

**Algorithmische Konstruktion
hyperelliptischer Kurven
mit kryptographischer Relevanz
und einem Endomorphismenring
echt größer als $\mathbb{Z}$**

Dem Fachbereich 6 (Mathematik und Informatik)

der Universität GH Essen

zur Erlangung des Doktorgrades

der Naturwissenschaften (Dr. rer. nat.)

im Oktober 1996 vorgelegt von

Hermann-Josef Weber

aus Waltrop

Inhaltsverzeichnis

0	Einleitung	i
1	Algorithmus	1
1.1	Stufe 1	2
1.1.1	Vorüberlegungen: Das Schottky-Problem für die hyperelliptischen Jacobischen	2
1.1.2	Entwurf der Stufe 1: Die Konstruktion des affinen Rosenhain-Modells über $\mathbb{C}$	6
1.2	Stufe 2	14
1.2.1	Vorüberlegungen: Geometrische Invariantentheorie und hyperelliptische Kurven	14
1.2.2	Entwurf der Stufe 2: Die Konstruktion einer affinen Kurvengleichung in Abhängigkeit vom Definitionskörper	21
2	Anwendungen	29
2.1	Allgemeines über Abelsche Varietäten mit reeller Multiplikation	29
2.2	Einfache 3- bis 5-dimensionale Faktoren der $J_0(N)$	33
2.2.1	3-dimensionale Faktoren der $J_0(N)$	34
2.2.2	4-dimensionale Faktoren der $J_0(N)$	43
2.2.3	5-dimensionale Faktoren der $J_0(N)$	44
2.3	Eine 2-dimensionale Abelsche Varietät mit komplexer Multiplikation	46
2.4	Hyperelliptische Jacobische und Public-Key Kryptosysteme	52
A	Algorithmus aus Kapitel 1	57
B	Tabellen zu den Anwendungen aus Kapitel 2	60
	Literaturverzeichnis	80