Inhaltsverzeichnis

0. Einleitung und Übersicht
0.1 Einleitung ... 1
0.2 Übersicht ... 6

1. Definitionen und Grundlagen
1.1 Fundamentale Definitionen und Eigenschaften ... 12
1.2 Definition des AR-Systems ... 24
1.3 Approximationstheoretische Optimierung ... 26
1.4 Beispiel eines AR-Systems mit Taylor-Approximation ... 33

2. Kryptoanalyse des AR-Systems
2.1 Abstrakte Brechungsansätze ... 39
2.2 Numerische Brechungsansätze ... 43
2.3 Ein Brechungsansatz mit Hilfe des binären Suchens ... 47
2.4 Analytische und approximationstheoretische Brechungsansätze ... 50
2.5 Walsh-Funktionen in AR-Systemen ... 70
2.6 Periodische Funktionen in AR-Systemen ... 73
2.7 Zusammenfassung der Kryptoanalyse des AR-Systems ... 81

3. Entwicklung nichtganzzahliger Public-Key-Kryptosysteme
3.1 Kryptologische Eigenschaften rationaler Zahlen ... 83
3.2 Ein Public-Key-Kryptosystem mit rationalen Zahlen ... 106
3.3 Kryptoanalyse des R-Systems mit Hilfe von Kettenbrüchen ... 118
3.4 Public-Key-Hill-Chiffren ... 124
3.5 Digitale Unterschriften mit dem R^k-System ... 137

4. Weitere Anwendungen
4.1 Exaktes Rechnen mit rationalen Zahlen ... 141
4.2 Anwendung auf reelle Kongruenzen und Faktorisierungsalgorithmen ... 145

5. Anhang
5.1 Liste der Bezeichnungen und Begriffe ... 163
5.2 Liste der Symbole ... 167

6. Literaturverzeichnis ... 170