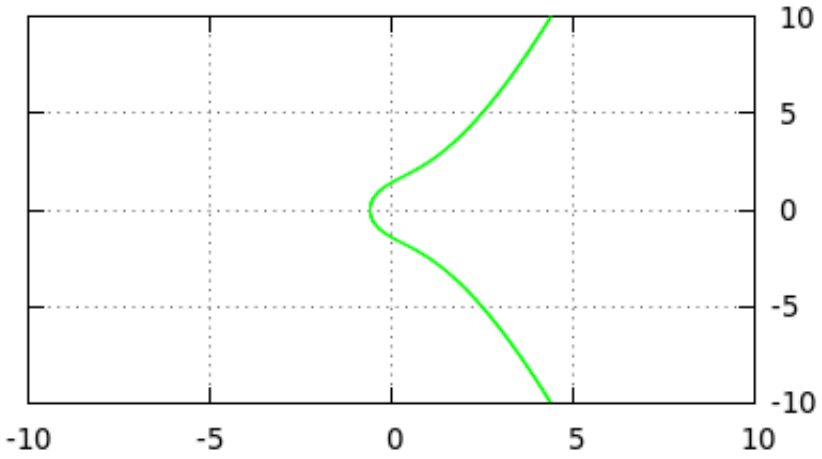
University of Applied Sciences Wedel

Studiengang: Master Informatik

Seminar: Kryptografie mittels elliptischer Kurven



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

Eingereicht am: 19. 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 Zur Erinnerung

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 Prime Restklassengruppen

Bei der Erzeugung asynchroner Verschlüsselungen, zu denen auch die Verfahren elliptischer Kurven gehören, befinden wir uns in mathematischen Gruppen. Eine Gruppe ist meist eine endliche Menge an Elementen, kombiniert mit einem Operator. Also sei $(G, \cdot)$ eine Gruppe. Die Ordnung der Gruppe G entspricht der Anzahl Elemente in G. Die Ordnung eines Elementes $\alpha \in G$ ist die niedrigste Zahl n für die gilt: $\alpha^n = e$ mit $e =$ dem neutralen Element bezüglich des Operators $\cdot$ in G.

Jede (zyklische) Gruppe besitzt einen Generator α, für den gilt, dass $\forall a \in G \; \exists i \in \mathbb{N} : \alpha^i = \alpha \cdot \alpha \cdot \cdots \alpha = a$. Sofern G eine zyklische endliche Gruppe ist und α ein Generator dieser, so entspricht die Ordnung von α der von G.

Ein Beispiel einer primen Restklassengruppe ist $(\mathbb{Z}_p, \cdot)$ mit der Voraussetzung, dass der Generator p eine Primzahl ist. Die Ordnung dieser Gruppe ist $p - 1$.

Alle Operationen asynchroner Verschlüsselungen finden im Kontext meist primer Restklassengruppen statt. Hier muss keine weitere Überprüfung auf Eindeutigkeit und Zyklen erfolgen, da der Generator, eine Primzahl, die gewünschten Eigenschaften der Gruppe bereits vorgibt.

2.2 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. Es eignet sich zur Nutzung in kryptografischen Systemen durch den Umstand, dass sich im Sinne der Komplexitätstheorie der diskrete Logarithmus nur sehr ineffizient berechnen lässt, während die Umkehrfunktion (auch im Sinne der Komplexitätstheorie) einfach berechnen lässt. Diese Art von Funktion nennt sich auch Einwegfunktion und bildet die mathematische Grundlage aller asynchronen Verfahren der Kryptografie.

2.3 Anforderungen an asynchrone kryptografische Verfahren

Asynchrone Verfahren der Kryptografie basieren auf dem Prinzip, dass zwei Kommunikationspartner verschlüsselt miteinander kommunizieren können ohne ein gemeinsames Geheimnis oder Schlüssel abgesprochen zu haben. Zwei entscheidende Anforderungen dabei sind, dass ein beliebiger Angreifer weder in der Lage sein soll die Kommunikation mitzulesen oder sie zu semantisch korrekt manipulieren.

3 Elliptische Kurven

3.1 Allgemeine Funktionsweise

3.2 Diffie-Hellman Schlüsseltausch

3.3 Elgamal ?

- 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
-