TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 22.06.2017

Elliptische Kurven in der Praxis: Signaturen mit CrypTool*

Henrik Koy, Deutsche Bank

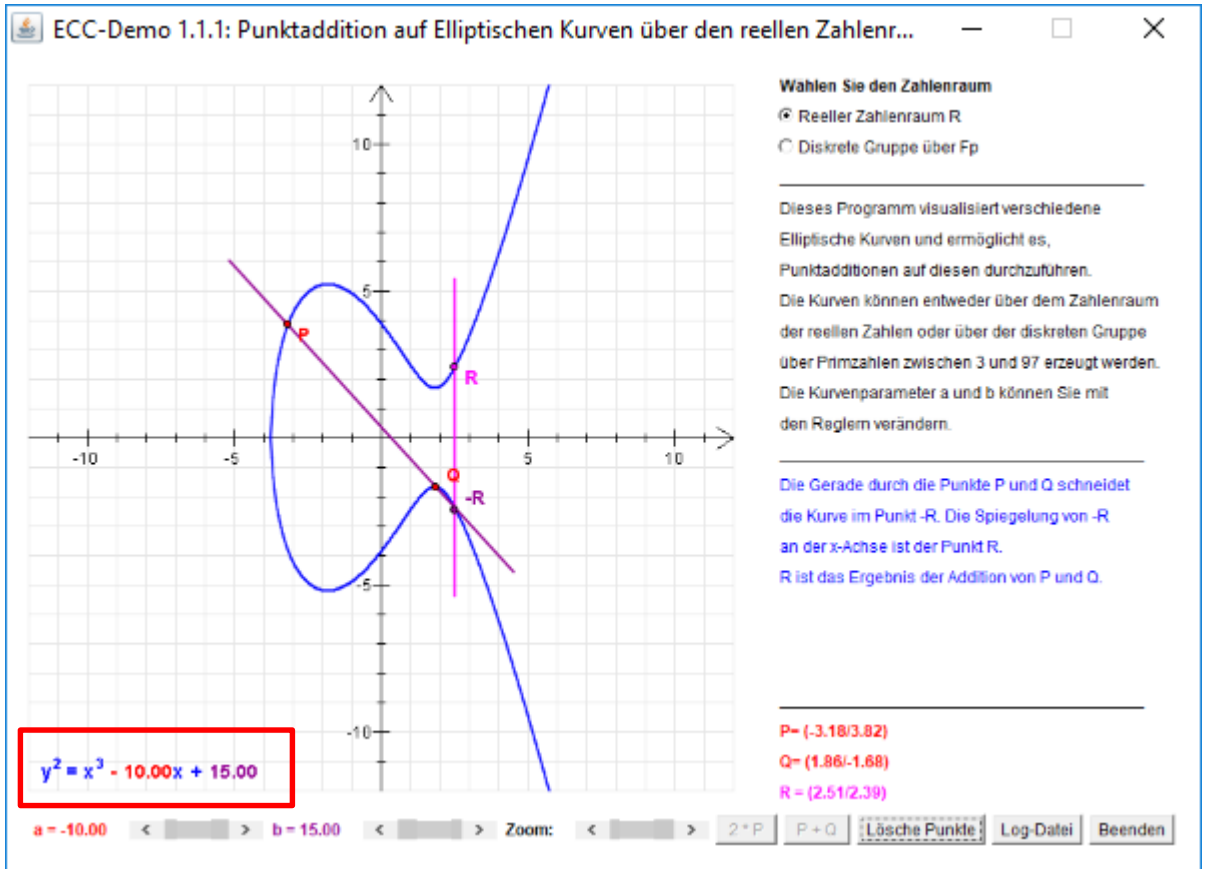
*** https://www.cryptool.de**

Elliptische Kurven Kryptographie
- Warum, und wie kann ich einsteigen?

- Vorteile gegenüber RSA und DSA:
  - Schlüssellängen besser vergleichbar zu den Sicherheitsparametern symmetrischer/Hash Verfahren
  - Viel schneller (Signatur-Erstellung und Diffie-Hellman Schlüsselaustausch)
- Frühere Einschränkungen (Patente, Interoperabilität, …) gelten heute nicht mehr.

➔ CrypTool bietet eine Visualisierung Elliptischer Kurven und man kann digitale Signaturen ausprobieren.

Elliptische Kurven



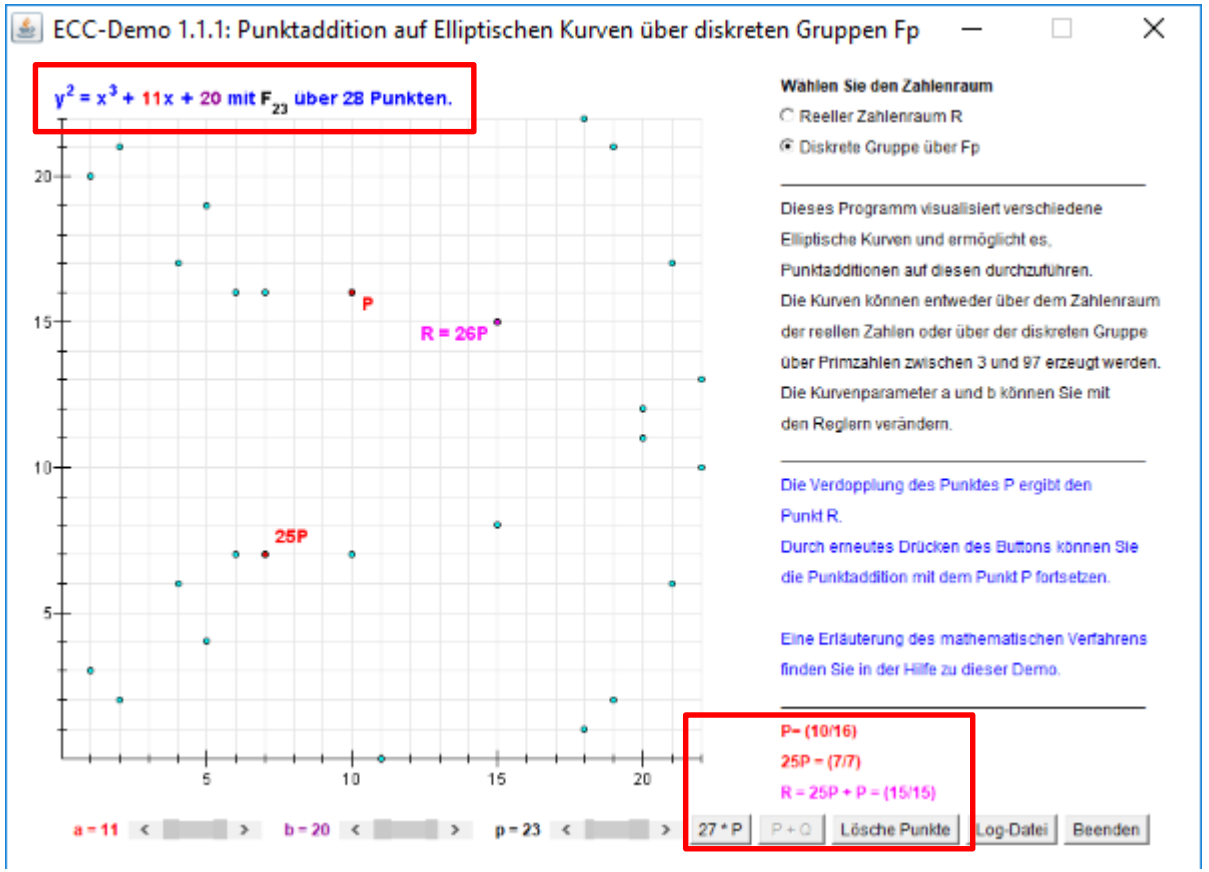
Auf Elliptischen Kurven – definiert durch die Gleichung

$$y^2 = x^3 + a*x + b$$

kann man zwei Punkte auf der Kurve P und Q "Addieren". Das Ergebnis ist wieder ein Punkt R auf der Kurve.

… Im CrypTool Menü:
- ➔ Einzelverfahren
- ➔ Zahlentheorie interaktiv
- ➔ Punktaddition auf Elliptischen Kurven

Elliptische Kurven Kryptographie



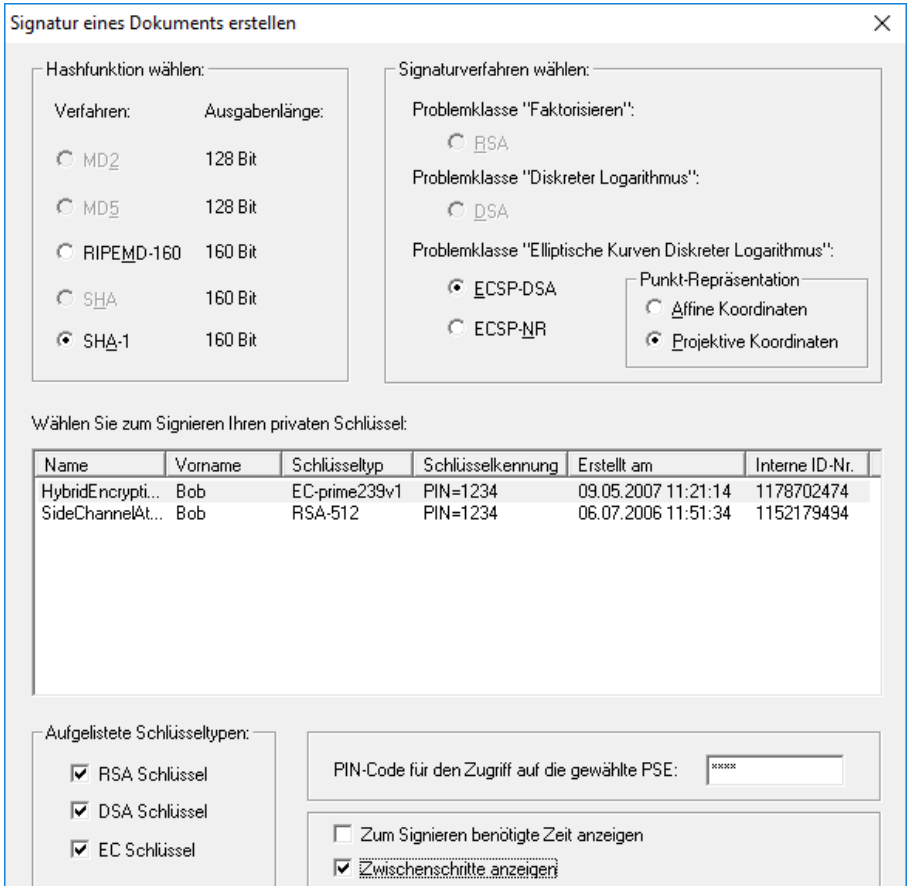
Die Eigenschaft der Punkt Addition bleibt erhalten, wenn man über diskrete Gruppen F_p statt mit reellen Zahlen rechnet.

Für die Kryptographie ist das Vielfache eines Punktes interessant:

Gegeben ist ein Punkt Q auf der Elliptischen Kurve und ein zweiter Punkt P.

Finde eine ganze Zahl z mit z*P = Q.

Elliptische Kurven Signaturen



Mit CrypTool kann man ECC Signaturen ausprobieren …

- Erzeugen von ECC Schlüssel und ECC Zertifikate
- ECC Signaturen
- ECC Signatur Verifikation

Vergleiche auch z.B.
BSI: TR-03111
"Elliptic Curve Cryptography", Section 4.2.1.1. Signature Algorithm

… Z.B. Im CrypTool Menü:
➔ Digitale Signaturen/PKI
➔ Dokument Signieren…

Workshop-Ergebnisse

- Cryptool ist auch für eine Einführung von Elliptischer-Kurven-Kryptografie geeignet http://www.cryptool.de

- Macht Migration auf ECC Zertifikate noch Sinn?
  - Sollte man gleich auf "*Post Quantum Cryptography*" Verfahren setzen?
  - Auf der anderen Seite sind RSA-Schlüsselparameter von mehr als 2048 Bit Schlüssellänge weniger effizient als sichere ECC Verfahren