

Inhalt

1	Einleitung	1
1.1	Allgemeine Bemerkungen zum Testproblem	1
1.2	Testverfahren	2
1.3	Motivation und Inhalt dieser Arbeit	6
1.4	Gliederung der nachfolgenden Kapitel	7
2	Mathematische Hilfsmittel	9
2.1	Algebraische Hilfsmittel	9
2.2	Codierungstheoretische Hilfsmittel	14
2.3	Analytische Hilfsmittel	16
2.4	Kombinatorische Hilfsmittel	19
3	Signaturanalyse, mathematisch beschrieben	23
3.1	Schaltkreise mit mehreren Ausgängen	23
3.2	Schaltkreise mit einem Ausgang	27
4	Signaturanalyse mit primitiven Polynomen	30
4.1	Approximation der Maskierungswahrscheinlichkeiten	30
4.2	Auffinden primitiver Polynome	33
5	Signaturanalyse mit dem Polynom $X^n + 1$	37
6	Mehrfache Signaturanalyse	43
6.1	Abschätzungen für die Maskierungswahrscheinlichkeit	44
6.2	Auffinden der charakteristischen Polynome von BCH-Codes	49
7	Behandlung mehrerer Ausgänge	52
7.1	Signaturanalyse mit intern-exklusivem LFSR	52
7.2	Signaturanalyse mit extern-exklusivem LFSR	53
8	Schlußwort	56
9	Literatur	57
10	Anhang	60