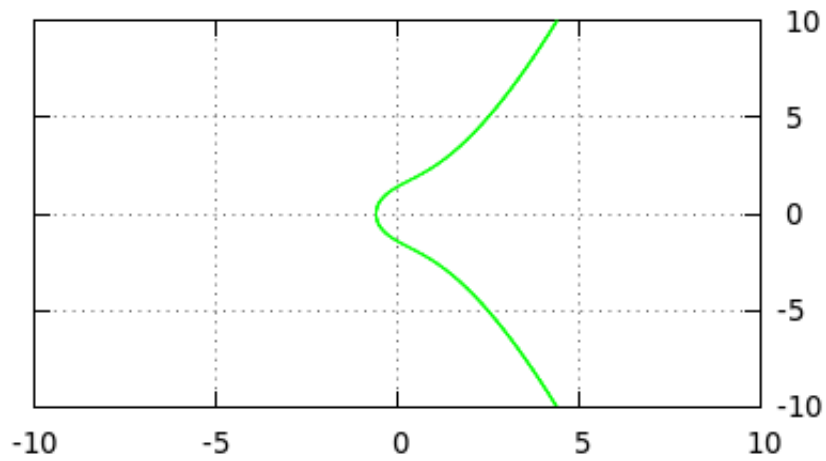


Studiengang: Master Informatik

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	1
2	Einleitung in die Mathematik	2

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

- 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
-