

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>9</b>
<b>2</b>	<b>Erweiterte parallelisierbare Version der Cantor-Multiplikation</b>	<b>12</b>
2.1	Die Cantor-Multiplikation	12
2.2	Rekonstruktion kleingradiger Polynome	13
2.3	Kombination von Rekonstruktion und Cantor-Multiplikation	15
2.4	Verallgemeinerung von Rekonstruktion und Anwendung auf die Cantor- Multiplikation	17
2.5	Benchmarks	21
2.5.1	Benchmarks: sequentielle Multiplikation	21
2.5.2	Benchmarks: parallele Multiplikation	22
<b>3</b>	<b>Algorithmen von Niederreiter und Wiedemann</b>	<b>25</b>
3.1	Die Berlekamp-Algebra	25
3.2	Der Niederreiter-Unterraum	28
3.3	Der Black-Box-Ansatz von Wiedemann	35
3.4	Elementarer Black-Box-Niederreiter-Algorithmus	38
<b>4</b>	<b>Black-Box-Niederreiter-Algorithmus</b>	<b>41</b>
4.1	Verbesserungen des elementaren Algorithmus	41
4.2	Datenstruktur	43
4.3	Der Algorithmus	45
4.4	Die Funktion <b>Faktorisierung</b>	49
4.5	Die Funktion <b>Folgenverwertung</b>	52
4.6	Zeitkritische Teile und Parallelisierung	54
4.7	Benchmarks	55
4.7.1	Benchmarks: Matrix · Vektor	55
4.7.2	Benchmarks: serieller Black-Box-Niederreiter-Algorithmus	56
4.7.3	Benchmarks: paralleler Black-Box-Niederreiter-Algorithmus	57
<b>5</b>	<b>Anhang</b>	<b>60</b>
5.1	Implementationsdetails der Multiplikation im binären Fall	60
5.1.1	“Kleine” irreduzible Polynome über $\mathbb{F}_2$ vom Grad 16	60
5.1.2	Arithmetik der Erweiterungskörper	62
5.1.3	Beschleunigung der Cantor-Multiplikation	62
5.2	Dokumentation der C-Library zur $\mathbb{F}_2[X]$ -Arithmetik	64
5.2.1	Sequentielle Implementation	64
5.2.2	Beschleunigte Funktionen	68
5.2.3	Parallele Implementation	69