Inhaltsverzeichnis

1 Einleitung **3**

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

2 Elemente der Kryptographie **12**

2.1 Bausteine für Kryptosysteme 14

2.2 Flußchiffren und Blockchiffren 17

2.3 Kryptographisches Hashing 21

2.4 Identifikationsprotokolle 23

3 Wie man die mutmaßliche Härte des exakten Handelsreisendenproblems nutzt **26**

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

4 Luby-Rackoff Chiffren **49**

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

Literaturverzeichnis **75**