

Inhaltsverzeichnis

Abbildungsverzeichnis	xi
Tabellenverzeichnis	xiii
1 Einführung	1
2 Kryptographische Algorithmen	5
2.1 Einordnung und Ziele der Kryptographie	5
2.2 Symmetrische Algorithmen	6
2.2.1 Beschreibung	6
2.2.2 Blockchiffren	7
2.2.3 Stromchiffren	13
2.3 Asymmetrische Algorithmen	13
2.3.1 Beschreibung	13
2.3.2 RSA	15
2.4 Kryptographische Komplexität	16
2.5 Traditionelle Kryptoanalyse	17
3 Seitenkanalangriffe	21
3.1 Einführung	21
3.1.1 Definition von Seitenkanalangriffen	21
3.1.2 Einordnung der Seitenkanalangriffe	22
3.1.3 Klassifikation von Seitenkanalangriffen	24
3.2 Zeitangriffe	25
3.3 Stromangriffe	30
3.3.1 Strommodell	30
3.3.2 Einfacher Stromangriff	33
3.3.3 Statistische Stromangriffe	38
3.3.4 Verbesserungen und Weiterentwicklungen	44
3.4 Elektromagnetische Angriffe	48
3.5 Systematisierung der Seitenkanalangriffe	49

Inhaltsverzeichnis	x
4 Herkömmliche Gegenmaßnahmen	51
4.1 Allgemein	51
4.2 Verhinderung der Datenabhängigkeit	52
4.3 Dekorrelation von Daten und Kanal	52
4.3.1 Verschlechterung des SNRs	53
4.3.2 Verschleierung der Daten	53
4.4 Limitierungen herkömmlicher Gegenmaßnahmen	54
5 Komplexität statistischer Seitenkanalangriffe	57
5.1 Komplexität statistischer Angriffe	57
5.2 Einfluss algorithmischer Parameter	59
5.2.1 Einfluss der Länge l_{k_T} des Teilschlüssels k_T	60
5.2.2 Einfluss der Anzahl n_T der Teilschlüssel k_T	62
5.2.3 Einfluss der Rundenschlüsselerzeugung	63
6 Designmerkmale symmetrischer Blockchiffren	65
6.1 Strukturmerkmale der Algorithmen	65
6.2 Merkmale der Operationen des Algorithmus	67
6.3 Merkmale der Rundenschlüsselerzeugung	72
6.4 Zusammenfassung	74
7 Implementierungsaspekte	77
7.1 Geheimhaltung des Algorithmus	77
7.2 Kaskadieren von Algorithmen	78
7.3 Hamming-Gewicht-konstante Schlüssel	78
8 Bewertung und Vergleich bestehender Algorithmen	83
8.1 AES/Rijndael	83
8.2 MARS	88
8.3 RC6	91
8.4 Serpent	94
8.5 Twofish	97
8.6 Auswertung	103
9 Zusammenfassung und Schlussfolgerungen	107
Abkürzungen und Formelzeichen	111
Abkürzungen	111
Formelzeichen	112
Literaturverzeichnis	115
Lebenslauf	129