Contents

Abstract . . . 3
Foreword . . . 5
Notation . . . 7
Contents . . . 9
1 Introduction . . . 11
1.1 Research question . . . 12
1.2 Limitations . . . 13
2 Background . . . 14
2.1 Principles of encryption . . . 14
2.2 Block ciphers . . . 16
2.2.1 Substitution-permutation networks . . . 17
2.2.2 Feistel ciphers . . . 18
2.3 Block cipher modes . . . 20
2.3.1 Electronic Codebook . . . 20
2.3.2 Cipher Block Chaining . . . 20
2.3.3 Counter Mode . . . 21
2.4 Different block ciphers . . . 22
2.4.1 Blowfish . . . 23
2.4.2 AES . . . 23
2.4.3 Camellia . . . 24
2.4.4 Serpent . . . 25
2.4.5 Twofish . . . 26
2.5 The x86-64 architecture . . . 26
3 Optimization Techniques in the Literature . . . 28
3.1 Table look-ups in general . . . 29
3.2 The use of look-up tables on the x86-64 architecture . . . 30
3.3 Parallel execution of instructions on “out-of-order” CPUs . . . 31
3.4 “Slicing” techniques . . . 32
4 Implementation . . . 34
4.1 Generic approach to block cipher implementation construction . . . 35
4.2 Blowfish . . . 36
4.3 AES . . . 39
4.4 Camellia . . . 41
4.5 Serpent . . . 50
4.6 Twofish . . . 52
5 Evaluation . . . 54
6 Results . . . 58
6.1 Blowfish . . . 59
6.2 AES . . . 60
6.3 Camellia . . . 62
6.4 Serpent . . . 63
6.5 Twofish . . . 64
7 Conclusions . . . 65
References . . . 68
Appendices . . . 73