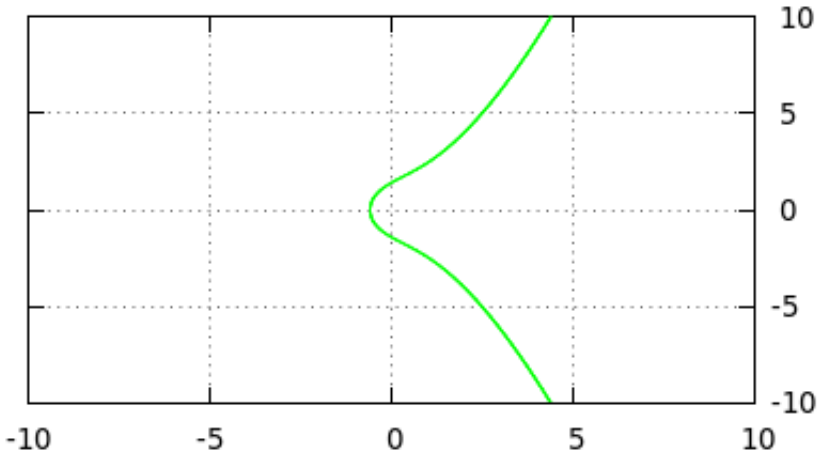
University of Applied Sciences Wedel

**Studiengang: Master Informatik**

**Seminar: Kryptografie mittels elliptischer Kurven**




**Bearbeitet von:** Maurice Tollmien – maurice.tollmien@gmail.com

**Eingereicht am:** 17. Oktober 2015

**FH-Wedel Betreuer:** Prof. Dr. Michael Anders

# Inhaltsverzeichnis

# 1 Einleitung

Die folgende Ausarbeitung dient dem Ziel, einen allgemeinen Überblick zu schaffen über aktuelle asymmetrische Verschlüsselungsverfahren. Dabei wird ein Schwerpunkt auf der Verschlüsselung, Entschlüsselung und Signatur mittels elliptischer Kurven gelegt.

Weiterhin wird die Fragestellung aufgegriffen, ob sich Kryptografie mittels elliptischer Kurven aus Sicht von Effizienz- und Sicherheitsgründen besser eignet als andere asymmetrische kryptografische Verfahren.

Die Motivation für eine weitere Forschung neuer oder unterschiedlicher kryptografischer Methoden abseits der bekannten und verwendeten ist besonders heutzutage wichtig, da es sehr schwer abzusehen ist, wie lange bekannte Verfahren noch sicher verwendet werden können.

In der folgenden Arbeit werden keine neuen Erkenntnisse auf dem Gebiet der Kryptografie mittels elliptischer Kurven gefunden. Vielmehr geht es darum, eine Abgrenzung zu schaffen und verschiedene Verfahren einander gegenüber zu stellen. Dabei wird auch auf praktische Beispiele eingegangen und anhand von Programmcode (Python mit *Sage* [1]) erläutert.

[1] http://www.sagemath.org/de/

# 2 Einleitung in die Mathematik

In den folgenden Abschnitten werden einige grundlegende Algorithmen und Probleme erläutert, welche im Kontext der kommenden Kapitel genutzt werden und essentiell sind für die Funktionalität und Effektivität vieler kryptografischer Verfahren, wie RSA und Methoden mit elliptischen Kurven.

Es wird ein Grundverständnis der diskreten Mathematik (Definition von Ringen, Feldern, Gruppen) für das Verständnis der folgenden Kapitel vorausgesetzt.

## 2.1 Diskretes Logarithmus Problem (DLP)

Sei $G$ eine zyklische Gruppe und $g \in G$.

Gegeben sei ein Element $h$ in der durch $g$ generierten Teilgruppe.

Das diskrete Logarithmus Problem für $G$ besteht nun darin, ein Element $m$ zu finden, welches die Gleichung $h = g^m$ erfüllt.

Der kleinste Wert $m$, welches $h = g^m$ erfüllt, ist der sogenannte Logarithmus von $h$ im Bezug auf $g$. Also: $m = log_g(h)$

Das diskrete Logarithmus Problem wird in der Kryptografie häufig als das zu Grunde liegende Problem für asynchronen Schlüsseltausch, digitale Signaturen oder Hash-Funktionen genutzt.

## 2.2 Diffie-Hellman Schlüsseltausch

## 2.3 Elgamal ?

- Arithmetik und Definition von finiten Feldern
- Diskretes Logarithmus-Problem für Elliptische Kurven (ECDLP)
- Elliptische Kurven über finiten Feldern
- Elliptic Curve Cryptography
- Elliptic Curve Diffie-Hellman
- Elliptic Curve Elgamal
- Abgrenzung zu RSA, Vor/Nachteile
-