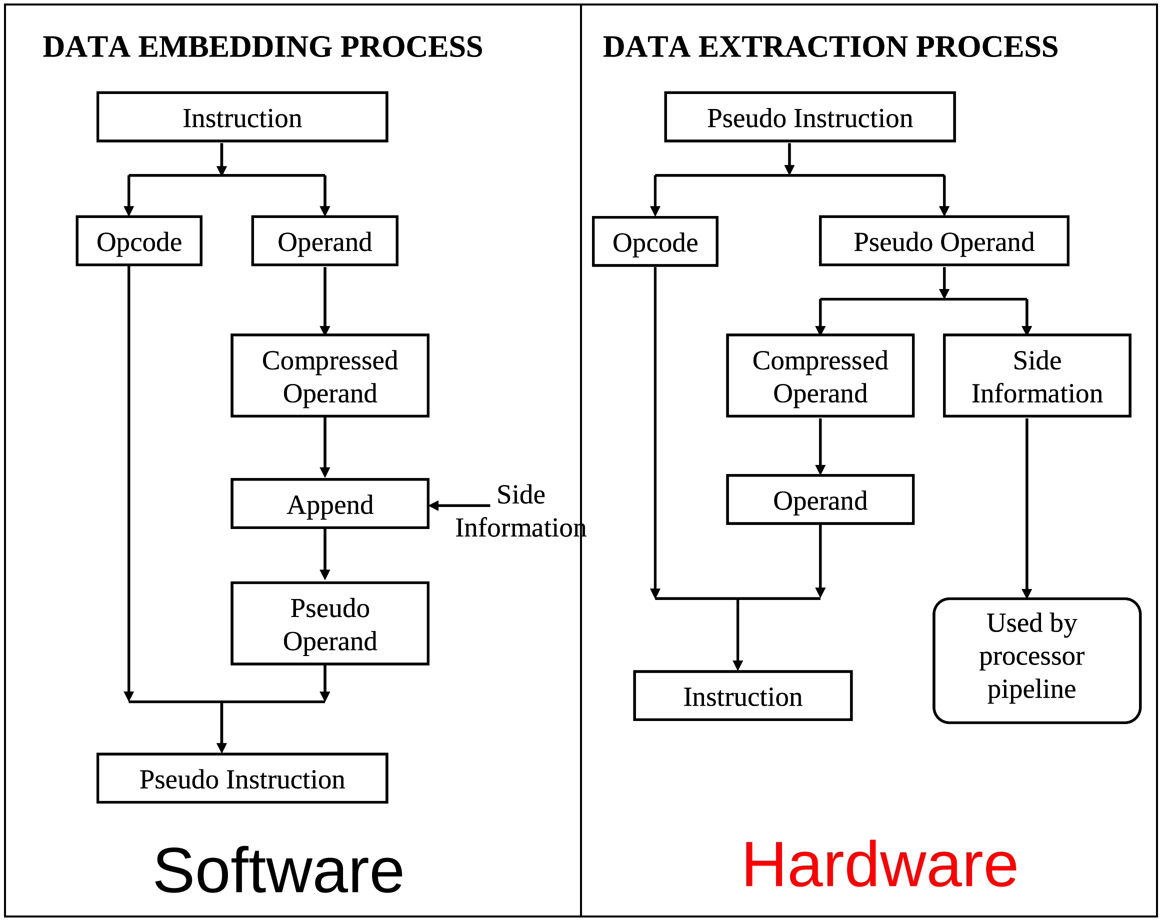
- Data embedding(Software)
  - Losslessly compress operand
  - Use resulting space to hide data by remapping certain bit positions
- Data extraction(Hardware)
  - Decompress operand using look-up table
  - Opcode and decompressed operand used normally
  - Hidden data used for security or performance purposes

$$\underbrace{010110}_{\text{6-bit opcode}}\ \underbrace{11000000000000000010000110}_{\text{26-bit operand}}$$

MERIT

2007 FAIR

Data Hiding Framework



DATA EMBEDDING PROCESS

Instruction → Opcode, Operand

Operand → Compressed Operand → Append (← Side Information) → Pseudo Operand

Opcode, Pseudo Operand → Pseudo Instruction

Software

DATA EXTRACTION PROCESS

Pseudo Instruction → Opcode, Pseudo Operand

Pseudo Operand → Compressed Operand, Side Information

Compressed Operand → Operand

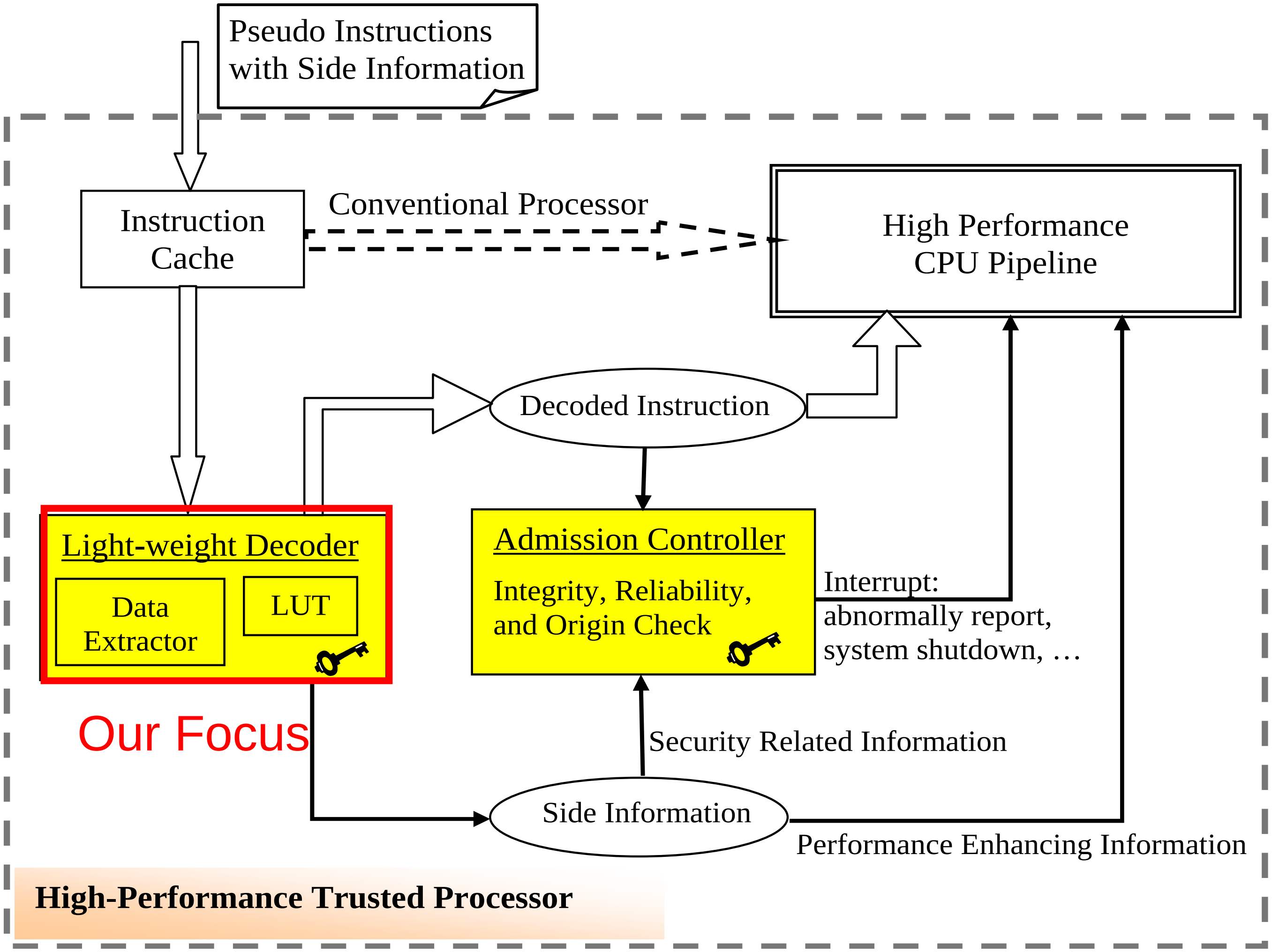
Opcode, Operand → Instruction

Side Information → Used by processor pipeline

Hardware

Proposed by Swaminathan et al. (2005)

High Performance Trusted Processor



Pseudo Instructions with Side Information

Instruction Cache

Conventional Processor

High Performance CPU Pipeline

Decoded Instruction

Light-weight Decoder

Data Extractor

LUT

Admission Controller

Integrity, Reliability, and Origin Check

Interrupt: abnormally report, system shutdown, …

Our Focus

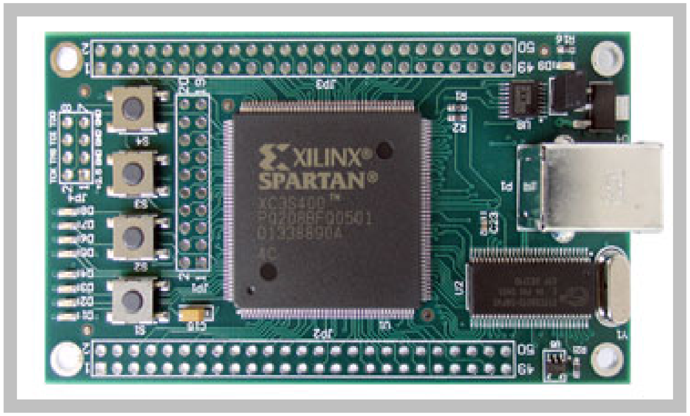
Security Related Information

Side Information

Performance Enhancing Information

Goal

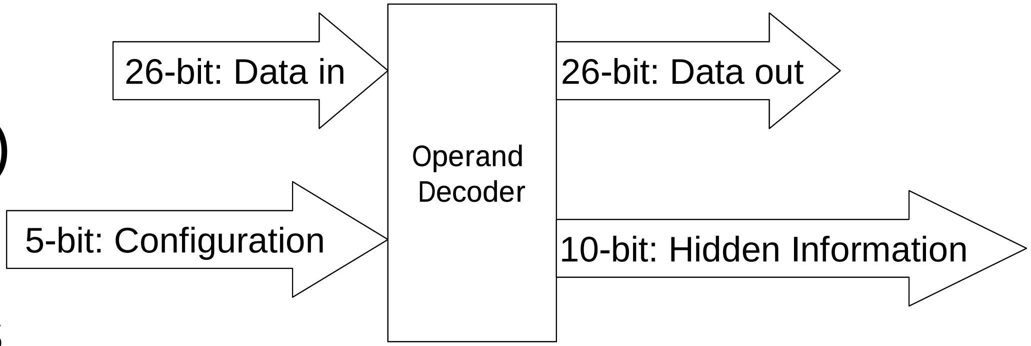
- Develop and prototype a hardware based lightweight decoder
- Assess
  - Feasibility
  - Performance
  - Hardware Characteristics
    - Size
    - Power Consumption
    - Delay



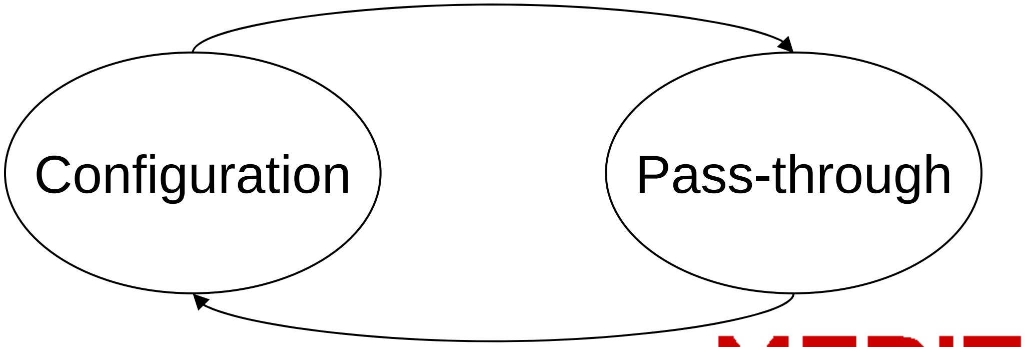
http://www.opalkelly.com/

Design Overview

- Purely combinational decoding (non-clocked)
- Easily configurable
- Minimal data interfaces
- Easy to expand and configure
- Characteristics of a device for our target architecture



2 State Design

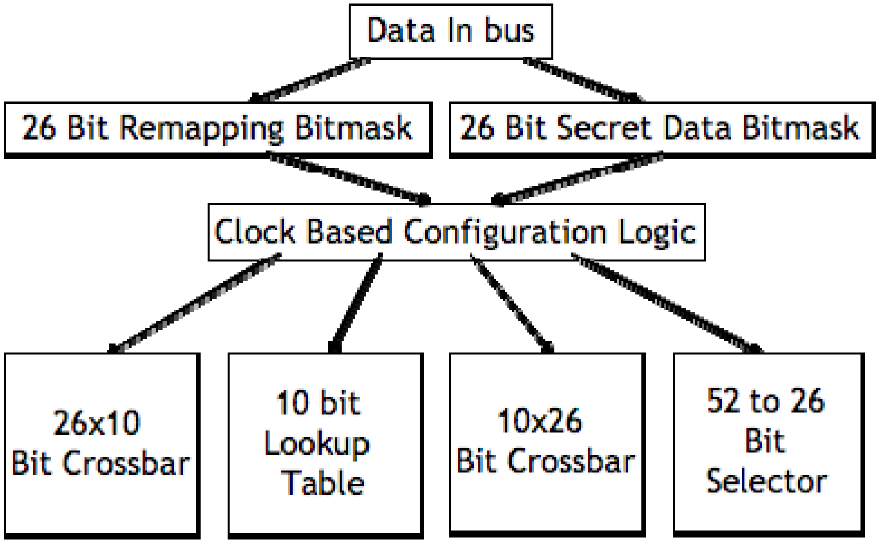


MERIT

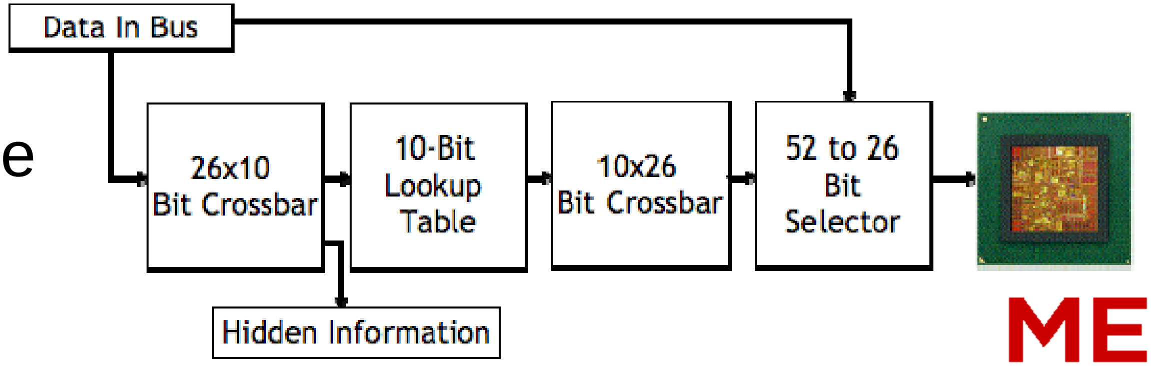
2007 FAIR

Internal Component Structure

Configuration State



Pass-through State



MERIT
2007 FAIR

Prototyping Results

- 100% ability to decode sent operands

Characteristic	Amount	Compared to a Common Single Core Processor
Power Consumption	60 nW	~0.07%
Gates	95,456	~0.2%
Gate Delay	30 ns	N/A

Conclusion

- Information hiding based software/hardware security solution is very feasible
- Decoding can be done with pure combinational logic
- Minimal resources needed to implement hardware decoder
- Integration into an existing architecture is possible with little modification