

Inhaltsverzeichnis

1. Einleitung	1
2. Eine kurze Einführung in Chiffriersysteme	3
2.1. Definition eines Chiffriersystems	3
2.2. Das Chiffriersystem von HILL	9
2.3. RSA	16
2.4. Nachrede	21
3. Eine abstrakte Darstellung von AES	23
3.1. Die S-Box	24
3.2. Die Abbildungen Ξ_j zur Addition der Rundenschlüssel	29
3.3. Die Abbildung Θ zur Elementesubstitution und die Abbildung Π zur Reihenrotation	30
3.4. Die Abbildung Φ zur Spaltenmischung	31
3.5. Die Berechnung der Rundenschlüssel	35
3.6. Das Zusammensetzen der Rundenabbildungen	36
3.7. Die strukturelle Anpassung von Chiffrierung und Dechiffrierung	37
4. Eine konkrete Darstellung von AES	39
4.1. Die S-Box	40
4.2. Die Elementesubstitution und die Reihenrotation	43
4.3. Die Spaltenmischung	44
4.4. Die Berechnung der Rundenschlüssel	45
4.5. Die Runden $\mathcal{R}_0$ bis $\mathcal{R}_{10}$ der Verschlüsselung	46
4.6. Die Umkehrunden $\mathcal{U}_{10}$ bis $\mathcal{U}_0$ der Entschlüsselung	49
4.6.1. Die Umkehrunden $\mathcal{U}_{10}$ bis $\mathcal{U}_1$	50
4.6.2. Die Umkehrrunde $\mathcal{U}_0$	52
5. Die Implementierung von AES für AVR-Mikrocontroller	53
5.1. Die Initialisierung	55
5.2. Die Berechnung der Rundenschlüssel	56
5.3. Die Spaltenmischung	62
5.4. Die optimierte Spaltenmischung	65
5.5. Die Verschlüsselung	69
5.6. Die Entschlüsselung	74
5.7. Nachrede	78
6. Die Implementierung von AES für dsPIC-Mikrocontroller	79
6.1. Die Initialisierung	82
6.2. Die Berechnung der Rundenschlüssel	85
6.3. Die Spaltenmischung	89

6.4. Die optimierte Spaltenmischung	92
6.5. Die Verschlüsselung	95
6.6. Die Entschlüsselung	100
6.7. Nachrede	104
7. Chipher Block Chaining (CBC) mit AES	105
7.1. Motivation	105
7.2. Definition	107
7.3. Implementierung für AVR	109
8. Chipher-Feedback Mode (CFM) mit AES	113
8.1. Motivation	113
8.2. Definition	114
8.3. Implementierung für AVR	117
9. Verschlüsselung mit dem Rucksackproblem	119
9.1. Theorie	120
9.2. Implementierung für AVR	130
9.2.1. Initialisierung	132
9.2.2. Verschlüsselung	139
9.2.3. Schnelle Multiplikation großer Zahlen	144
9.2.4. Entschlüsselung	154
9.3. Implementierung für dsPIC	163
9.3.1. Schnelle Multiplikation großer Zahlen	165
9.3.2. Initialisierung	173
9.3.3. Verschlüsselung	179
9.3.4. Entschlüsselung	181
9.4. Nachrede	183
10. Implementierung der Arithmetik von $\mathbb{K}_{2^8}$	185
10.1. Implementierung für AVR	189
10.1.1. Multiplikation	190
10.1.2. Optimierte Multiplikation	193
10.1.3. Division	197
10.2. Implementierung für dsPIC	199
10.2.1. Multiplikation und Division	199
10.3. Nachrede	204
A. Mathematischer Anhang	205
A.1. Die Teilerrestfunktion	206
A.2. Die EULERSche ϕ -Funktion	208
A.3. Polynome	211
A.4. Einiges zur Struktur endlicher Körper	219
A.5. Die Konstruktion von Körpern mit einer Primzahlpotenz als Elementezahl	222
B. Miszellen	225
B.1. Die Subtraktion großer positiver natürlicher Zahlen	226

B.2. Der Körper $\mathbb{K}_{2^8}$	229
B.3. AVR-Nomenklatur und AVR-Makros	234
B.4. Mathematische Symbole und Bezeichnungen	239
Literaturverzeichnis	241

AES und Rucksackverfahren

Theorie und Praxis mit AVR- und dsPIC-Mikrocontrollern

Schmidt, H.; Schwabl-Schmidt, M.

2017, IX, 241 S., Softcover

ISBN: 978-3-658-19703-2