

Contents

List of Acronyms	xv
1. Introduction	1
1.1. Contributions of this Thesis	2
1.2. Outline	3
2. Finite Fields	5
2.1. Basic Definitions and Properties	5
2.2. Special Elements of Finite Fields	7
2.3. Representation of Finite Fields	9
2.4. The Rijndael-Field	11
2.5. Arithmetic in $\text{GF}(2^8)$	12
2.6. Other Representations of $\text{GF}(2^8)$	15
3. The Advanced Encryption Standard	17
3.1. The AES State	17
3.2. The AES Round Functions	18
3.2.1. ShiftRows	18
3.2.2. MixColumns	19
3.2.3. SubBytes	20
3.2.4. AddRoundKey	21
3.3. The AES Keyschedule	21
3.4. Encryption/Decryption with AES-128	23
3.4.1. Encryption	23
3.4.2. Decryption	25
3.5. A Minimal Blockcypher	26
4. Serial Algorithms for Finite Field Inversion	27
4.1. Previous Work	27
4.2. Algorithms for Inversion via Field Enumeration	28
4.2.1. Algorithm A	29
4.2.2. Algorithm B	29
4.2.3. Algorithm C	30
4.3. Serial Inversion with Polynomial Basis Representation	31
4.4. From Vectors to State Machines	33
4.5. Choosing α	36
4.6. Further Serialisation	36

4.7.	Batch Inversion	37
4.8.	Other Methods for Inversion	37
5.	Serialising the AES-S-box	39
5.1.	The AES-S-box	39
5.2.	Popular Approaches for Implementation	40
5.2.1.	Lookup Tables	40
5.2.2.	Constructions with Direct Inversion	40
5.2.3.	Single-Cycle Combinational Designs	41
5.2.4.	A Remark on the Affine Transformation	41
5.3.	Theory of Serialisation	41
5.3.1.	Further Serialisation	43
5.3.2.	Partial Deserialisation	46
5.4.	Optimisation of the Affine Transformation	47
5.4.1.	Free Multiplications	47
5.4.2.	Factoring in the Affine Transformation	49
5.4.3.	Inverse Affine Transformation	50
5.5.	Implementations of Serialised S-boxes	50
5.6.	Side-Channel Leakage	50
6.	Search for Best Parameters	53
6.1.	Defining the Design Space and Generating the Inputs	54
6.2.	Verification, Synthesis and Simulation	56
6.3.	The Pitfalls of Logic Optimisation	56
6.4.	Results	58
6.4.1.	Area	59
6.4.2.	Power	64
6.4.3.	Timing	64
6.4.4.	Benchmarks	65
6.4.5.	A Final Note	66
7.	The Holzbaur-Wamser Implementation of the S-box	69
7.1.	Bases, Towers and an S-box	69
7.1.1.	Normal and Optimal Normal Bases	70
7.1.2.	Splits and Tower Fields	71
7.1.3.	The Tower Field of Canright	72
7.1.4.	The S-box of Canright	73
7.2.	Integrating Serial Inversion	74
7.2.1.	Step 1: Replacing the 4bit-Inversion	74
7.2.2.	Step 2: Exploiting Free Multiplication	74
7.2.3.	Step 3: Implicit Change of Basis	76
7.3.	Implementation results	76
7.4.	Open Problems	77
8.	Full AES Implementations	79
8.1.	Previous Low-Area Architectures	79

8.2.	A new 8-bit-Serial Architecture	81
8.2.1.	Design Rationale	81
8.2.1.1.	Data Flow	81
8.2.1.2.	Area-Runtime Tradeoff	83
8.2.1.3.	Flexibility	83
8.2.2.	Serial MixColumns	83
8.2.3.	Architecture Overview	84
8.2.4.	Public Interface	85
8.2.5.	AES Architecture in Detail	86
8.2.5.1.	Data State Module	86
8.2.5.2.	Key State Module	88
8.2.5.3.	Control Logic	89
8.2.6.	Differences for Dedicated Encryption Core	89
8.2.7.	Modification for a LFSR-based S-box	90
8.3.	Control Flow and Timing	92
8.3.1.	Encryption	92
8.3.2.	Decryption	94
8.3.3.	The Case of Serial S-boxes	96
8.4.	Synthesis Results	96
8.5.	Beyond 8-bit	98
9.	A 1st-order Threshold Implementation	101
9.1.	Common Countermeasures and Serial S-boxes	102
9.1.1.	Boolean Masking	102
9.1.2.	Affine Masking	102
9.2.	Threshold Implementations	103
9.2.1.	Properties of Threshold Implementations	104
9.2.1.1.	Property 1: Correctness	104
9.2.1.2.	Property 2: Non-Completeness	104
9.2.1.3.	Property 3: Uniformity	104
9.2.2.	Threshold Implementation (TI) for Simple and General Functions	105
9.2.2.1.	Linear and Affine Functions	105
9.2.2.2.	Non-Linear Functions	105
9.2.2.3.	Threshold Implementations of AND	106
9.2.2.4.	Threshold Implementations of Multiplexers	107
9.3.	Compact Threshold Implementation of the AES-S-box	109
9.4.	Threshold Implementation of the Full AES	111
9.5.	Evaluation	112
9.5.1.	Simple Power Analysis Attacks	114
9.5.2.	Differential Power Analysis Attacks	116
9.6.	Other Notable Protected Implementations of AES	123
9.7.	Further Countermeasures	125
10.	Conclusion	127
10.1.	Review of the Contributions of this Thesis	127
10.2.	Outlook	128

Appendix	131
A. Various Proofs	131
A.1. Inverse MixColumns from MixColumns	131
A.2. Inverse SubBytes from SubBytes	132
A.3. Special properties of Binary Extension Fields (BEFs)	133
B. Tables	137
B.1. Tables for the Rijndael-Field	137
B.1.1. Direct Multiplication Tables	137
B.1.2. Discrete Logarithm Tables	140
B.1.3. Inversion table	142
B.1.4. Squares and roots	143
B.2. The AES-S-box	144
C. Plots	145
C.1. Histograms of S-box Distributions	145
C.2. QQ-Plots of S-box Distributions	146
D. Scripts and Source Codes	149
D.1. GF-Multiplication with 03 and F6 in Software	149
D.2. VHDL Snippets and Full Sources	151
D.2.1. Affine Function Correction	151
D.2.2. An Example Affine Transformation	151
D.2.3. A Maximum Length Linear-Feedback Shift-Register (LFSR)	153
D.2.4. An Example Linear-Feedback State-Machine (LFSM)	155
D.2.5. Example Implementation of Algorithm 5.3	155
D.2.6. Example Implementation of Algorithm 5.4	158
D.2.7. Example Implementation of Algorithm 5.6	160
D.2.8. Example Implementattion for the Fast Variant of Design B	161
Bibliography	165
List of Figures	185
List of Tables	187
List of Algorithms	189
List of Pre-Publications	191