Analysis of Security in a Modern Processor

ECE 6750

April 26th, 2016

Justin Cox

Tyler Travis

Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

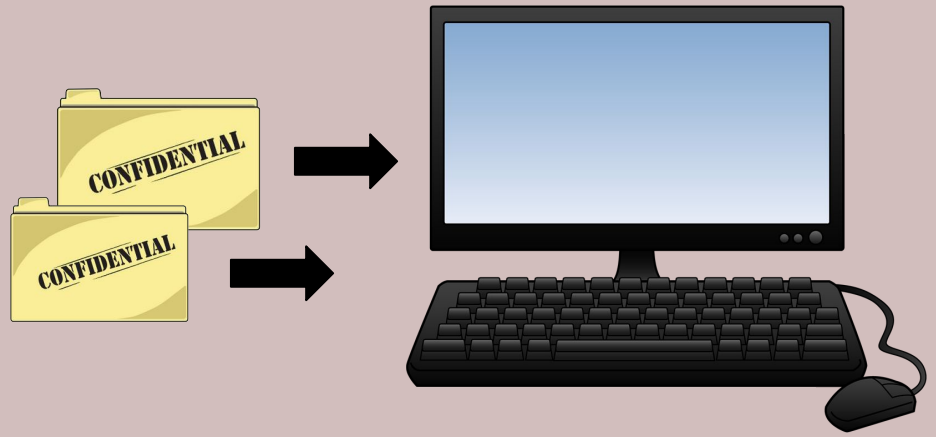
Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

Introduction & Motivation

The Problem:

- Most files are not encrypted
- CPU must decrypt in order to process data
- Attacker is able steal valuable information



Introduction & Motivation

The Reason:

- Computer architectures are designed for speed, efficiency, and power usage **NOT** security

- Too expensive and unrealistic to redesign architectures with security as primary focus

The Solution? **Add security modules to current architecture**

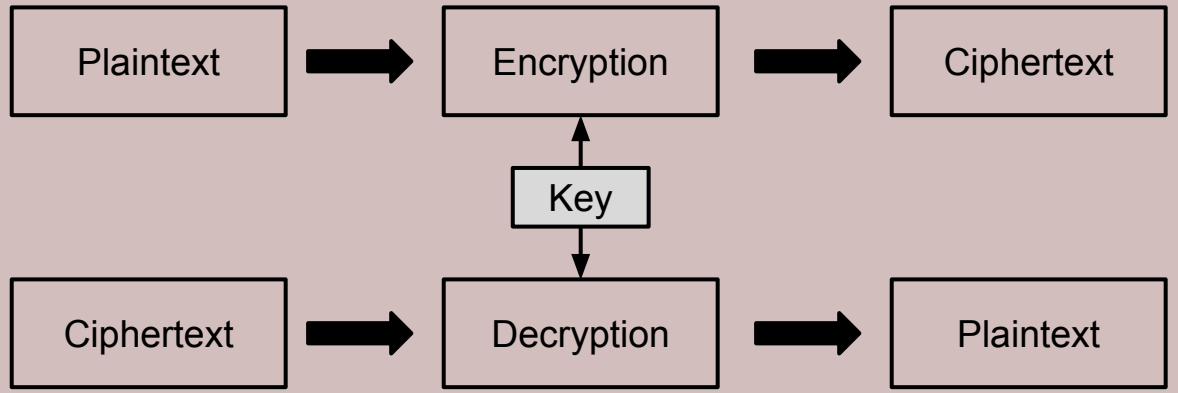
Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

Security Overview

Encryption & Decryption:

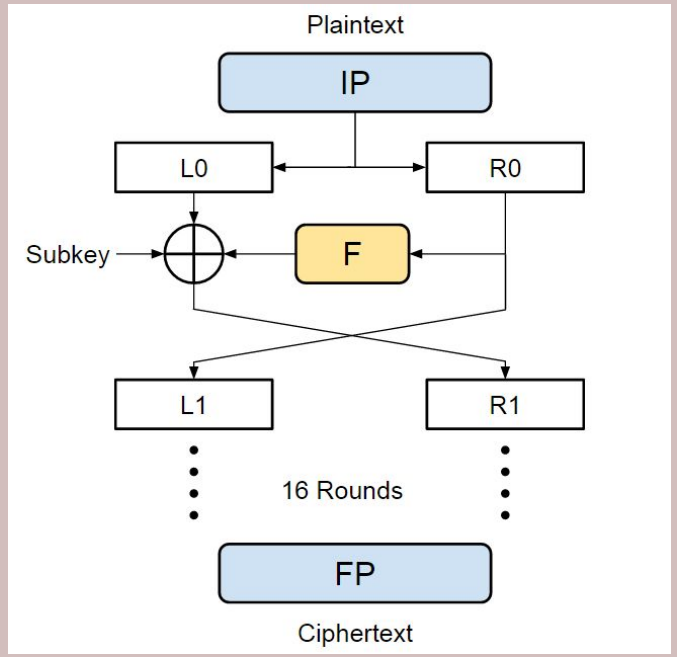
- Method used to obfuscate data making it secure



Security Overview

Algorithm Used: Data Encryption Standard (DES)

- Older and less secure than AES, but less demanding on CPU
- Security can be increased using a PUF to generate secret key



Security Overview

Physical Unclonable Function (PUF)

- Physical differences created during the manufacturing process are used to create unique information
- This information can only be regenerated using the same PUF that generated it initially

Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

gem5 Modifications

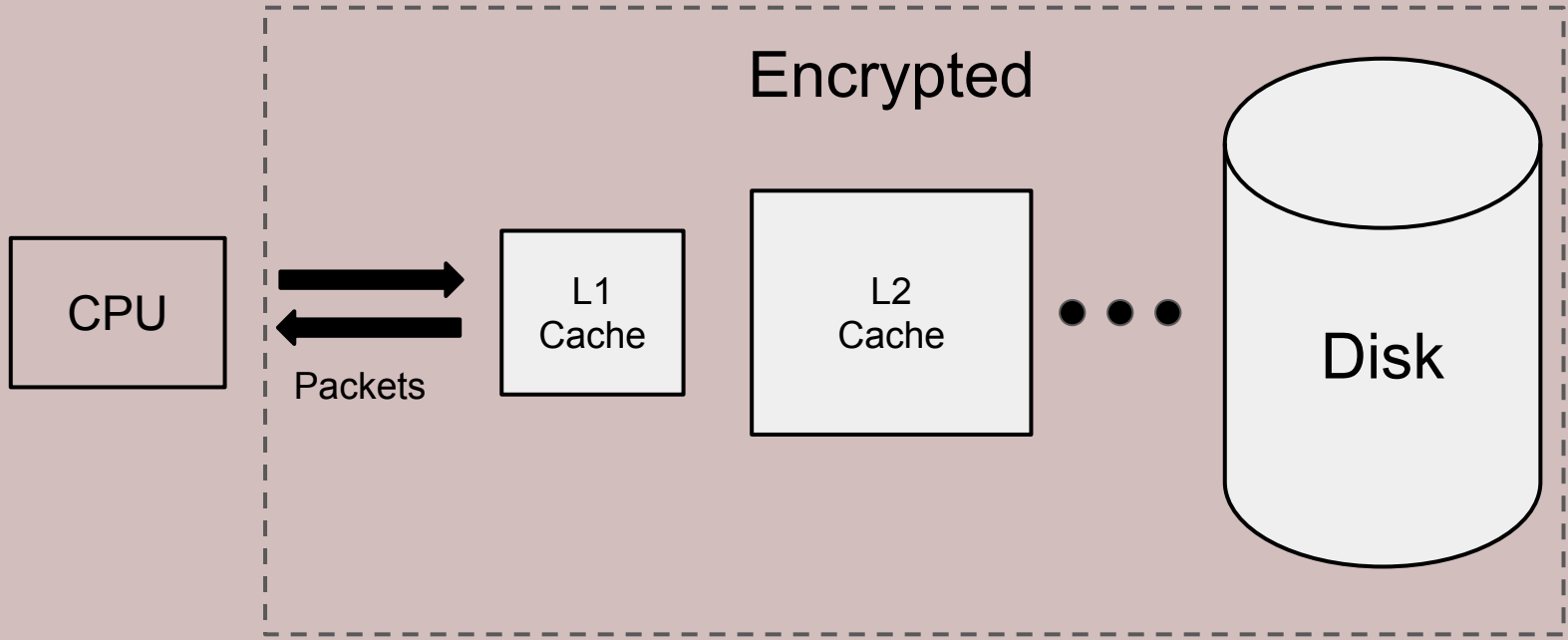
Files Modified: lsq_unit.hh, lsq_unit_impl.hh

Files Added: des.cc, des.hh

gem5 uses packets to communicate with memory

```
data_pkt->dataStatic(inst->memData);
snd_data_pkt->dataStatic(inst->memData + sreqLow->getSize());
```

gem5 Modifications

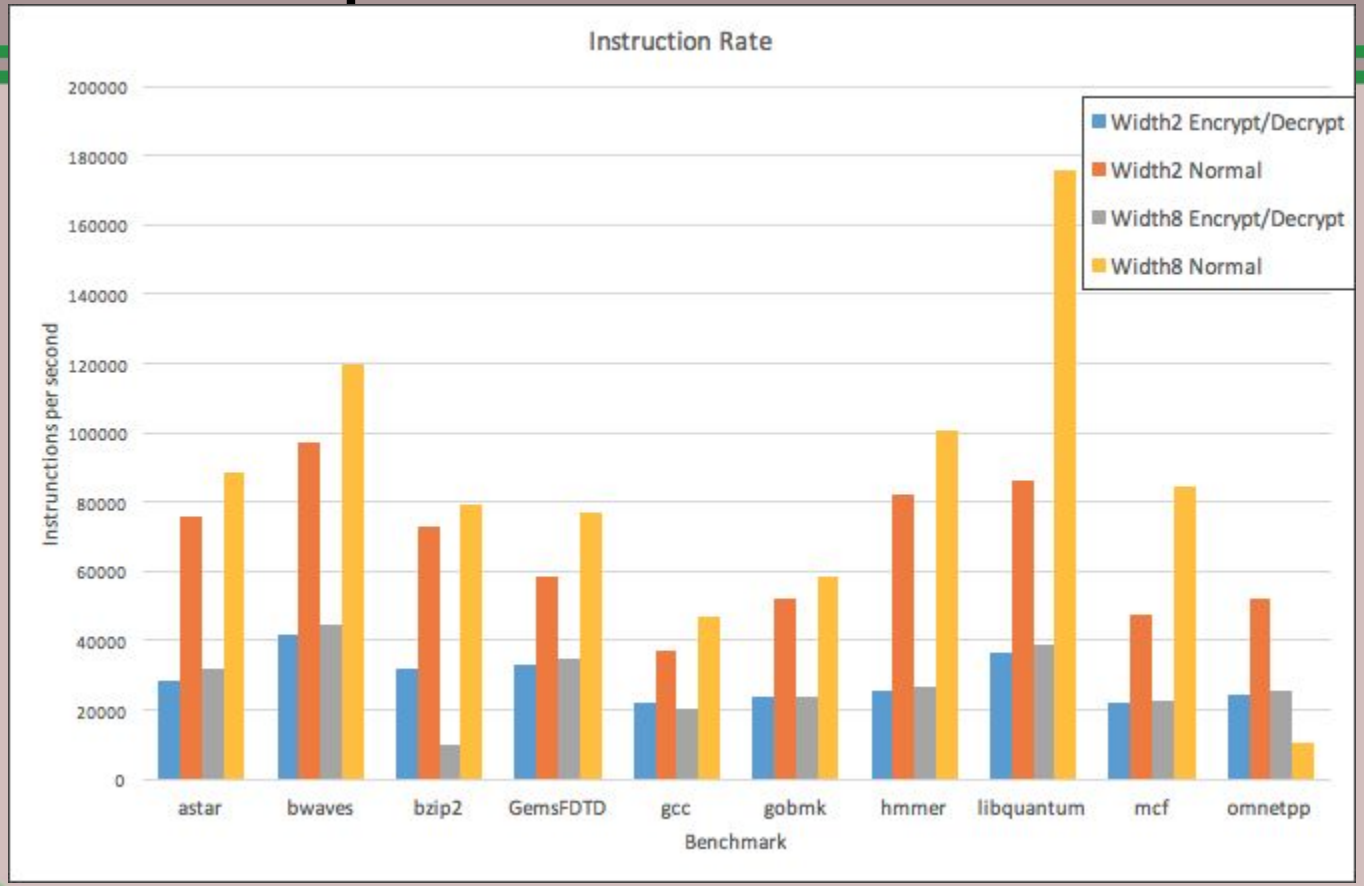


Note: registers are not encrypted

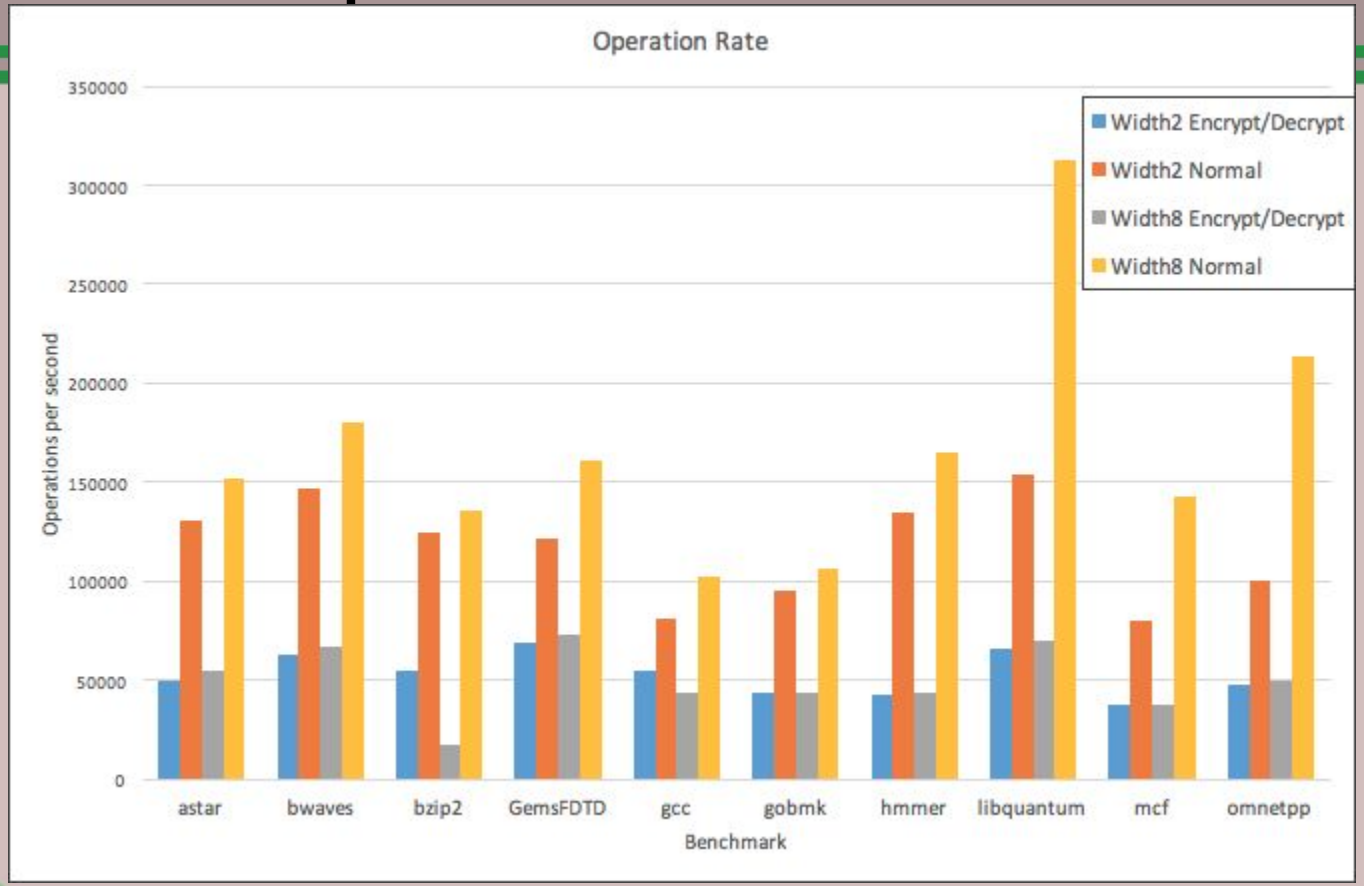
Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

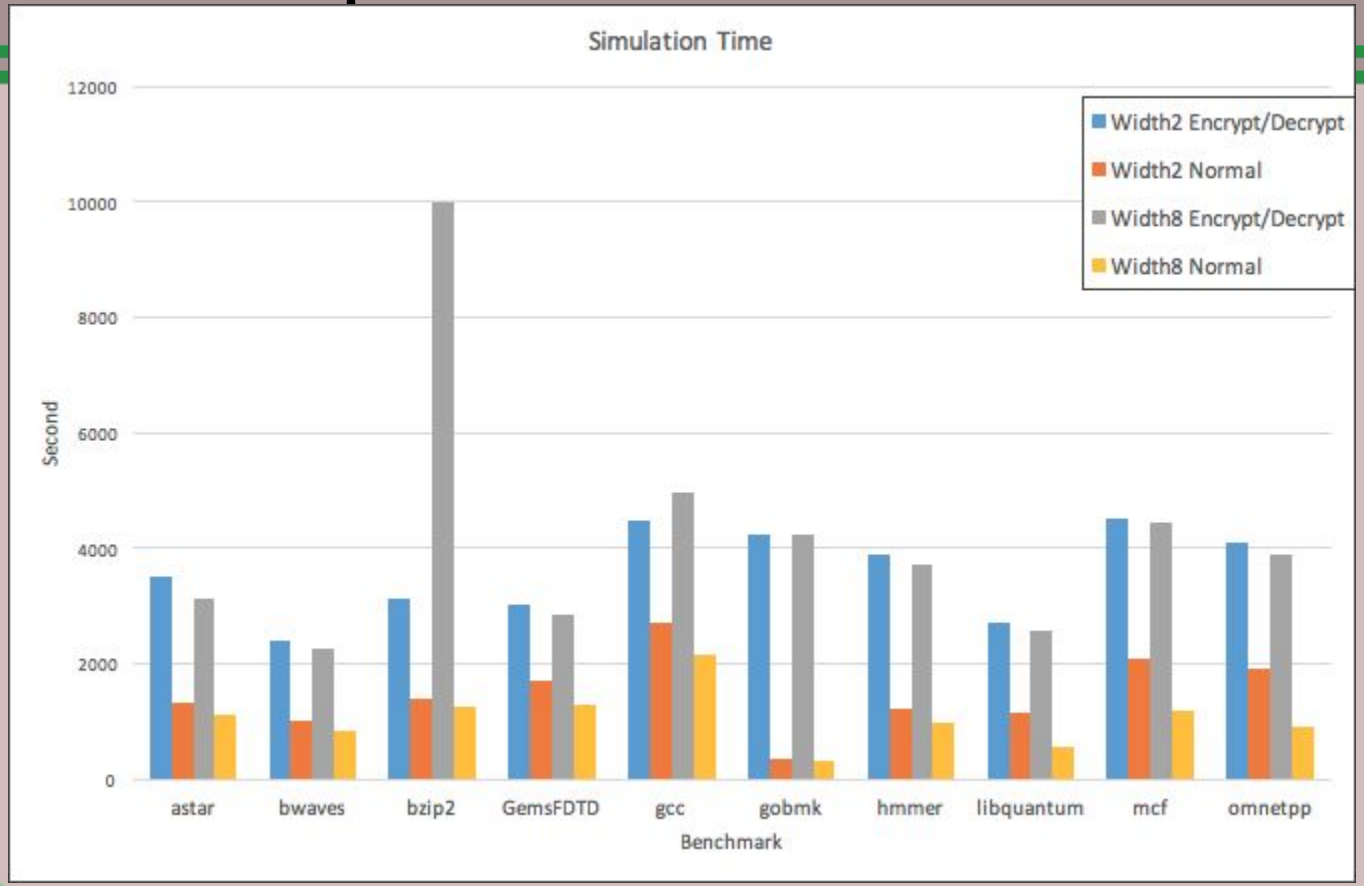
Experimental Results



Experimental Results



Experimental Results



Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

Conclusion

- Performance may decreases by as much as half when a security module is added to the O3 cpu model in gem5.
- Is the security worth the performance hit?
- May be used for applications of data that needs to be secure and performance isn’t a concern.

Presentation Overview

1. Introduction & Motivation
2. Security Overview
   a. Encryption/Decryption - DES
   b. PUFs
3. gem5 Modifications
4. Experimental Results
5. Conclusion
6. Questions

Questions?