Efficient Implementation Strategies for Block Ciphers on ARMv8

Bachelorarbeit

Bastian Engel

February 5, 2023

Abstract

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Declaration

I hereby declare that ...

Contents

Chapter 1

Introduction

1.1 Block ciphers

Modern-day communication relies on ...

1.1.1 GIFT

GIFT is a lightweight block cipher based on ...

Substitution layer

Permutation layer

Round key addition

Round key extraction

1.1.2 Camellia

1.2 The ARMv8 platform

With small devices, embedded processors and ASICs becoming ever more ubiquitous and essential in areas like medicine or automotive design, the need for ...

Chapter 2

A simple implementation

Chapter 3

Optimizations through bitslicing

Chapter 4

Leveraging NEON advanced SIMD instructions

Acknowledgements

I want to thank ...