

Jens Rüdinger

Auswirkungen von Seitenkanalangriffen auf das
Design kryptographischer Algorithmen

Beiträge aus der Informationstechnik

Jens Rüdinger

**Auswirkungen von Seitenkanalangriffen auf das
Design kryptographischer Algorithmen**

 VOGT

Dresden 2009

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.ddb.de> abrufbar.

Bibliographic Information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the internet at <http://dnb.ddb.de>.

Zugl.: Dresden, Techn. Univ., Diss., 2009

Die vorliegende Arbeit stimmt mit dem Original der Dissertation
„Auswirkungen von Seitenkanalangriffen auf das Design
kryptographischer Algorithmen“ von Jens Rüdinger überein.

© Jörg Vogt Verlag 2009
Alle Rechte vorbehalten. All rights reserved.

Gesetzt vom Autor
Printed in Germany

ISBN 978-3-938860-27-4

Jörg Vogt Verlag
Niederwaldstr. 36
01277 Dresden
Germany

Phone: +49-(0)351-31403921
Telefax: +49-(0)351-31403918
e-mail: info@vogtverlag.de
Internet : www.vogtverlag.de

Technische Universität Dresden

Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen

Jens Rüdinger

von der Fakultät Elektrotechnik und Informationstechnik der Technischen
Universität Dresden

zur Erlangung des akademischen Grades eines

Doktoringenieurs

(Dr.-Ing.)

genehmigte Dissertation

Vorsitzender: Prof. Dr. rer. nat. habil. H. G. Krauthäuser

Gutachter: Prof. Dr.-Ing. habil. A. Finger

Prof. Dr.-Ing. G. Fettweis

Dr. K. Mayes

Tag der Einreichung: 07.04.2008

Tag der Verteidigung: 21.11.2008

Danksagung

Die vorliegende Dissertation entstand während meiner Tätigkeit als Systemspezialist der Vodafone D2 GmbH. Mein besonderer Dank gilt Herrn Andreas Dorstel sowie der Vodafone D2 GmbH für die Anregung zu dieser Arbeit sowie die Unterstützung während der Durchführung.

In gleichem Maße danke ich meinem betreuenden Hochschullehrer Prof. Dr.-Ing. habil. Adolf Finger vom Lehrstuhl Theoretische Nachrichtentechnik des Instituts für Nachrichtentechnik der TU Dresden für die Betreuung der Arbeit sowie die langjährige erfolgreiche Zusammenarbeit weit über den Rahmen der vorliegenden Dissertation hinaus.

Den Herren Prof. Dr.-Ing. Gerhard Fettweis, Lehrstuhl Mobile Nachrichtensysteme des Instituts für Nachrichtentechnik der TU Dresden und Dr. Keith Mayes, Direktor des Smart Card Centre der Royal Holloway University of London danke ich für die Übernahme der Gutachten sowie die intensive Auseinandersetzung mit meiner Arbeit.

Ein besonderer Dank gilt meiner Frau Ute sowie unseren Kindern Gordon und Nora ohne deren Unterstützung und Verständnis die Durchführung dieser Arbeit nicht möglich gewesen wäre.

Nicht zuletzt danke ich meinen Eltern, die durch ihre Förderung und Unterstützung vor vielen Jahren den Grundstein für die vorliegende Dissertation gelegt haben.

Inhaltsverzeichnis

Abbildungsverzeichnis	xi
Tabellenverzeichnis	xiii
1 Einführung	1
2 Kryptographische Algorithmen	5
2.1 Einordnung und Ziele der Kryptographie	5
2.2 Symmetrische Algorithmen	6
2.2.1 Beschreibung	6
2.2.2 Blockchiffren	7
2.2.3 Stromchiffren	13
2.3 Asymmetrische Algorithmen	13
2.3.1 Beschreibung	13
2.3.2 RSA	15
2.4 Kryptographische Komplexität	16
2.5 Traditionelle Kryptoanalyse	17
3 Seitenkanalangriffe	21
3.1 Einführung	21
3.1.1 Definition von Seitenkanalangriffen	21
3.1.2 Einordnung der Seitenkanalangriffe	22
3.1.3 Klassifikation von Seitenkanalangriffen	24
3.2 Zeitangriffe	25
3.3 Stromangriffe	30
3.3.1 Strommodell	30
3.3.2 Einfacher Stromangriff	33
3.3.3 Statistische Stromangriffe	38
3.3.4 Verbesserungen und Weiterentwicklungen	44
3.4 Elektromagnetische Angriffe	48
3.5 Systematisierung der Seitenkanalangriffe	49

4	Herkömmliche Gegenmaßnahmen	51
4.1	Allgemein	51
4.2	Verhinderung der Datenabhängigkeit	52
4.3	Dekorrelation von Daten und Kanal	52
4.3.1	Verschlechterung des SNRs	53
4.3.2	Verschleierung der Daten	53
4.4	Limitierungen herkömmlicher Gegenmaßnahmen	54
5	Komplexität statistischer Seitenkanalangriffe	57
5.1	Komplexität statistischer Angriffe	57
5.2	Einfluss algorithmischer Parameter	59
5.2.1	Einfluss der Länge l_{k_T} des Teilschlüssels k_T	60
5.2.2	Einfluss der Anzahl n_T der Teilschlüssel k_T	62
5.2.3	Einfluss der Rundenschlüsselerzeugung	63
6	Designmerkmale symmetrischer Blockchiffren	65
6.1	Strukturmerkmale der Algorithmen	65
6.2	Merkmale der Operationen des Algorithmus	67
6.3	Merkmale der Rundenschlüsselerzeugung	72
6.4	Zusammenfassung	74
7	Implementierungsaspekte	77
7.1	Geheimhaltung des Algorithmus	77
7.2	Kaskadieren von Algorithmen	78
7.3	Hamming-Gewicht-konstante Schlüssel	78
8	Bewertung und Vergleich bestehender Algorithmen	83
8.1	AES/Rijndael	83
8.2	MARS	88
8.3	RC6	91
8.4	Serpent	94
8.5	Twofish	97
8.6	Auswertung	103
9	Zusammenfassung und Schlussfolgerungen	107
	Abkürzungen und Formelzeichen	111
	Abkürzungen	111
	Formelzeichen	112
	Literaturverzeichnis	115
	Lebenslauf	129

Abbildungsverzeichnis

2.1	Kanalmodell	5
2.2	Aufbau einer Runde in Feistel-Struktur	9
2.3	Aufbau einer Runde in SPN-Struktur	10
2.4	DES - Rundenfunktion $f(\cdot)$	11
2.5	Prinzipieller Aufbau eines LFSR	14
3.1	Modell der Seitenkanalanalyse	22
3.2	Klassifikation von Seitenkanalangriffe	24
3.3	RSA-Entschlüsselung mittels Schnellem Potenzieren	27
3.4	Hamming-Gewicht-Modell	32
3.5	Stromverbrauch einer DES-Ausführung [68]	34
3.6	Stromverbrauch der 2. und 3. Runde einer DES-Ausführung [68]	34
3.7	Anzahl der Schlüssel $n_{k h_G}$ in Abhängigkeit des Hamming-Gewichts h_G für einen 128 <i>Bit</i> -Schlüssel	36
3.8	Durchschnittlicher Hamming-Gewinn $\overline{g_H}$ eines 256-Bit-Schlüssels bei Kenntnis der Hamming-Gewichte aller n_T Teilschlüssel der Länge l_{k_T}	37
3.9	Graphische Darstellung der Zusammenhänge der DPA	40
3.10	Ergebnis einer DPA [68]	41
4.1	Einteilung herkömmlicher, implementierungsbezogener Maßnahmen gegen Seitenkanalangriffe	52
4.2	Prinzip der Maskierung anhand der Operation $c = m + k$	54
5.1	Algorithmenspezifischen Komplexität B_A in Abhängigkeit der Teilschlüssellänge l_{k_T} für einen Rundenschlüssel der Länge $l_{k_R} = 128$ <i>Bit</i>	61
7.1	Fehlerwahrscheinlichkeit bei der quantitativen Bestimmung des Hamming-Gewichts (± 0) [127]	81
7.2	Fehlerwahrscheinlichkeit bei der qualitativen Bestimmung des Hamming-Gewichts (± 2) [127]	81
8.1	AES - Operationen	84

8.2	AES Rundenschlüsselerzeugung für $n_{k_{32}} \leq 6$	86
8.3	MARS – Struktur einer Runde im vorwärtsgerichteten Kern . . .	89
8.4	MARS – Rundenfunktion E	90
8.5	RC6 – Funktion einer Runde i	92
8.6	RC6 – Funktion der Rundenschlüsselerzeugung i	93
8.7	Serpent - Rundenfunktion	95
8.8	Serpent – Lineartransformation L	95
8.9	Twofish – Rundenstruktur	98
8.10	Twofish – Rundenfunktion g	99

Tabellenverzeichnis

2.1	Anzahl der Runden für AES/Rijndael in Abhängigkeit von Blocklänge l_b und Algorithmenschlüssellänge l_{k_A}	12
3.1	Klassifizierung von Angriffen auf kryptographische Algorithmen entsprechend ihrer mathematisch- physikalischen Basis . . .	23
3.2	Beiträge der verschiedene Bestandteile am Gesamtstromverbrauch	31
3.3	Durchschnittlich effektiv wirksame Schlüssellänge $\overline{l_{k h_G}}$ für unterschiedliche Schlüssel der Länge l_k bei Kenntnis der Hamming-Gewichte h_G aller Teilschlüssel der Länge l_{k_T}	37
3.4	Klassifizierung von Seitenkanalangriffen entsprechend ihres Angriffsziels	49
5.1	Komplexität der statistischen Nachbearbeitung \mathcal{B}_N in Abhängigkeit der Anzahl der Messungen n_M und der Teilschlüssellänge l_{k_T} bei einer Rundenschlüssellänge von $l_{k_R} = 128 \text{ Bit}$	62
6.1	Gegenüberstellung von Algorithmenmerkmalen und algorithmenspezifischen Voraussetzungen von Seitenkanalangriffen . . .	76
7.1	Effektive Schlüssellänge $l_{k h_G}^{max}$ bezogen auf einen Schlüssel der Länge l_k bei ausschließlicher Verwendung von Schlüssel mit maximalen Hamming-Gewicht h_G^{max}	80
8.1	AES – Offset c_i der Operation ShiftRow $SR(\cdot)$ in Abhängigkeit der Blocklänge $n_{b_{32}}$ und der Zeilenzahl i	85
8.2	Propagation der Schlüsselbitabhängigkeit anhand des Bytes b_0 des Schlüsselwortes $w[i]$ bezogen auf die Bytes b_j des Algorithmenschlüssels k_A	87
8.3	Merkmale der betrachteten Algorithmen	102
8.4	Bewertung der betrachteten Algorithmen	104
8.5	Statistische Komplexität der Algorithmen auf Basis algorithmenspezifischer Zwischenergebnisse	106

Kapitel 1

Einführung

Die Kryptographie als die Wissenschaft des Entwurfs und der Analyse kryptographischer Algorithmen spielt eine immer größere Rolle in unserem Leben. So begegnen wir täglich mehrfach Implementierungen kryptographischer Verfahren und wenden diese an.

Kryptographische Verfahren kommen nicht nur in Form von Verschlüsselungssoftware auf dem PC oder beim Austausch von Zertifikaten zum sicheren Surfen im Internet zum Einsatz, sondern finden sich auch in den uns zahlreich umgebenden eingebetteten Geräten wieder.

Eingebettete Geräte (engl. embedded devices) sind spezielle Computer, die, anders als universelle Personalcomputer, für die Erfüllung dedizierter Aufgaben entwickelt wurden. Sie sind eingebettet in Maschinen und Systeme (z.B. Autos, Waschmaschinen, Videorecordern, Mobiltelefonen, usw.) und übernehmen Aufgaben der Steuerung und Kontrolle dieser Maschinen und Systeme.

Eine besondere Form eingebetteter Systeme sind Smartcards. Hierbei handelt es sich um Plastikkarten, die, anders als reine Speicherkarten oder Magnetstreifenkarten, über einen eigenen Prozessor – gegebenenfalls mit kryptographischem Koprozessor –, Speicher für die Speicherung von Programmen (Software) und Daten sowie Ein-/Ausgabeschlittstellen für die Kommunikation nach außen verfügen. Die Schnittstellen nach außen können je nach Bauart kontaktbehaftet oder kontaktlos (NFC, engl. near field communication) erfolgen.

Smartcards kommen unter anderem zum Einsatz als SIM- bzw. USIM-Karten (engl. (universal) subscriber identity modul) in der Telekommunikation, als Bankkarten im Finanzwesen, als Entschlüsselungskarten im Bezahlfernsehen oder auch als Zugangs- und Berechtigungskarten im Transport- und Veranstaltungswesen.

Relativ neu und an Bedeutung gewinnend sind RFID-Tags (engl. radio frequency identification), die beispielsweise in den neuen deutschen Reisepässen zum Einsatz kommen.

Integraler Bestandteil der oben beschriebenen und weiterer Formen einge-

betteter Systeme sind kryptographische Verfahren. Sie sichern – meist transparent für den Nutzer – Berechtigungen beim Zugriff oder Zutritt der genutzten Systeme (Authentizität) und wahren die Geheimhaltung (Verschlüsselung) und Unveränderbarkeit (Integrität) vertraulicher Daten. Sie bilden damit die Basis für die Nutzung eines Systems.

Systeme mit eingebetteten Geräten beruhen darauf, dass die zugrunde liegenden kryptographischen Verfahren (Algorithmen und Schlüssel) sicher sind. Ihre Sicherheit beeinflusst sowohl die Akzeptanz und Nutzung der Systeme beim Kunden als auch das Geschäftsmodell des Betreibers.

Die Sicherheit kryptographischer Verfahren wird dabei von 2 Aspekten bestimmt:

1. Der Algorithmus selbst muss sicher sein. Das heißt, der Algorithmus weist keine kryptographischen Schwächen auf, die einen mathematisch-kryptoanalytischen Angriff gegen ihn ermöglichen.
2. Die Implementierung des Algorithmus muss sicher sein.

Seit den Arbeiten von Kocher (1996, Zeitanalyse [67]) und Kocher, Jaffe und Jun (1998, Stromanalysen [68]) haben sich Seitenkanalanalysen als effiziente Methode erwiesen, Implementierungen kryptographischer Verfahren anzugreifen.

Seitenkanalanalysen sind implementierungsabhängige Methoden kryptographischer Verfahren anzugreifen. Sie beruhen auf Parametern, die während der Ausführung des Algorithmus gewonnen werden (Ausführungszeit, Stromverbrauch, usw.) und ergänzen somit traditionelle mathematischen Analysen, die nur auf Basis von Klartext und Chiffretext arbeiten.

Weisen Algorithmen keine kryptographischen Schwächen auf und sind rechnerisch sicher (engl. computational secure), so gewinnt die Sicherheit der Plattform an Bedeutung. Insbesondere statistische Seitenkanalangriffe auf Basis der differentiellen Stromanalysen (DPA, engl. differential power analysis) haben sich als besonders wirkungsvoll erwiesen. Ihnen ist nur schwer zu begegnen.

Prinzipiell gibt es 2 Möglichkeiten Seitenkanalangriffen zu begegnen:

Implementierungssicht Seitenkanalangriffe werden als Implementierungsangriffe betrachtet und ihnen wird auf Implementierungsebene begegnet. Ziel ist die Entwicklung von Hardware- und Software-Gegenmaßnahmen, um bestehende Algorithmen sicher zu implementieren.

Designsicht Wie im Rahmen der Arbeit gezeigt wird, sind Seitenkanalangriffe algorithmenspezifisch. Sie werden an den anzugreifenden Algorithmus angepasst, und sind damit abhängig vom Algorithmus. Die Designsicht beschäftigt sich daher mit den Fragen:

- Welche algorithmenspezifischen Merkmale beeinflussen die Anfälligkeiten des Algorithmus gegenüber Seitenkanalangriffen?
- Welche Algorithmen sind weniger anfällig als andere? Warum?
- Was kann im Designprozess getan werden Seitenkanalangriffen zu begegnen?

In der vorliegenden Arbeit geht es darum, den 2. Aspekt Seitenkanalangriffen zu begegnen, die Designsicht, näher zu betrachten. Die Betrachtung aus Designsicht hat weitgehende Konsequenzen für das gesamte Gebiet der Seitenkanalanalyse.

Die Seitenkanalanalyse ist ein relativ junges und dynamisches Wissenschaftsgebiet und wird erst seit Ende der 90er Jahre systematisch erforscht. Implementierungsbezogene Kryptokonferenzen wie die seit 1999 jährlich stattfindende CHES-Konferenz (engl. Workshop on Cryptographic Hardware and Embedded Systems) haben sich neben den mathematisch orientierten Kryptokonferenzen wie CRYPTO, EUROCRYPT und ASIACRYPT etabliert und verfolgen die Seitenkanalanalyse schwerpunktmäßig.

Dabei sind in den letzten Jahren sowohl zahlreiche Angriffe als auch Gegenmaßnahmen entwickelt und verbessert worden. Herkömmliche Gegenmaßnahmen betrachten vor allem die Implementierungsabhängigkeit der Seitenkanalangriffe und weisen hinsichtlich Wirksamkeit und Aufwand einige Limitierungen auf.

Anders als bei traditionellen kryptoanalytischen Angriffen ist der Erfolg eines Angriffs mittels Seitenkanalanalyse zudem von den Fähigkeiten und Fertigkeiten des Angreifers abhängig.

Ziel der Arbeit ist eine umfassende Betrachtung der Seitenkanalanalyse aus Algorithmensicht. Dabei geht es sowohl darum, bestehende Seitenkanalangriffe auf algorithmenspezifische Voraussetzungen zu untersuchen und zu klassifizieren, als auch darum, Designmerkmale von Algorithmen hinsichtlich ihres Einflusses auf die Voraussetzungen zu betrachten. Anhand dieser Merkmale soll es möglich sein, kryptographische Algorithmen in Bezug auf Anfälligkeit gegenüber Seitenkanalangriffen zu bewerten.

Der Schwerpunkt der Arbeit liegt dabei auf symmetrischen Verschlüsselungsalgorithmen und passiven nichtinvasiven Seitenkanalangriffen. Symmetrische Verschlüsselungsalgorithmen, insbesondere Blockchiffren, beruhen auf relativ einfachen Designprinzipien. Dadurch ist eine Beeinflussung der Anfälligkeit gegenüber Seitenkanalangriffen, anders als bei asymmetrischen Algorithmen - die auf komplexen mathematischen Problemen beruhen - durch Änderungen im Design möglich.

Passive nichtinvasive Angriffe sind sehr effektiv, einfach anzuwenden und setzen zum Teil keinerlei Kenntnis der Implementierung voraus. Anders als invasive und aktive nichtinvasive Angriffe sind sie nicht zu detektieren und mit herkömmlichen Gegenmaßnahmen schwer zu begegnen.