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

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 Koreferates 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 $c \in \mathrm{GF}(2)[x]$ und einer Booleschen Funktion $f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$ (Filterfunktion), der n Phasen $\Gamma = (\gamma_1, \ldots, \gamma_n)$ 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. Entwurfsvorschläge für Keystreamgeneratoren zur Stromverschlüsselung aufgeführt werden:

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

   Der ursprüngliche NLFG wird dabei durch eine lineare Transformation in einen äquivalenten Generator mit dem gleichen Schieberegister und Rückkopplungspolynom transformiert. Es können durch die Transformation lineare Strukturen in der Filterfunktion f aufgedeckt werden, so dass dadurch zum Beispiel bedingte Korrelationskoeffizienten (siehe Kapitel 5) einen höheren Wert ergeben. Dadurch ist dann eine bedingte oder hybride Korrelationsattacke mit einer größeren Erfolgswahrscheinlichkeit und einer kleineren Rundenzahl durchführbar. Ebenso kann die Spannung der Phasen des NLFGs durch die Transformation verringert werden. Dadurch kann dann eine Inversionsattacke (siehe Abschnitt 4.4) schneller durchgeführt werden.

   Für die Anzahl der Eingangsvariablen der Filterfunktion und den Wert für die Spannung der Phasen des äquivalenten Generators leiten wir Auftrittswahrscheinlichkeiten her, falls ein Angreifer alle möglichen linearen Transformationen testet. Bei der Herleitung wird dabei angenommen, dass die Nullen und Einsen in den Transformationsvektoren gleich und voneinander unabhängig in den Transformationsmatrizen verteilt sind. Fallstudien haben ergeben, dass diese Annahme für Rückkopplungspolynome 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 Transformationsattacke 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 $\Gamma = (0, 1, \ldots, n-1)$ 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 $T^m = (t_1, t_2 \ldots, t_m)$ 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 unbekannten 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:

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

bzw.

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

wobei $g : \mathrm{GF}(2)^{n-2} \to \mathrm{GF}(2)$ 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].

[1] Die 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 benötige Länge N des Keystreams und der Berechnungsaufwand C der einzelnen Attacken auf den E_0 in einer Tabelle zusammengefasst dargestellt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Algorithmenverzeichnis