ECE 5770 : Resilient Computer Systems Modeling On-Die Termination Power Overhead of Encrypted Data

Udit Gupta, Monica J. Lin

School of Electrical and Computer Engineering, Cornell University, Ithaca, NY

ug28@cornell.edu, mjl256@cornell.edu

Abstract

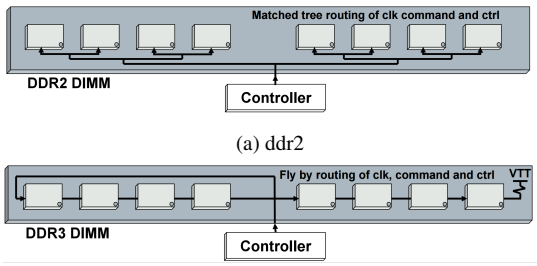
1. Introduction

Since the advent of the Internet, compute devices have become not only more prolific but also varied - encompassing not only high performance compute clusters but also general purpose computers and mobile systems. Moreover, the assumptions made about the security model of a system has changed drastically; users can no longer be trusted, and devices have the potential to interact with unknown and possibly untrustworthy hosts while communicating sensitive information. For example, the boom in smartphones has caused a secondary explosion in the mobile application industry, allowing users to log in to various trusted systems (e.g. bank accounts, medical records and shopping accounts) remotely.

However, the sudden increase in connectivity exposes users to adversaries that may attempt to leverage these interactions in order to obtain confidential information or disrupt the use of services or applications.

In response to these changes, there has been an increasing effort in developing trusted computing platforms augmented with specialized hardware modules that provide security features such as authentication and decryption/encryption. One such security feature that remains a focus in trusted computing research is protecting off-chip memory. Protecting off-chip memory includes maintaining confidentiality of private data. Challenges in designing memory protection mechanisms involves providing encryption primitives at a low cost (money, area, power and design complexity), high throughput and low latency without compromising security. Current work also focuses on memory protection schemes for general purpose and high performance computing systems. The domain of memory protection in the mobile and embedded computing domains is relatively less studied and poses interesting challenges. Mobile and embedded devices often operate under strict power and area constraints. Providing secure memory protection while following the prescribed power and area constraints as well as maintaining performance of the computing devices is an ongoing challenge.

1. Characterizing the power overhead of the memory system is still an open problem - especially in the context of encryption.
2. We use first order approximations to model the power overhead of
3. On die termination - ODT encrypting data on the memory system.
4. We verify that encrypted data has a significant power overhead [add numbers]
5. Outline the paper's sections



(a) ddr2

(b) ddr3

Figure 1: DDR DRAM Chip Topologies [1]

2. Problem Formulation

Figure 2 illustrates the general secure memory encryption architecture used in this study. The threat model assumes that the on-chip memory, `data-cache`, is secure and tamper-proof whereas the off-chip memory is not. The `encryption core` between the data-cache is supposed to provide cryptographic confidentiality properties that prevent unauthorized principals from reading sensitive information that user's wish to keep secret.

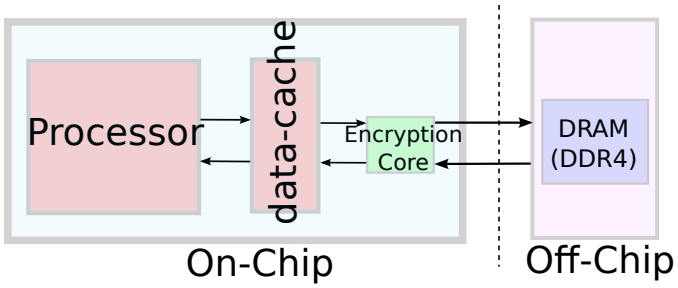
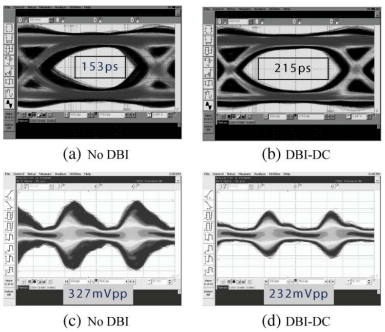


Figure 2: General Memory Encryption Architecture: All on-chip memory accesses, between the processor and data-cache, are performed in plaintext whereas all off-chip, between the data-cache and DRAM, are encrypted.



(a) No DBI (b) DBI-DC

(c) No DBI (d) DBI-DC

Figure 3: DBI DC Impact [2]

Typically, the encryption core seen in Figure 2 implements the `AES-CTR` mode scheme. Where previous studies have focused on the performance and area overhead of memory encryption, we wish to explore the impact of memory encryption on the power consumption of off-chip memory storage systems. Specifically we want use various computer architecture analysis tools to simulate memory access traces and model the power overhead of encryption on DDR4 memory technology. Our first order model characterizes the `ODT` power overhead when using `Data-Bus Inversion` for realisitic benchmarks targetting mobile systems using DDR4 memory technology.

3. Methodology

Describe the general computer architecture design that we are considering for memory encryption. Generally use AES-CTR mode encryption

3.1 Model

1. Introduce equation

$$P_t = A \times P_{dc} + B \times P_{ac}$$

2. Talk about encrypted data : A = 0.5, B = 0.5 : Assumption that Data is Completely random once encrypted
3. Say that DBI aims to reduce A, B by using program structure

3.2 Experimental Setup

1. PIN - dynamic binary instrumentaiton tool : describe cache settings
2. Computer architecture analysis tool
3. MiBench - Justify why MiBench (mobile) —- SPEC is not as good
4. DRAMSim - Did not work for us.
5. Python Script to analyze the loads and stores from the trace outptted from PIN

4. Evaulation

1. Looking at A, B ratios for loads and stores.
2. Put graphs and analyze them.
3. Intuition for decrease (store is lower - mostly misses)

5. Group Dynamics

6. Related Work

7. Conclusion

References

[1] J. Burnett. DDR3 Design Considerations for PCB Applications. Jul 2009.

[2] T. M. Hollis. Data Bus Inversion in High-Speed Memory Applications. *IEEE Transactions on Circuits and Systems*, 2009.