Über Methoden der Generierung binärer Pseudozufallsfolgen zur Stromverschlüsselung

Dissertation

zur Erlangung des akademischen Grades
eines Doktor-Ingenieurs
des Fachbereichs Elektrotechnik
der FernUniversität-Gesamthochschule
in Hagen

von

Markus Schneider

Hagen 1999

Tag der Einreichung	1. Februar 1999
Tag der mündlichen Prüfung	17. September 1999
1. Berichterstatter	Prof. Dr.-Ing. Firoz Kaderali
2. Berichterstatter	Prof. Dr.-Ing. Ludwig Kittel
3. Berichterstatter	Prof. Dr. rer. nat. Werner Poguntke

Berichte aus der Kommunikationstechnik herausgegeben von
Prof. Firoz Kaderali

Band 4

Markus Schneider

Über Methoden der Generierung binärer Pseudozufallsfolgen zur Stromverschlüsselung

Shaker Verlag
Aachen 1999

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Schneider, Markus:
Über Methoden der Generierung binärer Pseudozufallsfolgen zur Stromverschlüsselung / Markus Schneider.
- Als Ms. gedr. - Aachen : Shaker, 1999
(Berichte aus der Kommunikationstechnik herausgegeben von Prof. Firoz Kaderali ; Bd. 4)
Zugl.: Hagen, Univ., Diss., 1999
ISBN 3-8265-6750-1

Als Manuskript gedruckt. Printed in Germany.

ISBN 3-8265-6750-1
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

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrgebiet Kommunikationssysteme des Fachbereichs Elektrotechnik der FernUniversität-Gesamthochschule in Hagen. An dieser Stelle ist es mir ein Anliegen, allen denjenigen zu danken, die durch ihr Wirken und ihr Tun zu dem Gelingen dieser Arbeit beigetragen haben.

Mein besonderer Dank geht an meinen Doktorvater Herrn Prof. Dr.-Ing. Firoz Kaderali für die Betreuung meiner Arbeit und für die vielen wertvollen Dinge, welche ich unter seiner hilfreichen Anleitung in den Bereichen IT-Sicherheit und Kommunikationstechnik lernen konnte. Herrn Prof. Dr.-Ing. Ludwig Kittel danke ich für die Übernahme des Korreferates und sein Interesse an meiner Arbeit. Mein weiterer Dank gilt Herrn Prof. Dr. rer. nat. Werner Poguntke, der vom ersten Tag meiner wissenschaftlichen Tätigkeit an meine Arbeit mit Interesse verfolgt hat und mir in vielen Diskussionen mit wertvollen Hinweisen und Ratschlägen hilfreich zur Seite stand.

Im Rahmen meines Dankes möchte ich auch meine netten Kollegen hervorheben. Mit Ihnen zusammenzuarbeiten hat mir in der überaus angenehmen Atmosphäre des Lehrgebiets viel Freude bereitet. In zahlreichen – auch über die wissenschaftliche Beschäftigung hinausgehenden – Aktivitäten sind freundschaftliche Verbindungen entstanden, die ebenfalls dazu beitragen, daß ich die Hochschule nur schweren Herzens verlasse.

Keinesfalls vergessen, in meinen Dank einzuschließen, möchte ich alle meine guten Freunde, welche mich über die Jahre hin begleitet und ermuntert haben, und bei welchen ich stets die notwendige Kraft für das Gelingen meiner Arbeit schöpfen konnte.

Mein abschließender Dank gilt meinen lieben Eltern und meiner lieben Schwester, die mit ihrem Tun mich stets unterstützt und mir meine Ausbildung ermöglicht haben.

Hagen im September 1999

Kurzfassung

Verfahren zur Stromverschlüsselung sind zur Schaffung von Vertraulichkeit in der modernen Kommunikationstechnik von großer Relevanz. An die in diesem Kontext benötigten Pseudozufallsgeneratoren sind besonders hohe Anforderungen zu stellen.

In einem systemtheoretischen Ansatz spielen linear zurückgekoppelte Schieberegister zur Erzeugung von Pseudozufallsfolgen eine besonders wichtige Rolle. Um im Rahmen der Pseudozufallserzeugung kryptographisch verwendbare Folgen zu erhalten, sind bekannte Gütekriterien zu erfüllen. Im Fall neu identifizierter kryptographischer Schwächen sind neue Gütekriterien zu entwickeln, aus welchen sich dann neue Konstruktionsmethoden von Pseudozufallsgeneratoren ergeben.

In der vorliegenden Arbeit werden vorhandene Gütekriterien von binären Pseudozufallsfolgen untersucht. In diesem Zusammenhang werden kombinatorische Untersuchungen von Folgen mit geeigneten linearen Komplexitätsprofilen durchgeführt. Darüber hinaus werden statistische Momente der Symbolverteilung in binären Pseudozufallsfolgen mit perfekten linearen Komplexitätsprofilen berechnet und mit den korrespondierenden Momenten von echten binären Zufallsfolgen verglichen. Dabei zeigt sich, daß die Momente 1. und 2. Ordnung von Folgen mit perfektem linearen Komplexitätsprofil annähernd mit den Momenten echter Zufallsfolgen übereinstimmen. Korrespondierende Momente höherer Ordnung zeigen jedoch unterschiedliche Eigenschaften. Desweiteren wird das Komplexitätsmaß der Jump-Komplexität vor dem Hintergrund einer kryptographisch verwendbaren Menge von binären Folgen bewertet.

Im weiteren wird ein Verfahren in zwei Varianten vorgestellt, mit welchen sich jeweils binäre Pseudozufallsfolgen erzeugen lassen, deren lineare Komplexitätsprofile den gewünschten Anforderungen entsprechen. Da der Aufwand zur Folgenerzeugung mit der Folgenlänge ansteigt, eignen sich die beiden Varianten in der Praxis nur für entsprechend kleine Folgenlängen. Wegen des hohen Aufwandes wird der Einsatz der beiden Varianten zur Erzeugung von Folgen mit geeigneten Startprofilen vorgeschlagen.

Ein anderer Gegenstand der Betrachtung ist der Filter-Generator. Hierbei werden unterschiedliche Entwurfskriterien der Konstruktion eines Filter-Gene-

rators zunächst losgelöst voneinander behandelt und danach auf die simultane Erfüllbarkeit der gefundenen hinreichenden Bedingungen hin untersucht. In diesem Kontext werden Bedingungen für die Auswahl der Phasen zum Erreichen von geeigneten Eingangstupelverteilungen, hohe untere Schranken der linearen Komplexität und maximale Periodenlängen angegeben.

Abschließend werden korrelationsimmune Funktionen behandelt. In diesem Rahmen wird eine neue Methode zur Konstruktion m-korrelationsimmuner Funktionen gewünschter Hamming-Gewichte angegeben. Danach werden interessierende Komplexitätsparameter dieser Konstruktionsmethode untersucht und berechnet. Die gefundenen Komplexitätsparameter erlauben es schließlich, eine neue universelle obere Schranke für die Anzahl von m-korrelationsimmunen Funktionen mit n Eingängen angegeben, welche die bisher bekannte und ausschließlich für den Fall '$m = 1$' gültige obere Schranke unterbietet.

Inhaltsverzeichnis