CryptoGraphics
Exploiting Graphics Cards for Security

by

Debra L. Cook
Angelos D. Keromytis
Columbia University
NewYork, USA

Springer
## Contents

List of Figures ix
List of Tables xi
Preface xiii
Acknowledgments xv

1. INTRODUCTION 1
   1.1 Overview 1
   1.2 GPUs 3
   1.3 Motivation 3
   1.4 Encryption in GPUs 4
   1.5 Remotely Keyed CryptoGraphics 5
   1.6 Related Issues 5
   1.7 Extensions 6
   1.8 Conclusions 6

2. GRAPHICAL PROCESSING UNITS 9
   2.1 Overview 9
   2.2 GPU Architecture 10
   2.3 GPUs and General Purpose Programming 15
   2.4 APIs 17
   2.5 OpenGL and Pixel Processing 19
   2.6 Representing Data with Vertices 22
   2.7 Non-Graphic Uses of GPUs 23
3. MOTIVATION

3.1 Overview

3.2 Accelerating Cryptographic Processing

3.2.1 Issue

3.2.2 Previous Approaches

3.2.3 Summary of the GPU-Based Approach

3.3 Malware and Spyware

3.3.1 Issue

3.3.2 Motivating Applications

3.3.3 Other Related Work

3.3.4 Summary of the GPU-Based Approach

3.4 Side Channel and Differential Fault Analysis

4. ENCRYPTION IN GPUs

4.1 Overview

4.2 Feasibility of Asymmetric Key Ciphers

4.3 Feasibility of Symmetric Key Ciphers

4.4 Modes of Encryption

4.5 Example: AES

4.5.1 AES Background

4.5.2 AES in OpenGL

4.5.3 AES Experiments

4.5.4 Use of Parallel Processing in Attacks

4.6 GPUs and Stream Ciphers

4.6.1 Overview

4.6.2 Experiments

4.7 Conclusions

5. REMOTELY KEYED CRYPTOGRAPHICS

5.1 Overview

5.2 Keying of GPUs

5.3 Prototype

5.3.1 Purpose

5.3.2 Architecture

5.3.3 Implementation

5.4 Design Decisions

5.4.1 Remote Keying

5.4.2 Decryption of Data in the GPU