FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences
Informatik

Bedienungsanleitung des Taschenrechners für elliptische Kurven

Sebastian Hohns

Betreuer: Professor Dr. A. Scheerhorn

Trier, 03.04.2007

Inhaltsverzeichnis

Abbildungsverzeichnis

1

Anwenderhandbuch

Das Programm wurde in Java implementiert und ist damit auf jeder Plattform lauffähig, sofern diese ein installiertes „Java Runtime Environment“ besitzt.

1.1 Installation

Um das Programm ausführen zu können ist eine Installation einer Java JRE ab Version 6 [1] notwendig.

Die Installation des Programmpakets erfolgt mit Hilfe des „IzPack Java Installers“[2], einem, unter Apache Lizenz stehendem, graphischem Installationsprogramm für Javaprogramme, dass auf sämtlichen Plattformen lauffähig ist. Der Benutzer kann dabei, neben dem eigentlichem Programm, auch die vollständige Dokumentation, den Quellcode, inklusive JavaDoc, und einige Beispielkurven zur Installation auswählen. Außerdem können Programmverknüpfungen und ein Deinstallationsskript erzeugt werden.

Zur Anzeige dieser Dokumentation muss der Acrobat Reader installiert sein.

1.2 Aufbau

Das Aussehen des Programms orientiert sich grob an den Taschenrechnern der verschiedenen Betriebssysteme. So werden die Berechnungen in einem Anzeigefenster vorgenommen, das zusätzlich jedoch beliebig vergrößert oder verkleinert werden kann und außerdem scrollbar ist. Die Ausführlichkeit der Anzeige lässt sich, über eine Auswahlbox in der Symbolleiste und über das Menü, in drei Stufen regulieren:

1. „Endergebniss“ zeigt nur das entgültige Ergebnis der Berechnung an.

[1] Java JRE 6 Download
[2] http://www.izforge.com/izpack/

2. „Zwischenergebnisse“ liefert zusätzlich zum Endergebnis eine Ausgabe der wichtigsten Zwischenrechnungen.

3. „Rechenweg“ gibt den kompletten Rechenweg samt den zur Berechnung verwendeten Formeln aus.

Die Eingabe von Ziffern, die jedoch nur bei der Skalarmultiplikation benötigt werden, erfolgt über ein Tastenfeld, welches man, entweder mit der Maus, oder mit der Tastatur bedienen kann. Soll ein Punkt einer Kurve in die Berechnung mit einbezogen werden, so kann dies mit einem Doppelklick auf die entsprechende Zeile in der, auf der rechten Seite des Programmes dargestellten, Punktetabelle geschehen. Diese Tabelle zeigt alle Punkte, die für die aktuell angewählte Kurve definiert wurden. Es werden die beiden Koordinaten und ein, bei der Punktdefinition wählbarer, Name in dieser Tabelle angezeigt. Zusätzlich bekommt der Anwender die Ordnung des Punktes angezeigt. Ist diese Prim, so wird sie grün hervorgehoben.

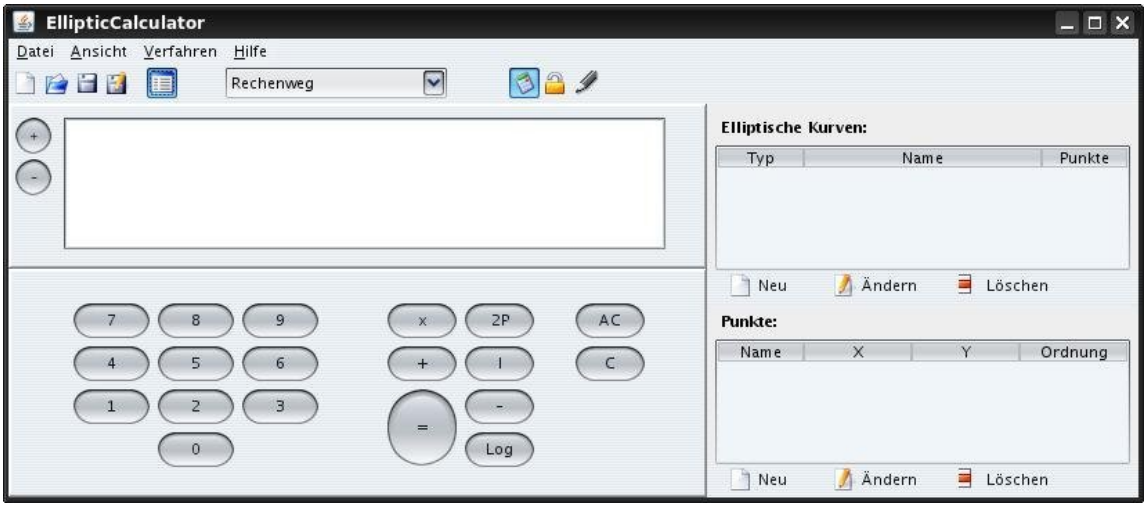

Abbildung 1.1. Programmstart

Neben der Möglichkeit Punkte einer Kurve mit den implementierten Grundrechenarten zu berechnen, können Verschlüsselungs- und Signierungsfunktionen über die Schaltflächen der Symbolleiste und über entsprechende Menüpunkte ausgewählt werden.

Die Symbolleiste und das Menü stellen Funktionen zum Speichern und Laden definierter Kurven bereit. Die Daten werden in einer CSV Datei mit folgendem Aufbau abgespeichert:

```
Feldtyp,Kurvenname,Feldparameter,Kurvenparameter a,Kurvenparameter
b,(Punkt1/X-Koordinate/Y-Koordinate/Ordnung);
```

Der Pfad der aktuell geladenen Datei wird in der Titelleiste des Programms angezeigt.

Neben Kurvendaten wird auch der Zustand des Programms abgespeichert, so dass, nach einem Programmneustart, wieder die vorherigen Einstellungen aktiv sind. Dies umfasst:

- Größe des Anzeigefensters.
- Letzte geladenen Kurvendefinitionsdatei.
- Gewählte Verfahren zur Verschlüsselung und Signierung.
- Position des Programmfensters.

1.2.1 Kurvendefinition

Dem Benutzer steht es frei, beliebige Kurven zu definieren, um mit diesen später Berechnungen durchzuführen zu können. Die bereits definierten Kurven werden in einer Tabelle dargestellt, die Feldtyp, den definierten Kurvennamen und die Anzahl der bereits definierten Punkte beinhaltet. Um neue Kurven anzulegen, bereits definierte Kurven zu editieren oder um Kurven zu entfernen, stehen Optionen über eine Symbolleiste bereit.

Soll eine neue Kurve angelegt werden, so geschieht dies über ein seperates Fenster, in dem alle notwendigen Parameter eingegeben werden können. Dabei ist es für sämtliche Parameter möglich einen Zufallswert erzeugen zu lassen, dessen Größe durch eine Einstellung der maximalen Bitanzahl angepasst werden kann. Das Definitionsfenster ist in zwei Abschnitte unterteilt, die der Reihe nach ausgefüllt werden müssen, um eine gültige Kurve zu erzeugen.

1. Hier wird der Feldparameter definiert. Der Benutzer wird bei der Eingabe unterstützt, indem überprüft wird, ob die derzeitige Eingabe einer Primzahl entspricht. Der Benutzer kann keine Werte eingeben, die über der, in der Aufgabenstellung festgelegten, 32-bit Grenze liegen.

2. Mit der Auswahl der Kurvenparameter a und b wird die Definition der Kurve abgeschlossen. Die Parameter a und b dürfen einen beliebigen Wert, kleiner als der Feldparameter, besitzen.

All diese Werte werden, bereits während der Eingabe, auf ihre Plausiblität überprüft, so dass der Anwender seine Eingaben, mit Hilfe des, im oberstem

Abbildung 1.2. Kurvendefinition

Abschnitt des Fensters platziertem, Bereichs, auf einen Blick überprüfen kann. Genauere Angaben, wie der Wert von Diskriminate und J-Invariante, werden in „ToolTextTips“ angezeigt. Folgende Punkte werden überprüft:

- Die Option **„Feldparameter“** überwacht, ob sich der angegebene Feldparameter innerhalb der Spezifikationen bewegt. So wird sichergestellt, dass er nicht kleiner als die Kurvenparameter a und b ist und er die jeweilige Mindestgröße überschreitet (bei Feldern über F_p muss der Feldparameter einer Primzahl größer drei entsprechen).
- **„Kurvenparameter“** überprüft, ob sich die beiden Kurvenparameter innerhalb des, durch den Feldparameter vorgegebenen, Intervalls bewegen.
- **„Kryptographisch geeignet“** sind Kurven, deren Diskriminate ungleich 0 ist (F_p) ist. .

Ein Speichern der Kurve ist nur dann möglich, wenn alle drei Überwachungsfunktionen ein positives Ergebnis liefern.

Beispiel

Es soll eine neue elliptische Kurve, wie in der Abbildung dargestellt, angelegt werden. Zuerst wird der Feldparameter mit der Primzahl 24317 festgelegt. Nun können die beiden Kurvenparameter ausgewählt werden. Wir wählen den Parameter a mit 8744 und den Parameter b mit 15163. Die Diskriminate kann

mit Hilfe des *„ToolTextTips“* des Unterpunktes *„Kryptographisch geeignet“* überprüft werden. Die so definierte Kurve wird durch betätigen des *„Speichern“* Buttons in die Liste der gespeicherten Kurven aufgenommen.

1.2.2 Punktdefinition

Zu jeder definierten Kurve können Punkte definiert werden. Definierte Punkte werden in einer Tabelle angezeigt, in der der Punktname und die Koordinaten sowie die Ordnung des Punktes ablesbar sind.

Mit Hilfe der, unter der Punkttabelle befindlichen, Symbolleiste können Punkte angelegt,editiert oder gelöscht werden. Das Anlegen eines neuen Punktes geschieht in einem seperatem Fenster.

Abbildung 1.3. Punktdefinition

Jeder Punkt benötigt einen Namen, mit der er vom Anwender identifiziert werden kann. Zusätzlich sind die beiden affinen Koordinaten anzugegeben, entweder per Zufallsgenerator oder manuell durch den Benutzer.

Bei manueller Koordinateneingabe unterstützt das Programm bei der Eingabe, indem die verfügbaren Punkte der Kurve vorberechnet werden, um in einer intelligenten Auswahlliste angezeigt zu werden. Bei Kurven über große Zahlenräume ist die Berechnung der Punkte sehr zeitaufwändig, weshalb diese Funktion erst aktiv wird, wenn die letzten vier Stellen der Koordinate eingegeben werden.

Beispiel

Es soll ein neuer Punkt der Kurve „12-bit“ definiert werden. Dazu wird das Fenster zur Punktdefinition durch Druck der Schaltfläche „Neu“ aufgerufen. Es müssen drei Parameter angegeben werden. Zuerst wird der Punktname mit „P“ festgelegt. Anschließend hat der Anwender die Wahl zwischen der Erzeugung

eines zufälligen Punktes oder der manuellen Parametereingabe.

Wir wählen manuell den Punkt P (757 , 719) aus und speichern ihn mit Hilfe der *„Speichern“* Schaltfläche ab.

1.2.3 Rechnermodus

Der Rechnermodus erlaubt das Rechnen mit Punkten elliptischer Kurven. Es stehen folgende Rechenoperationen zur Verfügung:

- Addition zweier Punkte.
- Subtraktion zweier Punkte.
- Punktverdoppelung
- Berechnung des Inversen eines Punktes.
- Skalarmultiplikation eines Punktes mit einer Zahl.
- Berechnung des diskreten Logarithmus eines Punktes zur Basis eines anderen Punktes.

Die Eingabe der für die Operationen benötigten Parameter erfolgt über ein Tastenfeld, das sowohl mit der Maus als auch mit der Tastatur gesteuert werden kann. Punkte werden per Doppelklick auf den gewünschten Punkt in der, auf der rechten Seite befindlichen, Tabelle zur Punktauswahl ausgewählt.

Durch die Schaltflächen „C“ und „AC“ können alle eingegebenen Werte aus dem Speicher entfernt und der Inhalt des Textfeldes zur Anzeige der Berechnungen gelöscht werden.

Beispiel Punktaddition

Wir wählen die Kurve „12-bit“. Durch Doppelklick wird der Punkt P(1273 , 46) ausgewählt. Anschließend wird die „+“ Schaltfläche betätigt und der Punkt Q(1903 , 2366) in das Berechnungsfenster übernommen. Betätigt man nun die Schaltfläche „=“ erhält man das Ergebnis P + Q = R mit R = (1968 , 1888). Um das Ergebnis in die Punktliste aufzunehmen wird die Schaltfläche „Speichern“ der Symbolleiste betätigt.

Beispiel Punktverdoppelung

Wir wählen die Kurve „12-bit“. Der Punkt P (1273 , 46) soll verdoppelt werden. Dazu wird er durch Doppelklick ausgewählt. Der Benutzer kann ihn nun durch Auswahl der Schaltfläche „2P“ verdoppeln. Man erhält 2P = (2315 , 84).

Beispiel Skalarmultiplikation

Wir wählen die Kurve „12-bit“. Der Punkt P (1273 , 46) soll mit dem Skalarwert „15“ multipliziert werden. Dazu wird der Punkt zuerst durch einen Doppelklick ausgewählt. Anschließend wird die Schaltfläche „x“ betätigt und der Skalarwert über die Oberfläche eingegeben. Man erhält 15 x P mit (640 , 578).

1.2.4 Verschlüsselung

Den Verschlüsselungsmodus erreicht man entweder über die Symbolleiste oder über das Ansichtsmenü. Es stehen zwei Verschlüsselungsverfahren zur Verfügung, ECIES und ElGamal, zwischen denen über das „Verfahren“-Menü gewechselt werden kann.

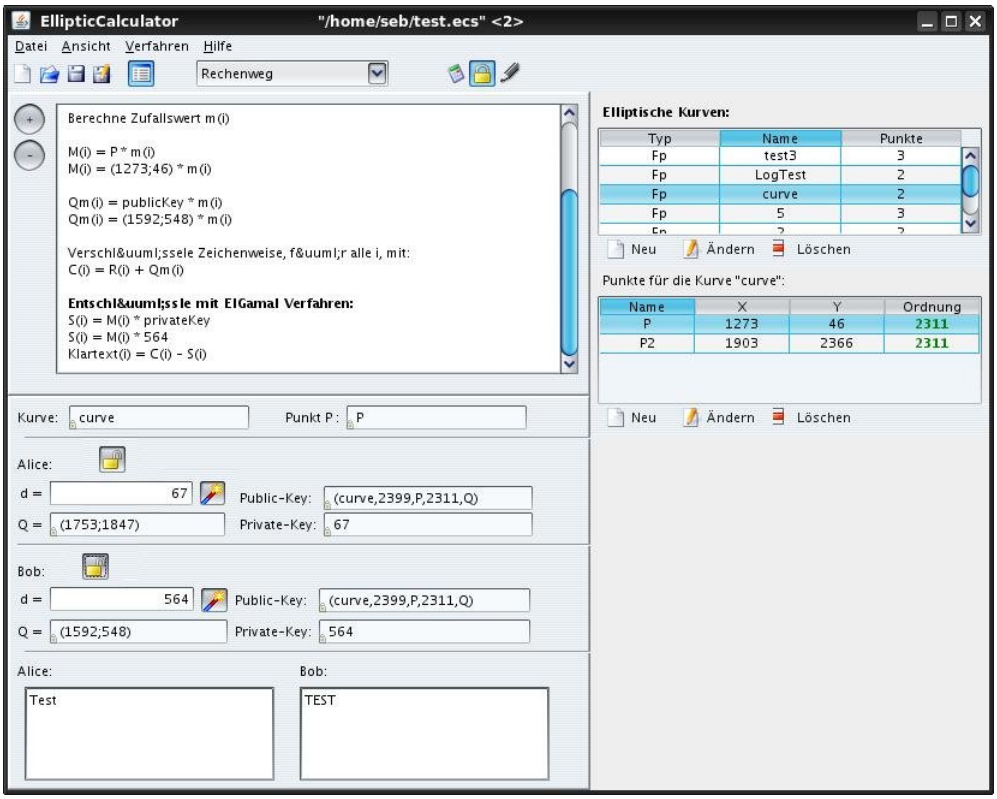

Abbildung 1.4. Verschluesselung

Für beide Verfahren ist es Grundvorraussetzung, dass ein Punkt einer Kurve ausgewählt wird. Der Anwender kann dies mit einem Doppelklick auf einen beliebigen Punkt tun. Anschließend können die beiden Rollen, Alice und Bob, ihre Schlüssel anlegen. Dies kann entweder manuell, durch Eingabe des privaten Schlüssels, oder über einen Zufallsgenerator getan werden. Der private Schlüssel muss dabei einen Wert kleiner als die Ordnung des ausgewählten Punktes besitzen.

Haben beide Parteien ihre Schlüssel erzeugt, können Texte in den Textfelder eingegeben werden. Über die Schaltflächen zum Verschlüsseln wird dann der, im Textfeld der jeweiligen Rolle vorhandene, Text verschlüsselt und versandt. Die Schaltfläche der anderen Partei ändert daraufhin ihr Symbol und erlaubt das Entschlüsseln des gesendeten Textes.

Sämtliche Rechenoperation werden im Ausgabetextfeld angezeigt, dessen Auflösung auch hier über die Symbolleiste in den drei bekannten Stufen verändert werden kann.

Beispiel ElGamal Verschlüsselung

Der Text „Test“ soll mit dem ElGamal Verfahren, wie in der Abbildung dargestellt, verschlüsselt werden. Dazu einigen sich die beiden Parteien Alice und Bob auf die Kurve „12-bit“ und wählen den Punkt P (1243 , 46) durch Doppelklick aus. Nun legen beide Parteien ihre Schlüsselpaare fest. Dazu wählt Alice den Parameter d mit „67“ aus, während Bob den Parameter „d = 564“ festlegt. Das Programm berechnet nun automatisch die beiden Schlüsselpaare. Anschließend kann Alice den Text in ihr Eingabefeld eingeben und die Verschlüsselungsschaltfläche betätigen. In Bobs Anzeige erscheint nun der verschlüsselte Chipertext. Er kann ihn durch die „Entschlüsseln“ Schaltfläche wieder lesbar machen.

1.2.5 Signatur

Den Signierungsmodus aktiviert man über die Schaltfläche der Symbolleiste oder über das Ansichtsmenü. Neben ECDSA steht auch das ElGamal Verfahren im „Verfahren“-Menü zur Auswahl.

Auch hier wird zuerst, wie im Verschlüsselungsmodus, ein Punkt einer Kurve mit einem Doppelklick ausgewählt, wodurch die beiden Rollen, Alice und Bob, ihre Schlüssel, entweder durch einen Zufallsgenerator oder durch manuelle Eingabe, anlegen können.

Beide Parteien teilen sich ein Textfeld zur Eingabe der Nachricht und ein Textfeld zu Anzeige der Signatur. Sobald entweder Bob oder Alice die „Signieren“-Schaltfläche betätigt wird eine Signatur mit ihrem Schlüssel erzeugt und im Textfeld angezeigt. Gleichzeitig ändert sich die Schaltfläche der Gegenpartei und erlaubt ihr die Signatur zu überprüfen.

Beispiel ElGamal Signatur

Der Text „Test“ soll mit dem ElGamal Verfahren, wie in der Abbildung dargestellt, signiert werden. Dazu einigen sich die beiden Parteien Alice und Bob

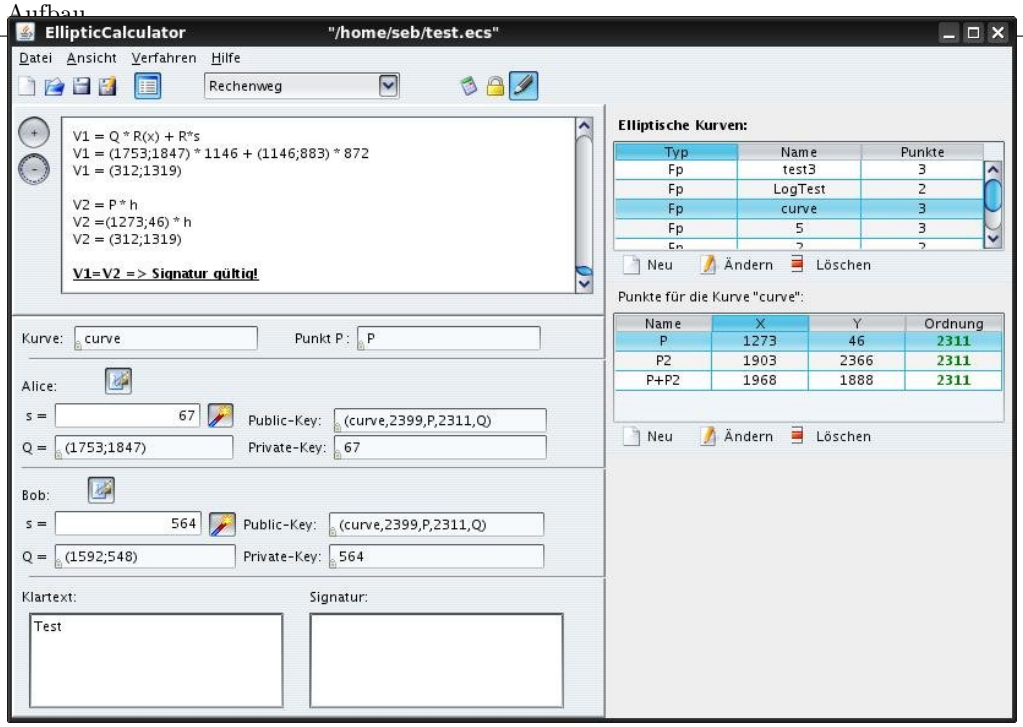

Abbildung 1.5. Signaturmodus

auf die Kurve „15-bit“ und wählen den Punkt P durch Doppelklick aus. Nun legen beide Parteien ihre Schlüsselpaare fest. Dazu wählt Alice den Parameter d mit „67“ aus, während Bob den Parameter „d = 564“ festlegt. Das Programm berechnet nun automatisch die beiden Schlüsselpaare.

Anschließend kann die Partei Alice den Text in das Eingabefeld eingeben und durch betätigen der „Signieren“ Schaltfläche eine Signatur erzeugen. Die Gegenpartei Bob kann diese Signatur mit der „Signatur prüfen“ Option überprüfen.