

Contents

- 1 Introduction 1
 - 1.1 Cryptographic Hashing 1
 - 1.2 The SHA3 Competition 2
 - 1.3 BLAKE, in a Nutshell 5
 - 1.4 Conventions 6
- 2 Preliminaries 9
 - 2.1 Applications 9
 - 2.1.1 Modification Detection 9
 - 2.1.2 Message Authentication 10
 - 2.1.3 Digital Signatures 11
 - 2.1.4 Pseudorandom Functions 12
 - 2.1.5 Entropy Extraction and Key Derivation 13
 - 2.1.6 Password Hashing 13
 - 2.1.7 Data Identification 14
 - 2.1.8 Key Update 14
 - 2.1.9 Proof-of-Work Systems 14
 - 2.1.10 Timestamping 15
 - 2.2 Security Notions 15
 - 2.2.1 Security Models 15
 - 2.2.2 Classical Security Definitions 17
 - 2.2.3 General Security Definition 19
 - 2.3 Black-Box Collision Search 20
 - 2.3.1 Cycles and Tails 20
 - 2.3.2 Cycle Detection 21
 - 2.3.3 Parallel Collision Search 22
 - 2.3.4 Application to Meet-in-the-Middle 22
 - 2.3.5 Quantum Collision Search 23
 - 2.4 Constructing Hash Functions 24
 - 2.4.1 Merkle–Damgård 24
 - 2.4.2 HAIFA 27

2.4.3	Wide-Pipe	27
2.4.4	Sponge Functions	27
2.4.5	Compression Functions	28
2.5	The SHA Family	31
2.5.1	SHA1	31
2.5.2	SHA2	32
2.5.3	SHA3 Finalists	34
3	Specification of BLAKE	37
3.1	BLAKE-256	37
3.1.1	Constant Parameters	37
3.1.2	Compression Function	38
3.1.3	Iteration Mode	40
3.2	BLAKE-512	41
3.2.1	Constant Parameters	41
3.2.2	Compression Function	42
3.2.3	Iteration Mode	42
3.3	BLAKE-224	43
3.4	BLAKE-384	43
3.5	Toy Versions	44
4	Using BLAKE	45
4.1	Simple Hashing	45
4.1.1	Description	45
4.1.2	Hashing a Large File with BLAKE-256	46
4.1.3	Hashing a Bit with BLAKE-512	48
4.1.4	Hashing the Empty String with BLAKE-512	49
4.2	Hashing with a Salt	49
4.2.1	Description	49
4.2.2	Hashing a Bit with BLAKE-512 and a Salt	49
4.3	Message Authentication with HMAC	50
4.3.1	Description	50
4.3.2	Authenticating a File with HMAC-BLAKE-512	50
4.4	Password-Based Key Derivation with PBKDF2	53
4.4.1	Basic Description	53
4.4.2	Generating a Key with PBKDF2-HMAC-BLAKE-224	53
5	BLAKE in Software	55
5.1	Straightforward Implementation	55
5.1.1	Portable C	55
5.1.2	Other Languages	58
5.2	Embedded Systems	60
5.2.1	8-Bit AVR	60
5.2.2	32-Bit ARM	62
5.3	Vectorized Implementation Principle	64

5.4	Vectorized Implementation with SSE Extensions	64
5.4.1	Streaming SIMD Extensions 2 (SSE2)	64
5.4.2	Implementing BLAKE-256 with SSE2	65
5.4.3	Implementing BLAKE-512 with SSE2	66
5.4.4	Implementations with SSSE3 and SSE4.1	70
5.5	Vectorized Implementation with AVX2 Extensions	70
5.5.1	Relevant AVX2 Instructions	71
5.5.2	Implementing BLAKE-512 with AVX2	73
5.5.3	Implementing BLAKE-256 with AVX2	77
5.6	Vectorized Implementation with XOP Extensions	79
5.6.1	Relevant XOP Instructions	80
5.6.2	Implementing BLAKE with XOP	80
5.7	Vectorized Implementation with NEON Extensions	83
5.7.1	Relevant NEON Instructions	83
5.7.2	Implementing BLAKE-256 with NEON	84
5.7.3	Implementing BLAKE-512 with NEON	86
5.8	Performance	88
5.8.1	Speed Summary	89
5.8.2	8-Bit AVR	90
5.8.3	ARM Platforms	91
5.8.4	x86 Platforms (32-bit)	91
5.8.5	amd64 Platforms (64-bit)	92
5.8.6	Other Platforms	93
6	BLAKE in Hardware	97
6.1	RTL Design	97
6.2	ASIC Implementation	98
6.2.1	High-Speed Design	98
6.2.2	Compact Design	100
6.3	FPGA Design	100
6.4	Performance	101
6.4.1	ASIC	102
6.4.2	FPGA	102
6.4.3	Discussion	105
7	Design Rationale	107
7.1	NIST Call for Submissions	107
7.1.1	General Requirements	107
7.1.2	Technical and Security Requirements	109
7.1.3	Could SHA2 Be SHA3?	110
7.2	Needs Analysis	111
7.2.1	Ease of Implementation	112
7.2.2	Performance	113
7.2.3	Security	113
7.2.4	Extra Features	114

7.3	Design Philosophy	114
7.3.1	Minimalism	115
7.3.2	Robustness	119
7.3.3	Versatility	120
7.4	Design Choices	120
7.4.1	General Choices	121
7.4.2	Iteration Mode	122
7.4.3	Core Algorithm	122
7.4.4	Rotation Counts	125
7.4.5	Permutations	126
7.4.6	Number of Rounds	128
7.4.7	Constants	128
8	Security of BLAKE	131
8.1	Differential Cryptanalysis	131
8.1.1	Differences and Differentials	132
8.1.2	Finding Good Differentials	133
8.2	Properties of BLAKE's G Function	133
8.2.1	Basic Properties	134
8.2.2	Differential Properties of G	136
8.3	Properties of the Round Function	141
8.3.1	Bijectivity	141
8.3.2	Diffusion and Low-Weight Differences	142
8.3.3	Invertibility	145
8.3.4	Impossible Differentials	147
8.4	Properties of the Compression Function	151
8.4.1	Finalization	151
8.4.2	Local Collisions	152
8.4.3	Fixed Points	152
8.4.4	Fixed Point Collisions	153
8.4.5	Pseudorandomness	153
8.5	Security Against Generic Attacks	154
8.5.1	Indifferentiability	154
8.5.2	Length Extension	155
8.5.3	Collision Multiplication	155
8.5.4	Multicollisions	156
8.5.5	Second Preimages	157
8.6	Attacks on Reduced BLAKE	158
8.6.1	Preimage Attacks	158
8.6.2	Near-Collision Attack	159
8.6.3	Boomerang Distinguisher	160
8.6.4	Iterative Characteristics	161
8.6.5	Breaking BLOKE	163
8.6.6	Attack on a Variant with Identical Constants	163

- 9 BLAKE2** 165
 - 9.1 Motivations 165
 - 9.2 Differences with BLAKE 166
 - 9.2.1 Fewer Rounds 167
 - 9.2.2 Rotations Optimized for Speed 167
 - 9.2.3 Minimal Padding 168
 - 9.2.4 Finalization Flags 168
 - 9.2.5 Fewer Constants 168
 - 9.2.6 Little-Endianness 169
 - 9.2.7 Counter in Bytes 170
 - 9.2.8 Salt Processing 170
 - 9.2.9 Parameter Block 170
 - 9.3 Keyed Hashing (MAC and PRF) 172
 - 9.4 Tree Hashing 172
 - 9.4.1 Basic Mechanism 173
 - 9.4.2 Message Parsing 174
 - 9.4.3 Special Cases 174
 - 9.4.4 Generic Tree Parameters 175
 - 9.4.5 Updatable Hashing Example 175
 - 9.5 Parallel Hashing: BLAKE2sp and BLAKE2bp 176
 - 9.6 Performance 177
 - 9.6.1 Why BLAKE2 Is Fast in Software 177
 - 9.6.2 64-bit Platforms 178
 - 9.6.3 Low-End Platforms 179
 - 9.6.4 Hardware 180
 - 9.7 Security 180
 - 9.7.1 BLAKE Legacy 180
 - 9.7.2 Implications of BLAKE2 Tweaks 181
 - 9.7.3 Third-Party Cryptanalysis 181
- 10 Conclusion** 185
- References** 187
- A Test Vectors** 195
 - A.1 BLAKE-256 195
 - A.1.1 One-Block Message 195
 - A.1.2 Two-Block Message 196
 - A.2 BLAKE-224 198
 - A.2.1 One-Block Message 198
 - A.2.2 Two-Block Message 199
 - A.3 BLAKE-512 201
 - A.3.1 One-Block Message 201
 - A.3.2 Two-Block Message 202
 - A.4 BLAKE-384 205

- A.4.1 One-Block Message 205
 - A.4.2 Two-Block Message 206
- B Reference C Code 209**
 - B.1 blake.h 209
 - B.2 blake224.c 211
 - B.3 blake256.c 214
 - B.4 blake384.c 217
 - B.5 blake512.c 220
- C Third-Party Software 225**
 - C.1 BLAKE 225
 - C.2 BLAKE2 226
- Index 227**