Elliptische-Kurven-Kryptographie

Kevin Kappelmann, Lukas Stevens

16. April 2016

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Darstellungsformen nicht vergessen! Edwards Kurven und so

1 Einleitung und Motivation

Kryptosysteme wie RSA, Diffie-Hellman[1] und ElGamal[1], die sich auf die Schwere der Primafaktorzerlegung bzw. dem diskreten Logarithmenproblem über Ganzzahlen stützen, benötigen sehr große Schlüssellängen, um eine ausreichend hohe Sicherheit zu garantieren. Daraus ergibt sich sowohl eine hoher Energie- als auch Speicherbedarf für die Berechnung der Algorithmen, was vor allem für Microchips und eingebettete Systeme ein Problem darstellt.
Eine Lösung für dieses Problem sind elliptische Kurven. Diese algebraischen Kurven tragen eine Gruppenstruktur, über die das diskrete Logarithmenproblem deutlich schwerer lösbar ist, als über Gruppen mit Ganzzahlen. Kryptosysteme, die auf elliptische Kurven beruhen, kommen dadurch mit erheblich kürzeren Schlüsseln bei vergleichbarer Sicherheit aus. [2, Seite 53]
Nachfolgende Tabelle verdeutlicht diesen Sachverhalt. Spalte 1 kennzeichnet die maximale Sicherheit (in Bits) für den jeweiligen Algorithmus und der angegebenen Schlüssellänge (in Bits). Rot markierte Felder gelten als kryptographisch unsicher, grüne als aktuell sicher.

Sicherheitsniveau	RSA/Diffie-Hellman[1]	Elliptische-Kurven
≤ 80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

Tabelle 1: Vergleich Schlüssellängen

Die Verwendung elliptischer Kurven in der Kryptographie wurde Mitte der 1980er Jahre von Neal Koblitz [3] und Victor S. Miller [4] unabhängig voneinander vorgeschlagen. Aufgrund der vorteilhaften Eigenschaften gewinnt die Elliptische-Kurven-Kryptographie (kurz ECC für Elliptic Curves Cryptography) stets mehr an Bedeutung und löst ältere Verfahren wie RSA in den verschiedensten Bereichen ab. Vor allem in Umgebungen mit begrenzten Kapazitäten, wie z.B. Smartcards, ist ECC bereits weit verbreitet.
So verwendet beispielsweise Österreich seit 2004 als Vorreiter für alle gängigen Bürgerkarten ECC [1]. Aber auch die Reisepässe der meisten Europäischen Staaten nutzen inzwischen meist in einer Form ECC. [5]

2 Grundbegriffe

Um elliptische Kurven einführen zu können, müssen wir uns zunächst mit affiner und projektiver Geometrie auseinander setzen. Wir führen hierfür zunächst allgemein die Begriffe der affinen und projektiven Ebene ein und konstruieren uns eine projektive Ebene PG(2, $\mathbb{F}$) über einen beliebigen Körper $\mathbb{F}$.

[1] In der jeweiligen Implementierung als Gruppe über ganze Zahlen

2.1 Affine Ebenen

Definition 2.1. *Es sei $\mathcal{A}$ eine Menge und $\mathcal{G}$ eine Teilmenge der Potenzmenge von $\mathcal{A}$, d.h. $\mathcal{G} \subseteq Pot(\mathcal{A})$. Das Paar $(\mathcal{A}, \mathcal{G})$ heißt affine Ebene, falls folgende vier Bedingungen erfüllt sind:*

(A1) $\forall G \in \mathcal{G} : |G| \geq 2$ *(auf jeder Gerade liegen mindestens zwei Punkte).*

(A2) Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$ (durch zwei verschiedene Punkte geht genau eine Gerade).
Wir schreiben $\overline{a, b}$ für dieses G.

(A3) Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$ (durch jeden Punkt geht genau eine Gerade, die zu einer gegebenen Gerade parallel ist).

(A4) Es gibt drei Punkte $a, b, c \in \mathcal{A}$ mit $c \notin \overline{a, b}$ (es gibt drei Punkte, die nicht alle auf einer Gerade liegen).

Die Menge $\mathcal{A}$ nennt man die Punktmenge und die Menge $\mathcal{G}$ die Geradenmenge der affinen Ebene $(\mathcal{A}, \mathcal{G})$.

TODO Anschaulich beschreibt eine affine Ebene den uns bekannten geometrischen Raum

2.2 Projektive Ebenen

Definition

2.2.1 Die projektive Ebene PG(2, $\mathbb{F}$)

Konstruktion, Beispiel

2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

3 Elliptische Kurven E

Macht Lukas

3.1 Definiton elliptischer Kurven

Wir haben bereits die projektive Ebene PG(2, $\mathbb{F}$) über beliebige Körper $\mathbb{F}$ eingeführt.
Diese hat die folgende Punktemenge:

$$P = \left\{(u : v : w) \,|\, (u, v, w) \in \mathbb{F}^3 \setminus (0, 0, 0)\right\} \tag{1}$$

Nun wollen wir die Punktemenge der elliptischen Kurve einführen. Dazu benötigen wir Polynome in drei Unbestimmten. Der Polynomring mit drei Unbestimmten über $\mathbb{F}$ ist mit

$$\mathbb{F}[X,Y,Z] = \left\{ \sum_{k,l,m \geq 0} a_{k,l,m} \, X^k Y^l Z^m \mid a_{k,l,m} \in \mathbb{F} \right\} \tag{2}$$

definiert. Bemerkung von Kevin: Ich würde Unbekannte statt Unbestimmte verwenden. Ist der gebräuchliche Begriff dazu.

3.2 Die unendliche Gerade über PG(2, $\mathbb{F}$)

Isomorphismus von $\mathbb{F}^2 \to \mathcal{P}_U$

3.3 Affine Darstellung elliptischer Kurven

Erklärung, Beispiel(Graphen)

4 Eine Gruppe über E

Macht Kevin bis 4.3

4.1 Tangenten elliptischer Kurven

4.2 Schnittpunkte von Geraden mit elliptischen Kurven

Unendlich ferne Gerade mit Schnittpunkt $\mathcal{O}$, Affine Geraden, Parallele zur y-Achse

4.3 Die Schnittpunkt-Verknüpfung $\oplus$ über E

Definition, Beweis der Abgeschlossenheit, graphische Interpretation

4.4 Die Gruppe $(E, +)$

Macht Lukas bis fertig
Gruppe ist abelsch mit neutralem Element $\mathcal{O}$, Beispiel

5 Anwendung elliptischer Kurven in der Kryptologie

5.1 ElGamal

Welche Charakteristiken für elliptische Kurven, Domänenparameter

5.2 Noch einen für Signaturen

Welche Charakteristiken für elliptische Kurven, Domänenparameter

Literaturverzeichnis

[1] Elliptische Kurven (Elliptic Curve Cryptography - ECC). https://www.a-sit.at/de/technologiebeobachtung/ecc_curves/index.php. Abgerufen am 15.04.2016.

[2] Elaine Barker. Recommendation for Key Management. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, 2016. Abgerufen am 15.04.2016.

[3] Neal Koblitz. Elliptic curve cryptosystems, 1987.

[4] Victor S. Miller. Use of elliptic curves in cryptography, 1985.

[5] Zdeněk Říha. Electronic passports. https://web.archive.org/web/20100215182600/http://www.buslab.org/SummerSchool2008/slides/Zdenek_Riha.pdf. Archiviert vom Original, abgerufen am 15.04.2016.