

## INHALTSVERZEICHNIS

1. Einführung	1
2. Zopfgruppen	2
2.1. Erzeuger und Relatoren	2
2.2. Coxeter-Gruppen	10
2.3. Symmetrische Gruppen	20
2.4. Zopf-Gruppen	26
2.5. Positive Monoide	31
2.6. Das Fundamental-Element $G_n$ im Zopf-Monoid $\mathcal{A}_n^+$	37
2.7. Garside-Element	49
2.8. Garside-Monoide	56
3. Gruppenbasierte Kryptographie	66
3.1. Rechnen in Zopf-Gruppen	67
3.2. Codieren von Nachrichten	71
3.3. Zufälliges Ziehen von Zöpfen	72
3.4. Probleme	72
3.5. Schlüsselaustauschverfahren	73
3.6. Verschlüsseln-Entschlüsseln	74
4. Kryptoanalyse	74
4.1. Attacke auf das Konjugator-Such Problem	74
4.2. Zufälliges Ziehen	78
4.3. Sicherheitsbeweise	78
4.4. Einschätzung der Attacken	79
Literatur	80