

**Entwurf und Analyse
kryptographisch sicherer Keystreamgeneratoren
zur Stromverschlüsselung**

Dissertation

zur

Erlangung des akademischen Grades
eines Doktor-Ingenieur
des Fachbereichs
Elektrotechnik und Informationstechnik
der FernUniversität-Gesamthochschule
in Hagen

von

Diplom-Informatiker

Bernhard Löhlein

geboren in Würzburg

Hagen 2001

Eingereicht am:	5. Juli 2001
Tag der mündlichen Prüfung:	7. Dezember 2001 in Hagen
1. Berichterstatter:	Prof. Dr.-Ing. Firoz Kaderali, FernUniversität Hagen
2. Berichterstatter:	Prof. Dr.-Ing. Ludwig Kittel, FernUniversität Hagen
3. Berichterstatter:	Prof. Dr. Werner Poguntke, Märkische Fachhochschule in Hagen

Berichte aus der Kommunikationstechnik herausgegeben von
Prof. Firoz Kaderali

Band 10

Bernhard Löhlein

**Entwurf und Analyse kryptographisch sicherer
Keystreamgeneratoren zur Stromverschlüsselung**

Shaker Verlag
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Löhlein, Bernhard:

Entwurf und Analyse kryptographisch sicherer Keystreamgeneratoren zur Stromverschlüsselung / Bernhard Löhlein.

Aachen : Shaker, 2002

(Berichte aus der Kommunikationstechnik herausgegeben von
Prof. Firoz Kaderali ; Bd. 10)

Zugl.: Hagen, Univ., Diss., 2001

ISBN 3-8265-9948-9

Copyright Shaker Verlag 2002

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8265-9948-9

ISSN 1437-7497

Shaker Verlag GmbH • Postfach 1290 • 52013 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • eMail: info@shaker.de

Berichte aus der Kommunikationstechnik
herausgegeben von
Prof. Dr.-Ing. Firoz Kaderali

Band 10

Bernhard Löhlein

**Entwurf und Analyse
kryptographisch sicherer Keystreamgeneratoren
zur Stromverschlüsselung**

Shaker Verlag
Aachen 2002

Vorwort

Die vorliegende Dissertationsarbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrgebiet Kommunikationssysteme des Fachbereichs Elektrotechnik und Informationstechnik der FernUniversität Gesamthochschule in Hagen.

In meiner Zeit am Lehrgebiet Kommunikationssysteme hatte ich die Möglichkeit, mich intensiv mit aktuellen Themen im Bereich der Kommunikationstechnik, der Kryptographie und der Netzwerksicherheit im Rahmen universitärer Lehre und von Forschungsprojekten auseinander zusetzen. Insbesondere war das Themengebiet der Stromchiffren in einem Teilprojekt des NRW Forschungsverbundes Datensicherheit eingebettet.

Mein besonderer Dank geht an Herrn Prof. Dr.-Ing. Firoz Kaderali für die Betreuung, Anregungen und wertvollen Hinweise bei Erstellung dieser Dissertationsarbeit.

Herrn Prof. Dr.-Ing. Ludwig Kittel danke ich für die Übernahme des Korreferates und sein wohlwollendes Interesse an die in dieser Arbeit aufgeworfenen Fragestellungen.

Herrn Prof. Dr. rer. nat. Werner Poguntke sage ich Dank für Hilfestellungen bei Problemen aus der diskreten Mathematik.

In meinem Dank an meine ehemaligen Kolleginnen und Kollegen am Lehrgebiet für die freundliche Arbeitsatmosphäre möchte ich Herrn Dr.-Ing. Markus Schneider für die Einführung in das Themengebiet der Stromchiffren und Booleschen Funktionen und Herrn Taher Nasched für die Unterstützung bei der Programmierung besonders erwähnen.

Bei Herrn Prof. Dr. Tran van Trung vom Institut für Experimentelle Mathematik der Universität Essen bedanke ich mich für die Einführung in die Designtheorie und den Differenzenmengen.

Auch bedanke ich mich bei meinen Eltern und meinem Bruder, die mich in vielerlei Hinsicht unterstützten.

Hagen im Dezember 2001

Kurzfassung

Sowohl private als auch geschäftliche Kommunikation und Informationsaustausch werden zunehmend über offene Kommunikationstechnologien abgewickelt. Zur Gewährleistung von Sicherheitsbedürfnissen werden kryptographische Primitive und Protokolle in die Informationsverarbeitung und die Kommunikationsabläufe eingeführt. Die Vertraulichkeit zwischen den Kommunikationspartnern kann durch Verschlüsselungssysteme hergestellt werden.

In der vorliegenden Arbeit werden symmetrische und synchrone Stromverschlüsselungssysteme auf der Basis von Keystreamgeneratoren entworfen und analysiert. Der Keystreamgenerator hat die Aufgabe nach der Initialisierung mit einem geheimen kurzen Schlüssel, eine (lange) pseudo-zufällige Folge zu erzeugen.

Ein gängiger Keystreamgenerator ist der nichtlineare Filtergenerator (NLFG). Dieser besteht aus einem linear zurückgekoppelten Schieberegister der Länge k und einem Rückkopplungspolynom $c \in \text{GF}(2)[x]$ und einer Booleschen Funktion $f : \text{GF}(2)^n \rightarrow \text{GF}(2)$ (Filterfunktion), der n Phasen $\Gamma = (\gamma_1, \dots, \gamma_n)$ zur Erzeugung des Keystreams \tilde{z} zugeführt werden. Für den NLFG stellen wir im Kapitel 4 zunächst die aus der Literatur bekannten Angriffsformen vor und entwickeln im Abschnitt 4.8 die lineare Transformationsattacke und im Kapitel 5 die bedingte Korrelationsattacke weiter. Wir verallgemeinern die bedingte Korrelationsattacke auf beliebige Phasen, geben Greedy Algorithmen zum Auffinden von suboptimalen Abtastzeitpunkten an und definieren neue bedingte Korrelationskoeffizienten. Aus den Ideen zu den schnellen Korrelationsattacken und der bedingten Korrelationsattacke entwerfen wir im Abschnitt 5.11 die hybride Korrelationsattacke gegen den NLFG. Auf Basis dieser Untersuchungen geben wir im Kapitel 6 explizite Entwurfsrichtlinien für einen kryptographisch sicheren nichtlinearen Filtergenerators aus Sicht der Systemtheorie an. Eine wichtige Rolle spielt die Auswahl der Filterfunktion als eine hoch nichtlineare und balancierte Boolesche Funktion und die sorgfältige Positionierung der Phasen. Für diese schlagen wir kombinatorische Objekte aus der Designtheorie vor, so dass ein Mindestberechnungsaufwand zur Durchführung einer bedingten Korrelationsattacke bewiesen werden kann. Die Ergebnisse werden durch systematische Fallstudien untermauert.

Im weiteren entwerfen wir im Kapitel 7 eine universelle time-memory-tradeoff Attacke gegen eine allgemeine Klasse von Keystreamgeneratoren. Dieses Angriffsverfahren ist unter Rahmenbedingungen in denen andere Angriffsformen keine

Aussicht auf Erfolg haben noch einsetzbar. Darüber hinaus ist eine Parametrisierbarkeit der TMT-Attacke, bezüglich der Variablen Länge des beobachteten Keystreams, benötigter Zeit- und Speicheraufwand und der Erfolgswahrscheinlichkeit, möglich.

Ein weiterer Gegenstand der Betrachtung bildet im Kapitel 8 der E_0 -Keystreamgenerator, der zur Familie der Combiner-Generatoren mit Speicher zu zählen ist. Der E_0 wird in der Bluetooth Übertragungstechnologie zur additiven Stromverschlüsselung der Pakete auf der Luftschnittstelle verwendet. Es wird eine umfassende Sicherheitsanalyse durch die Anwendung aller bekannten Angriffsverfahren durchgeführt. Dazu ist es notwendig, dass Eigenschaften zur Invertierbarkeit der Zustandsüberführung und unbedingte und bedingte Korrelationen ermittelt werden.

Im Anhang wird die Anwendung der selbstprogrammierten Analysetools beschrieben. Außerdem werden Methoden zur Bestimmung von Kontrollgleichungen aufgeführt, funktionale Beschreibungen von allgemeinen Generatoren erläutert und ein Überblick zur Bluetooth Übertragungstechnologie geliefert.

Zusammenfassend können die folgenden Beiträge in dieser Arbeit als neue und eigenständig entwickelte Analysen von bzw. Entwurfsvorschlage fur Keystreamgeneratoren zur Stromverschlüsselung aufgefuhrt werden:

1. Im Abschnitt 4.8 entwerfen wir die lineare Transformationsattacke gegen den NLFG. Diese stellt kein vollstandiges Angriffsverfahren dar, sondern ist als eine Vorstufe zu anderen Angriffsverfahren (im Kapitel 4 und 5) gegen den NLFG anzusehen.

Der ursprungliche NLFG wird dabei durch eine lineare Transformation in einen aquivalenten Generator mit dem gleichen Schieberegister und Ruckkopplungspolynom transformiert. Es konnen durch die Transformation lineare Strukturen in der Filterfunktion f aufgedeckt werden, so dass dadurch zum Beispiel bedingte Korrelationskoeffizienten (siehe Kapitel 5) einen hoheren Wert ergeben. Dadurch ist dann eine bedingte oder hybride Korrelationsattacke mit einer groeren Erfolgswahrscheinlichkeit und einer kleineren Rundenzahl durchfuhrbar. Ebenso kann die Spannung der Phasen des NLFGs durch die Transformation verringert werden. Dadurch kann dann eine Inversionsattacke (siehe Abschnitt 4.4) schneller durchgefuhrt werden.

Fur die Anzahl der Eingangsvariablen der Filterfunktion und den Wert fur die Spannung der Phasen des aquivalenten Generators leiten wir Auftrettswahrscheinlichkeiten her, falls ein Angreifer alle moglichen linearen Transformationen testet. Bei der Herleitung wird dabei angenommen, dass die Nullen und Einsen in den Transformationsvektoren gleich und voneinander unabhangig in den Transformationsmatrizen verteilt sind. Fallstudien haben ergeben, dass diese Annahme fur Ruckkopplungspolynome mit einem

Gewicht von ungefähr $k/2$ sehr gut erfüllt ist, wobei k die Länge des linear zurückgekoppelten Schieberegisters des NLFGs ist. Als Ergebnis der mathematischen Analysen, basierend auf der obigen Annahme, erhält man die Aussage, dass man bei sorgfältiger Wahl des Rückkopplungspolynoms keinen leichter angreifbaren Generator durch die lineare Transformations-
 attacke bestimmen kann.

2. Im Kapitel 5 entwickeln wir die bedingte Korrelationsattacke gegen den NLFG in folgenden Punkten weiter:
 - (a) Die bisherige Beschreibungsform der bedingten Korrelationsattacke war auf den Spezialfall von benachbarten Phasen $\Gamma = (0, 1, \dots, n-1)$ beschränkt. Wir lassen in unserer Beschreibung der bedingten Korrelationsattacke beliebige Phasen Γ zu. Hierfür wird ein neuer Begriffs- und Notationsapparat entwickelt und angewendet.
 - (b) Zur Minimierung des Berechnungsaufwandes in der Vorberechnungsphase und zur Erhöhung der Werte der bedingten Korrelationskoeffizienten werden nicht aufeinander folgende, sondern optimale Abtastzeitpunkte $T^m = (t_1, t_2, \dots, t_m)$ bestimmt.
 - (c) An die Eingaben zur Filterfunktion werden neue lineare Bedingungen zum Aufstellen von bedingten Korrelationskoeffizienten formuliert. Diese neuen Korrelationskoeffizienten sind effektiver zu bestimmen und können in der im Abschnitt 5.11 entwickelten hybriden Korrelationsattacke benutzt werden.
 - (d) Im Satz 5.7 wird eine Klasse von Filterfunktionen identifiziert, bei der die Korrelationskoeffizienten zur Bedingung B_1 und B_4 verschwinden und somit nicht durch die hybride Korrelationsattacke angegriffen werden können.
3. Im Abschnitt 5.11 wird die hybride Korrelationsattacke gegen den NLFG entwickelt und dargestellt. Diese neue Angriffsform ist eine dreiphasige Attacke gegen den NLFG, die in der ersten Phase bedingte Korrelationen benutzt, um eine erste Korrektur auf der Keystreamfolge \tilde{z} durchzuführen. In der zweiten Phase können dann entweder weiter bedingte Korrelationen herangezogen oder eine schnelle Korrelationsattacke angewendet werden, um den Initialzustand des NLFGs zu rekonstruieren. Im ersteren Fall werden die Folgensymbole mit den höchsten berechneten Zuverlässigkeitswerten in der dritten Phase genutzt, um den Initialzustand des Schieberegisters des NLFGs zu ermitteln.

Die Anwendung der hybriden Korrelationsattacke ist indiziert, falls die normierte Nichtlinearität $p_{e,f}$ der Filterfunktion f den Wert 0.45 übertrifft und man keine ausreichende Anzahl von hohen bedingten Korrelationen ermitteln konnte. Im Fall der hohen Nichtlinearität ($p_{e,f} \geq 0.45$) von f führt die

reine Anwendung einer schnellen Korrelationsattacke nicht zum Erfolg. Die hybride Korrelationsattacke kann in diesen Fällen auch bei kleinen bedingten Korrelationen den unbekanntem Initialzustand \underline{s}_0 ermitteln. Die hybride Korrelationsattacke stellt eine vollständige Neuentwicklung dar. Vergleichbare Ansätze sind in der Literatur nicht zu finden.

4. Im Kapitel 6 werden die Erkenntnisse aus den Angriffsverfahren gegen den NLFG benutzt, um einen aus der Sicht der Systemtheorie sicheren NLFG für ein gegebenes Sicherheitsniveau in Form eines zeitlichen Mindestberechnungsaufwandes für die einzelnen Angriffsverfahren explizit anzugeben. Dazu werden im Abschnitt 6.4 minimale Werte für die Länge k des Schieberegisters mit Rückkopplungspolynom c und der Anzahl n der Eingaben zur Filterfunktion f ermittelt und für diese die einzelnen Komponenten (c , Phasenauswahl Γ und f) des NLFGs entworfen. Wir schlagen für n gerade die Typen I bzw. II als Filterfunktionen vor:

$$\text{Typ I: } f(x_1, \dots, x_n) = x_1 + g(x_2, \dots, x_{n-1}) + x_n$$

bzw.

$$\text{Typ II: } f(x_1, \dots, x_n) = x_1 + g(x_2, \dots, x_{n-1}) + \prod_{i=2}^{n-1} x_i + x_n,$$

wobei $g : \text{GF}(2)^{n-2} \rightarrow \text{GF}(2)$ eine beliebige Bent Funktion mit maximalen algebraischen Grad $(n-2)/2$ ist. Diese Filterfunktionen haben die Eigenschaft, dass die bedingten Korrelationskoeffizienten für die Bedingungen B_1 und B_4 verschwinden und somit eine Anwendung der hybriden Korrelationsattacke nicht möglich ist. Die bedingten Korrelationskoeffizienten zu den Bedingungen B_2 und B_3 zu den Filterfunktionen vom Typ I und Typ II weisen im Vergleich zu andersartig aufgebauten Filterfunktionen mit der gleichen Anzahl von Eingangsvariablen deutlich niedrigere Werte auf. Diese Eigenschaft wird im Abschnitt 6.3.5 bei einem Vergleich mit der Filterfunktion des unregelmäßig getakteten LILI-128 Keystreamgenerators nachhaltig verdeutlicht. Im Beispiel 6.6 entwerfen wir unter der Randbedingung, dass der Keystreamgenerator maximal 132 bit haben darf, einen NLFG mit 131 bit Speicher auf der Basis unserer Entwurfsrichtlinien. Dieser ist damit mit den Keystreamgeneratoren E_0 (132 bit) und LILI-128 (128 bit) vergleichbar. Sowohl bezüglich unbedingter als auch bedingter Korrelationskoeffizienten erreicht unser Vorschlag ein höheres Sicherheitsniveau als das des E_0 ¹.

¹Die Evaluation des LILI-128 Keystreamgenerators und weiterer Vorschläge für Keystreamgeneratoren werden derzeit im Projekt NESSIE, finanziert durch die Europäische Kommission, vorgenommen, so dass zum jetzigen Zeitpunkt kein Vergleich zum Sicherheitsniveau des NLFGs hergestellt werden kann.

5. In vielen konkreten Angriffsszenarien in Kommunikationssystemen findet man als Angreifer die Situation vor, nur kleine Teilstücke des Keystreams beobachten zu können. In diesen Fällen führen bedingte und unbedingte Korrelationsattacken nur sehr eingeschränkt zum Erfolg. Es bieten sich dann meist nur noch Formen einer Inversionsattacke an, die allerdings für die meisten Keystreamgeneratoren einen sehr großen Berechnungsaufwand in der eigentlichen Angriffsphase haben. Eine weitere Alternative stellt die im Kapitel 7 entwickelte allgemeine TMT-Attacke gegen beliebige Keystreamgeneratoren dar, die auf den Ideen des allgemeinen TMT-Schemas von Hellman und der TMT-Attacke von Biryukov und Shamir gegen den $A_5/1$ basiert. Die hier entwickelte TMT-Attacke ist grundsätzlich auf beliebige Keystreamgeneratoren anwendbar und erlaubt die Angabe eines expliziten Angriffsverfahrens für die Wahl der Parameter aus Speicherbedarf, Berechnungsaufwand, vorhandener Keystreamlänge und Erfolgswahrscheinlichkeit gemäß einer Tradeoff-Kurve.
6. Im Kapitel 8 wird eine umfassende Sicherheitsanalyse für den E_0 -Generator vorgenommen. Es werden nach der Beschreibung der Basiseigenschaften des E_0 alle aus der Literatur bekannten Angriffsverfahren gegen Combiner-Generatoren mit Speicher auf den E_0 angewandt. Es zählen dazu die Inversionsattacke, drei verschiedene Varianten der unbedingten Korrelationsattacke, die bedingte Korrelationsattacke und die im Kapitel 7 entwickelte TMT-Attacke. Zur Durchführung der unbedingten bzw. bedingten Korrelationsattacken werden unbedingten bzw. bedingten Korrelationen ermittelt. Im Abschnitt 8.11 werden die benötigte Länge N des Keystreams und der Berechnungsaufwand C der einzelnen Attacken auf den E_0 in einer Tabelle zusammengefasst dargestellt.

Inhaltsverzeichnis

Vorwort	v
Kurzfassung	vii
Tabellenverzeichnis	xviii
Abbildungsverzeichnis	xxi
Algorithmenverzeichnis	xxiii

I Grundlagen 1

1 Einführung 3

1.1 Kryptologie, eine moderne Wissenschaft	3
1.2 Klassifikation von Verschlüsselungssystemen	5
1.3 Standardisierung von symmetrischen Verschlüsselungssystemen	10
1.4 Grundlegende mathematische Begriffe und Notationen	12
1.5 Inhaltlicher Ausblick über die folgenden Kapitel	16

2 Klassifikation und Entwurf von Stromverschlüsselungssystemen 21

2.1 Klassifikation von symmetrischen Stromchiffresystemen	21
2.1.1 Synchrone und symmetrische Stromchiffren	22
2.1.2 Selbstsynchronisierende Stromchiffren	25
2.2 Angreifermodelle für Verschlüsselungssysteme	28
2.3 Entwurfsprinzipien für Verschlüsselungssysteme	29
2.3.1 Informationstheoretischer Entwurf	30
2.3.2 Komplexitätstheoretischer Entwurf	32
2.3.3 Systemtheoretischer Entwurf	36
2.3.3.1 Keystreamgeneratoren mit regulär getakteten Schieberegistern	39
2.3.3.2 Taktgesteuerte Keystreamgeneratoren	46
2.3.3.3 Ablauf des systemtheoretischen Entwurfs	48
2.4 Phasen für den Betrieb eines Verschlüsselungssystems	49

3	Boolesche Funktionen für Keystreamgeneratoren	51
3.1	Grundlagen und Begriffe zu Booleschen Funktionen	54
3.2	Die Walsh Transformation	60
3.2.1	Definition	61
3.2.2	Eigenschaften der Walsh Transformation	62
3.2.3	Schnelle Berechnung der Walsh Transformation	64
3.3	Korrelationskoeffizienten	66
3.4	Nichtlinearität	70
3.5	Bent Funktionen	74
3.5.1	Definition und Basiseigenschaften	74
3.5.2	Die Maiorana-McFarland Klasse \mathcal{M} von Bent Funktionen	75
3.6	Korrelationsimmune Funktionen	77
3.7	Resilient Abbildungen	79
II	Der nichtlineare Filtergenerator	81
4	Angriffsverfahren gegen den nichtlinearen Filtergenerator	83
4.1	Korrelationsattacke nach Siegenthaler	84
4.2	Schnelle Korrelationsattacken	87
4.2.1	Schnelle Korrelationsattacke nach Zeng	94
4.2.2	Schnelle Korrelationsattacke nach Forré	95
4.2.3	Schnelle Korrelationsattacke mit Bayesscher Decodierungsregel	96
4.2.4	Schnelle Korrelationsattacke nach Canteaut und Trabbia	97
4.3	BAA-Attacke	100
4.4	Inversionsattacke nach Golić	101
4.5	Trellis-basierte Viterbi-Decodierung	103
4.6	Lokale Reduktion von Gleichungen	104
4.7	Dezimierungsattacke	105
4.8	Lineare Transformationsattacke	106
4.9	Zusammenfassung	111
5	Bedingte Korrelationsattacke gegen den NLFG	113
5.1	Notationen und Begriffe	115
5.2	Lineare Bedingungen	118
5.3	Bildung von bedingten Korrelationskoeffizienten	120
5.4	Lineare Gleichungen zu den bedingten Korrelationen	124
5.5	Die Durchführung einer bedingten Korrelationsattacke	126
5.6	Bestimmung von T^m	129
5.7	Bemerkungen zum Berechnungsaufwand	136
5.8	Eigenschaften der bedingten Korrelationskoeffizienten	142
5.9	Fallstudie	148

5.10	Nichtlineare Bedingungen	155
5.11	Hybride Korrelationsattacke	157
5.12	Zusammenfassung	164
6	Entwurf eines kryptographisch sicheren NLFGs	167
6.1	Rückkopplungspolynom c	167
6.2	Phasenauswahl Γ	170
6.3	Filterfunktion f	182
6.3.1	Balanciertheit	182
6.3.2	Nichtlinearität und algebraischer Grad	184
6.3.3	Parametrisierung	187
6.3.4	Fallstudie	189
6.3.5	Vergleich mit der Ausgabefunktion f_{LILLI} des Keystreamgenerators LILL-128	192
6.4	Bestimmung von k und n	195
6.5	Zusammenfassung und Hinweise auf offene Forschungsfragen	200
III	TMT-Attacke und der E_0-Keystreamgenerator	203
7	Eine time-memory-tradeoff Attacke gegen Keystreamgeneratoren	205
7.1	TMT-Schemata	206
7.2	Die TMT-Attacke auf Basis des Hellman Schemas	214
7.3	Untersuchungen zur Reduktionsfunktion R_1	226
7.4	Zusammenfassung	230
8	Analyse der kryptographischen Sicherheit des E_0-Generators	233
8.1	Beschreibung des E_0 -Keystreamgenerators	234
8.2	Basiseigenschaften des E_0	237
8.3	Kryptographisch relevante Eigenschaften	242
8.4	Mögliche Angriffsformen gegen den E_0	246
8.5	Eigenschaften zur Invertierbarkeit des E_0	251
8.6	Spezielle Inversionsattacke	254
8.7	Unbedingte lineare Korrelationen	255
8.7.1	LSCA-Analyse	255
8.7.1.1	LSCA-Analyse für einen nicht-autonomen Generator	255
8.7.1.2	LSCA-Analyse angewandt auf den E_0	259
8.7.2	Korrelationsgleichungen nach Hermelin und Nyberg	262
8.7.3	Korrelationsgleichungen durch Vollsuche	262
8.8	Ultimative Divide-and-Conquer Attacke	263
8.9	Bedingte Korrelationsattacke	266

8.9.1	Zustandsanalyse für den E_0	267
8.9.2	Bedingte Korrelationen durch Vollsuche	275
8.10	Anwendung der TMT-Attacke auf den E_0	279
8.11	Zusammenfassung	281
9	Zusammenfassung	285
IV	Anhang	291
A	Verzeichnis der Abkürzungen, Symbole und Formelzeichen	293
B	Programmbeschreibungen	309
B.1	Linear zurückgekoppeltes Schieberegister	310
B.2	Nichtlinearer Filtergenerator	311
B.3	LB-Algorithmus	313
B.4	Eigenschaften von Booleschen Funktionen	314
B.5	Bestimmung eines optimalen bzw. suboptimalen T^m	316
B.6	Bedingte Korrelationskoeffizienten zum NLFG	318
B.7	Angriffsverfahren gegen den NLFG	319
B.8	Bestimmung einer optimalen bzw. suboptimalen Phasenauswahl Γ	326
B.9	Konstruktion von Singer Differenzenmengen	327
B.10	Konstruktion von Bose Differenzenmengen	328
B.11	TMT-Attacke und Reduktionsfunktion R_1	329
B.12	Korrelationskoeffizienten für den E_0	332
C	Allgemeine Generatorenmodelle	335
D	Schranken der linearen Komplexität für den NLFG	339
E	Der Summationsgenerator	343
F	Bestimmung von Kontrollpolynomen und Kontrollgleichungen	347
F.1	Einführung	347
F.2	Methode zur Gewinnung von Kontrollpolynomen nach Golić	349
F.3	Gewinnung weiterer Kontrollpolynome	350
F.3.1	Verschieben der Kontrollgleichung	351
F.3.2	Methode des Potenzierens	351
F.4	Anmerkungen	351
G	Die Bluetooth Übertragungstechnologie und der E_0-Generator	353
G.1	Systemübersicht zu Bluetooth	354
G.2	Die Stromverschlüsselung	355

Abbildungsverzeichnis

1.1	Symmetrisches Verschlüsselungssystem	5
1.2	Asymmetrisches Verschlüsselungssystem	7
1.3	Hybrides Verschlüsselungssystem	8
2.1	Synchrone, symmetrische Stromchiffre	22
2.2	Keystreamgenerator	23
2.3	Betrieb einer Blockchiffre im OFB-Modus	24
2.4	Selbstsynchronisierende, symmetrische Stromchiffre	25
2.5	Betrieb einer Blockchiffre im CFB-Modus	27
2.6	Nichtlinearer Filtergenerator	39
2.7	Beispiel zum nichtlinearen Filtergenerator	42
2.8	Combiner-Generator ohne Speicher	44
2.9	Combiner-Generator mit Speicher	45
2.10	Realisierung des $A_5/1$ Algorithmus als Schieberegisterschaltung	48
3.1	Grenzwerte für die Nichtlinearität	73
4.1	Kommunikationsmodell für die Angriffsverfahren gegen den nicht-linearen Filtergenerator	84
4.2	Äquivalentes System bei der Korrelationsattacke nach Siegenthaler	85
4.3	Binäre Entropiefunktion $h(p)$	89
4.4	Zusammenhang der beteiligten Folgen bei den schnellen Korrelationsattacken	90
4.5	Reale Fehlerwahrscheinlichkeit $p_{real}(N)$ beim NLFG aus Beispiel 4.1	91
4.6	Verhältnis $r(N)$ beim NLFG aus Beispiel 4.1	92
4.7	Lineare Approximation des NLFGs bei der BAA-Attacke	100
4.8	Approximation des NLFGs bei der BAA-Attacke	101
4.9	Äquivalenter Generator durch eine lineare Transformation	109
5.1	Funktion $r(k, p, 1)$	139
5.2	Funktion $C'(k, p, 1)$	140
5.3	Funktion $p_{gr}(k, 1, d)$	141
5.4	Die Veränderung der Menge S beim Schritt vom m auf $m + 1$	144
5.5	Fehlermodell der hybriden Korrelationsattacke	159

5.6	Normierte Häufigkeitsverteilung der bedingten Korrelationskoeffizienten zum Beispiel 5.10	161
6.1	Darstellung der Fano Ebene aus dem Beispiel 6.2 als Hypergraphen	173
6.2	Normierte Häufigkeitsverteilung $h'(p) = 2^{-m}h'_1(f, \Gamma, T^m, p)$ zum Abschnitt 6.3.5	193
6.3	Normierte Häufigkeitsverteilung $h'(p) = 2^{-m}h'_2(f, \Gamma, T^m, p)$ zum Abschnitt 6.3.5	193
6.4	Normierte Häufigkeitsverteilung $h'(p) = 2^{-m}h'_3(f, \Gamma, T^m, p)$ zum Abschnitt 6.3.5	194
6.5	Bestimmung von k und n beim Entwurfsprozess des NLFGs	199
7.1	Überlappung von zwei Zustandsketten ohne zufällige Funktion	208
7.2	Zusammentreffen von zwei Zustandsketten mit einer zufälligen Funktion	209
7.3	Funktion $g(u)$	211
7.4	Untere Schranke der Erfolgswahrscheinlichkeit des TMT-Verfahrens von Hellman	212
7.5	ME in Abhängigkeit von TI für die TMT-Schemata	213
7.6	Summe TI + ME für die TMT-Schemata	213
8.1	Aufbau des E_0 -Keystreamgenerators	236
8.2	Durchführung der Basiskorrelationsattacke	248
8.3	Durchführung einer schnellen (unbedingten) Korrelationsattacke	250
8.4	Zustandsgraph für den unbedingten Fall	272
8.5	Zustandsgraph für den bedingten Fall $z_t = 0$	273
8.6	Zustandsgraph für den bedingten Fall $z_t = 1$	274
8.7	Graphische Zusammenfassung aller Attacken gegen den E_0	284
C.1	Nicht-autonomer Generator mit Eingabe und Ausgabe	335
D.1	Untere Schranke der linearen globalen Komplexität beim NLFG	340
D.2	Key-Schranke der linearen globalen Komplexität beim NLFG	340
D.3	Wahrscheinlichkeit für die Erreichung der Key-Schranke beim NLFG341	341
E.1	Aufbau des Summationsgenerators	344

Tabellenverzeichnis

2.1	Zustand des Schieberegisters und erzeugter Keystream für das Beispiel 2.1	43
2.2	Angriffsvarianten der TMT-Attacke gegen den $A_5/1$	48
3.1	Wertetabelle einer Booleschen Funktion	58
3.2	Walsh Transformation einer Booleschen Funktion	62
3.3	Grenzwerte für die Nichtlinearität	72
5.1	Wertetabelle der Booleschen Funktion aus dem Beispiel 5.2	119
5.2	Mächtigkeiten der Mengen $S(\cdot)$	119
5.3	Tabelle mit den spannungsoptimalen T_m^m zu $\Gamma = (0, 2, 3, 8, 12)$. .	131
5.4	Tabelle mit den spannungsoptimalen T_m^m zu $\Gamma = (0, 1, 6, 16, 19)$. .	132
5.5	Tabelle mit suboptimalen T^m zu $\Gamma = (0, 2, 3, 8, 12)$	135
5.6	Werte für die maximalen bedingten Korrelationskoeffizienten $\Lambda_l(f, \Gamma, T^m)$ und $m_{min,l}(f, \Gamma, T^m)$	143
5.7	Werte für $M'(\Gamma_i, T_i^m)$ für die drei Konfigurationen	149
5.8	Werte für die maximalen bedingten Korrelationskoeffizienten $\Lambda_l(f, \Gamma_i, T_i^m)$ und $m_{min,l}(f, \Gamma_i, T_i^m)$	150
5.9	Normierte Werte $2^{-m}h'_l(f, \Gamma_1, T_1^m, p)$ für die Konfiguration K_1 . .	151
5.10	Normierte Werte $2^{-m}h'_l(f, \Gamma_2, T_2^m, p)$ für die Konfiguration K_2 . .	152
5.11	Werte für $2^{-m}h'_l(f, \Gamma_3, T_3^m, p)$ für die Konfiguration K_3	153
5.12	Werte für $2^{-m}h'_l(f, \Gamma_i, T_i^m, p)$ für die Konfigurationen K_1 bis K_3 und $p = 0.8$	154
5.13	Veränderung der Restfehlerwahrscheinlichkeit im Beispiel 5.10 . .	162
6.1	Werte von k für die kein primitives Polynom über dem $GF(2)$ vom Grad k und Gewicht 3 existiert	169
6.2	Werte von k für die kein primitives Polynom über dem $GF(2)$ vom Grad k und Gewicht k existiert	169
6.3	Werte für Γ_{opt} und $M'_{opt}(\Gamma_{opt}, m)$	171
6.4	Untere Schranke $g_u(n, m)$	177
6.5	Spannungsoptimale Singer Differenzenmengen	178
6.6	Spannungsoptimale Bose <i>Modular Distinct Difference Sets</i>	179

6.7	<i>Golomb Ruler</i>	181
6.8	Auswahl der Filterfunktionen für die Fallstudie	191
6.9	Werte der maximalen bedingten Korrelationskoeffizienten der einzelnen Filterfunktionen für die Fallstudie	191
6.10	Primitive Polynome c über dem GF(2) vom Grad $k = 131$ und Gewicht $w = 2^i + 1, 2 \leq i \leq 5$	197
7.1	Normierte Werte für \overline{N}_1 für den Summationsgenerator	229
7.2	Werte für $k_{1,opt}, w_{opt}$ und normiertes \overline{N}_2 für den Summationsgenerator und der Reduktionsfunktion $R_{1,1}$	229
7.3	Werte für $k_{1,opt}, w_{opt}$ und normiertes \overline{N}_2 für den Summationsgenerator und Reduktionsfunktion $R_{1,2}$	230
7.4	Erfolgswahrscheinlichkeiten bei der Durchführung der TMT-Attacke mit $r = 1$ und $u = 1$ auf den Summationsgenerator	230
7.5	Erfolgswahrscheinlichkeiten bei der Durchführung der TMT-Attacke mit $r = 1$ und $u = 0.25$ auf den Summationsgenerator	231
8.1	Beste affine Approximationen von f_3	238
8.2	Zustandsüberföhrungsfunktionen f_3 und f_4 und die Ausgabefunktion g des E_0 sortiert nach y_t	240
8.3	Zustandsüberföhrungsfunktion f_3 und f_4 und Ausgabefunktion g des E_0 sortiert nach Zuständen v_t	241
8.4	Die Werte für $c_{min}(m)$ für $n = 4, M = 4$ und $1 \leq m \leq 8$	246
8.5	Die Werte der besten (unbedingten) Korrelationskoeffizienten	264
8.6	Die Werte der besten bedingten Korrelationswahrscheinlichkeiten vom Typ I	276
8.7	Die Werte der besten bedingten Korrelationswahrscheinlichkeiten vom Typ II	279
8.8	Die Werte der besten bedingten Korrelationswahrscheinlichkeiten vom Typ II separiert nach Gewicht	279
8.9	Werte für TI, ME und ME'' bei der Durchführung der TMT-Attacke	282
8.10	Zusammenfassung aller Attacken gegen den E_0	283
A.1	Verzeichnis der Abkürzungen, Symbole und Formelzeichen	307
E.1	Beispiel zum Summationsgenerator	345
F.1	Werte für den zeitlichen Aufwand zur Berechnung von Kontrollpolynomen	350
F.2	Werte für den Grad der Kontrollpolynome	350

Algorithmenverzeichnis

5.1	Greedy-T^m : Bestimmung eines suboptimalen T^m	133
5.2	Greedy-T^m-(s, w) : Bestimmung eines suboptimalen T^m	134
6.1	Find_c(k, w) : Bestimmung eines primitiven Polynoms mit Maple	169