



Stefan Lucks (Autor)

## **Systematische Entwurfsmethoden für praktikable Kryptosysteme**

### **Systematische Entwurfsmethoden für praktikable Kryptosysteme**

Disseration zur Erlangung des Doktorgrades  
der Mathematisch-Naturwissenschaftlichen Fakultäten  
der Georg-August-Universität zu Göttingen

vorgelegt von  
Stefan Lucks  
aus Lüneburg

Göttingen, 1997

<https://cuvillier.de/de/shop/publications/5011>

Copyright:

Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen,  
Germany

Telefon: +49 (0)551 54724-0, E-Mail: [info@cuvillier.de](mailto:info@cuvillier.de), Website: <https://cuvillier.de>

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Die moderne Kryptographie . . . . .	3
1.2	Der Entwurf von Kryptosystemen: Drei methodische Ansätze . . . . .	4
1.3	Quantifizierte Reduktionen . . . . .	6
1.4	Zielsetzung und Inhalt der vorliegenden Arbeit . . . . .	9
1.5	Veröffentlichungen . . . . .	11
1.6	Anmerkungen zu Sprache und Notation . . . . .	11
<b>2</b>	<b>Elemente der Kryptographie</b>	<b>12</b>
2.1	Bausteine für Kryptosysteme . . . . .	14
2.2	Flußchiffren und Blockchiffren . . . . .	17
2.3	Kryptographisches Hashing . . . . .	21
2.4	Identifikationsprotokolle . . . . .	23
<b>3</b>	<b>Wie man die mutmaßliche Härte des exakten Handelsreisendenproblems nutzt</b>	<b>26</b>
3.1	Das exakte Handelsreisendenproblem (XTSP) . . . . .	28
3.2	Eigenschaften des (modularen) XTSP . . . . .	29
3.3	Wie Handelsreisende sich identifizieren . . . . .	33
3.4	Eigenschaften des Protokolls . . . . .	34
3.5	Heuristische Algorithmen für das XTSP . . . . .	35
3.6	Hamiltonsche Pfade und ihre Bruchstücke . . . . .	38
3.7	Die Kosten des Protokolls . . . . .	41
3.8	Einweg-Hashing und das Erzeugen von Pseudozufallsbits . . . . .	44
3.9	Anmerkungen zu den Kryptosystemen aus Abschnitt 3.8 . . . . .	46

<b>4</b>	<b>Luby-Rackoff Chiffren</b>	<b>49</b>
4.1	Sichere unbalancierte Luby-Rackoff Chiffren . . . . .	49
4.2	Untersuchung der ersten Runde . . . . .	51
4.3	Eine „Abkürzung“ in der dritten Runde . . . . .	54
4.4	Die Rundenfunktionen . . . . .	54
4.5	Die Verschlüsselungsfunktion von SFS . . . . .	56
4.6	Pseudo-Zufälligkeit und “Sicherheit” . . . . .	58
4.7	Beispiel-Chiffren . . . . .	59
4.8	Die Blockchiffren BEAR und LION . . . . .	61
4.9	Die Blockchiffre BEAST . . . . .	63
4.10	“Remote-key”-Verschlüsselung mit BEAST-RK . . . . .	65
4.11	Luby-Rackoff Chiffren und zweiseitige Angriffe . . . . .	70
4.12	Weitere Forschung . . . . .	73
	<b>Literaturverzeichnis</b>	<b>75</b>