Kryptografie mit elliptischen Kurven ECC

Uli Kleemann

October 5, 2020

About me

- Uli KLeemann
- Linux-Systemadninistrator
- crypto
- geheim
- code

Vorwort

Schon sehr früh haben sich Menschen Gedanken daruber gemacht, wie Informationen geheim und sicher an andere ubertragen werden konnen. Waren die Methoden für die sichere Datenübertragung früher noch deutlich unterschiedlicher als zu heutigen Zeiten, sind sie im Grunde noch sehr ähnlich und verfolgen stets dasselbe Ziel: Informationen sicher von Person A nach Person B zu transportieren, ohne dass eine Person C Auskunft über den Inhalt der Informationen erhalten kann

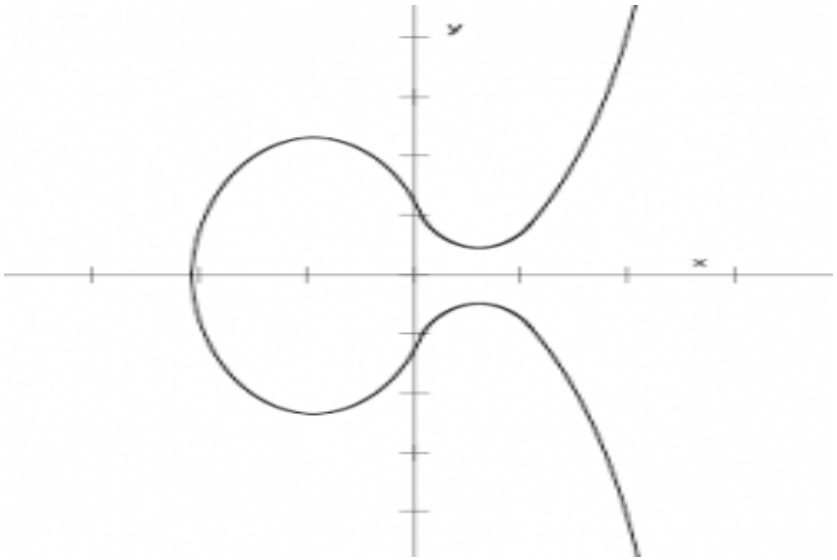
Agenda

1. Warum elliptische Kurven
2. Definition elliptische Kurven
3. Anwendungen in der Kryptografie
4. Prinzip der ECC
5. Problem des diskreten Logarithmus
6. Edwards Kurven
7. Diffie-Hellmann Schlüsselaustausch
8. DH Protokoll
9. Entstehung und Schwachpunkt von DH
10. Elliptic Curve DH
11. Signaturerzeugung
12. Angriffe auf ECDH (Minerva, Känguruh)
13. Sicherheit von ECC
14. Schwache eliptische Kurven
15. der MOV Algorithmus
16. reine anormale Kurven
17. ECC vs. RSA Schlüssel

Warum elliptische Kurven?

- bei RSA sind die maximalen Schlüssellängen erreicht
- immer längere Schlüssel immer längere Rechenzeit immer höherer Energieverbrauch
- keine wesentlich höhere Sicherheit durch Verdopplung der Schlüssellänge
- 128-bit ECC entprechen 3072-bit RSA

Definition elliptische Kurven



Eine elliptische Kurve ist eine Menge von Punkten (x, y) in der Ebene, die folgender Gleichung genügen:

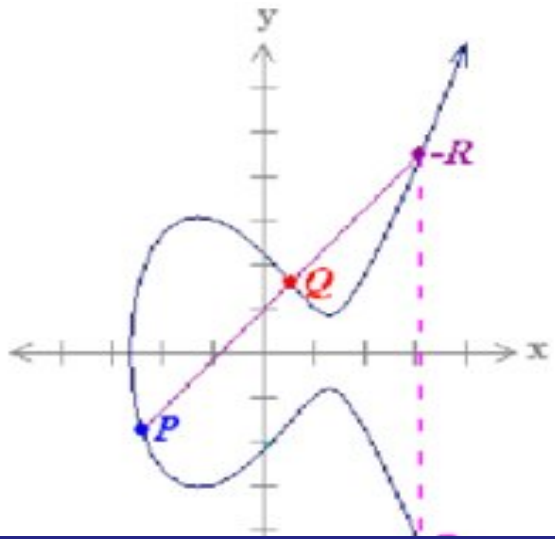
E = (x, y) — y2 = x3 + ax + b vereinigt u zusammen mit dem Punkt im Unendlichen O.

Zur Erinnerung

Es ist bekannt, dass im Körper der reellen Zahlen R unendlich viele Elemente existieren. Mit diesen Elementen lassen sich die Grund-Operationen +, -, * und / durchführen. **Ein endlicher Körper F besitzt dieselben Operationen unterscheidet sich aber dadurch, dass die Anzahl der Elemente auf eine bestimmte Menge q begrenzt ist.** Eine elliptische Kurve über einem endlichen Körper K ist die Menge der Punkte (x,y) welche z.B. eine Gleichung der Form

$$Y2 = X3 + Ax + B$$

erfüllt.wobei x, y, A, B Elemente von K sind. Zusammen mit einem speziellen Punkt 0, der "Punkt an Unendlich" genannt wird, bildet eine elliptische Kurve eine Gruppe.



Anwendung in der Kryptografie

- 1986 von Neal Koblitz (University of Washington) und Victor Miller (IBM) vorgeschlagen
- ECC wurde von Certicom entwickelt (heute BLACKBERRY)
- 3Com, Cylink, Motorola, Pitney Bowes, Siemens, TRW und VerFone, Firefox und Thunderbird und der neue Bundespersonalausweis nutzen Elliptic Curve Cryptography

Prinzip der ECC

Wird ein Punkt g auf einer elliptischen Kurve E über ganze Zahlen gewählt und v-mal mit sich selbst verknüpft, so lässt sich aus dem Ergebnis

$$\mathbf{q = gv} \tag{1}$$

nicht auf v zurückschließen.

Das Problem des diskreten Logarithmus

G

Gegeben seien eine Primzahl **p** und zwei ganze Zahlen **g, y.** Gesucht ist eine ganze Zahl **x** mit der Eigenschaft $\mathbf{g^x \bmod p = y}$ Gesucht ist also der Logarithmus* von y zur Basis g, allerdings nicht über den reellen Zahlen, sondern modulo einer Primzahl, daher auch der Name diskreter Logarithmus. * den Exponenten, mit dem eine vorher festgelegte Zahl, die Basis, potenziert werden muss, um die gegebene Zahl, den Numerus, zu erhalten

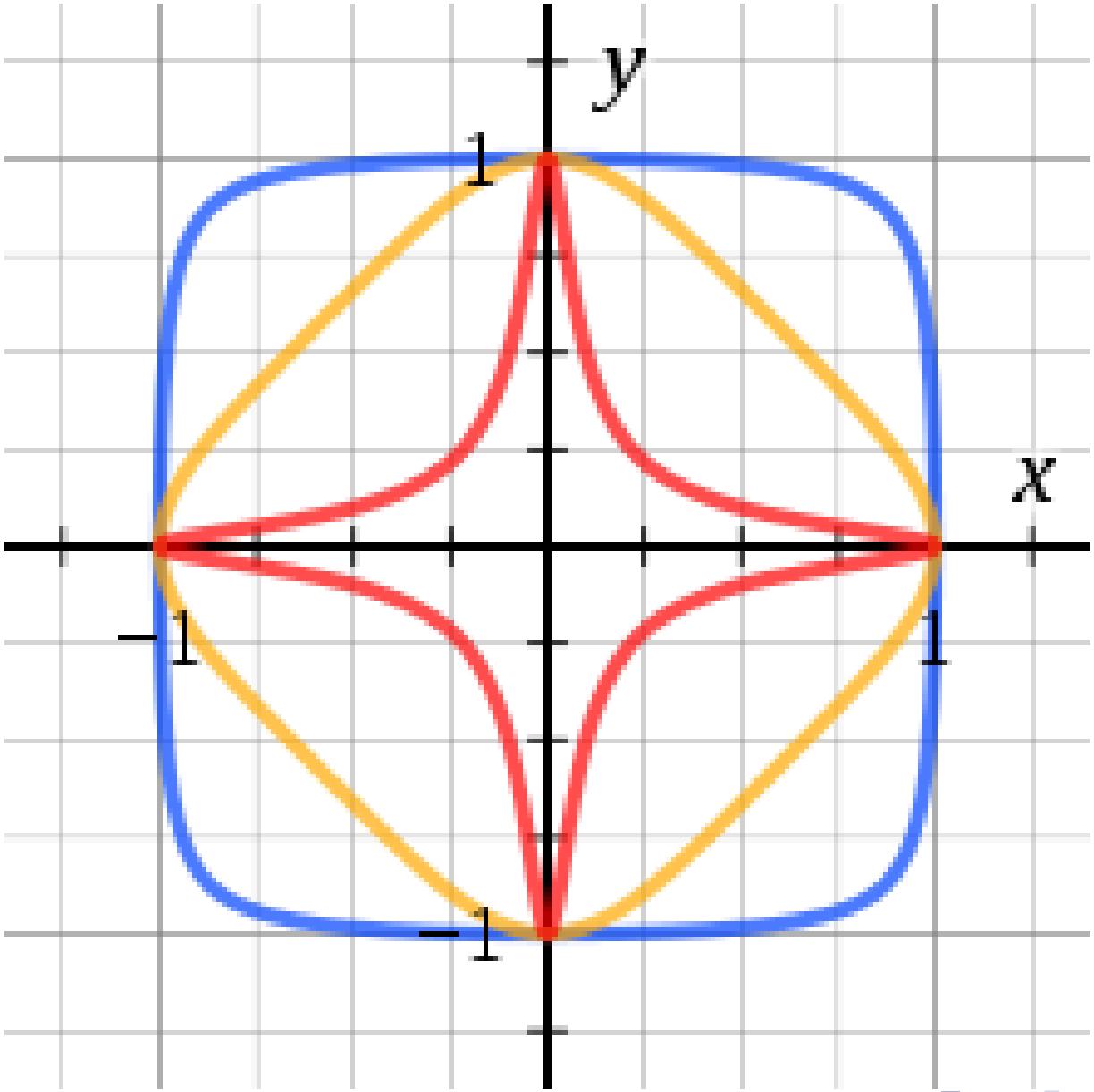
Curve Cryptofraphy

Die Edwards Kurven

- 2007 von Harold Edwards zum ersten Mal vorgestellt
- folgen der Gleichung

$$x^2 + y^2 = 1 + dx^2y^2 \tag{2}$$

Vorteil von Edwards-Kurven



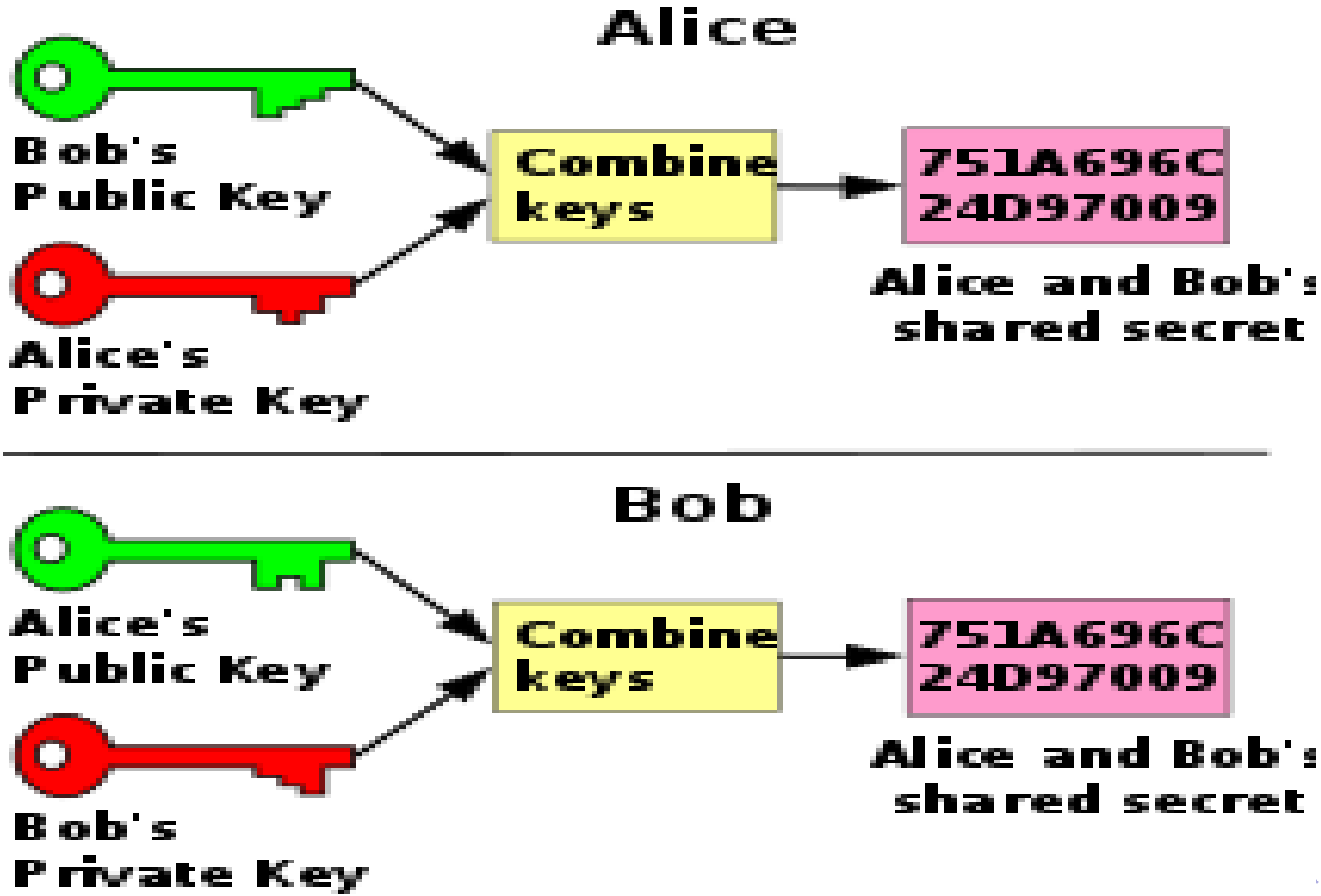
Diffie-Hellmann Schlüsselaustausch

- **wurde von Whitfield Diffie und Martin Hellman entwickelt**
- **im Jahr 1976 unter der Bezeichnung ax1x2 veröffentlicht**
- **ist ein Protokoll zur Schlüsselvereinbarung**
- **ermöglicht, dass zwei Kommunikationspartner über eine abhörbare Leitung einen gemeinsamen geheimen Schlüssel in Form einer Zahl vereinbaren können, den ein Lauscher nicht berechnen kann**
- zählt zu den Krypto-Systemen auf Basis des diskreten Logarithmus
- basieren darauf, dass die diskrete Exponentialfunktion in bestimmten zyklischen Gruppen eine Einwegfunktion ist

$$b^x \, mod p$$

p ist auch für große Exponenten effizient berechenbar Umgekehrt, der diskrete Logarithmus, jedoch nicht Es existiert bis heute kein „schneller“ Algorithmus zur Berechnung des Exponenten x, bei gegebener Basis b, Modul p und gewünschtem Ergebnis.

Geheimer DH Schlüsselaustausch



Das Diffie-Hellman Protokoll

Alice und Bob verständigen sich, über einen unsicheren Kanal auf zwei möglichst grosse Primzahlen a und p, die auch Eve bekannt sein dürfen. Bob wählt einen geheimen Schlüssel Xb und berechnet den dazugehörigen öffentlichen Schlüssel nach folgender Formel:

$$Yb = aXbmodp.$$

Alice geht genauso vor, wählt allerdings einen eigenen geheimen Schlüssel Xa und berechnet den öffentlichen wie folgt:

$$Ya = aXamodp$$

Nun können beide die öffentlichen Schlüssel Ya und Yb austauschen und es wird wieder gerechnet. Der Schlüssel Sa (Alice) berechnet sich aus

$$YbXamodp$$

und Sb (Bob) aus

$$YaXbmodp$$

Beide Berechnungen führen zum selben Ergebnis - dem geheimen Schlüssel S (Sa = Sb).

Entstehung und Schwachpunkt des DH Verfahrens

Bereits in den frühen 1970er-Jahren entwickelten Mitarbeiter des britischen Government Communications Headquarters (GCHQ) als Erste asymmetrische Kryptosysteme
Der DHM-Schlüsselaustausch ist allerdings nicht mehr sicher, wenn sich ein Angreifer zwischen die beiden Kommunikationspartner schaltet und Nachrichten verändern kann. Diese Lücke schließen Protokolle wie das Station-to-Station-Protokoll (STS), indem sie zusätzlich digitale Signaturen und Message Authentication Codes verwenden.

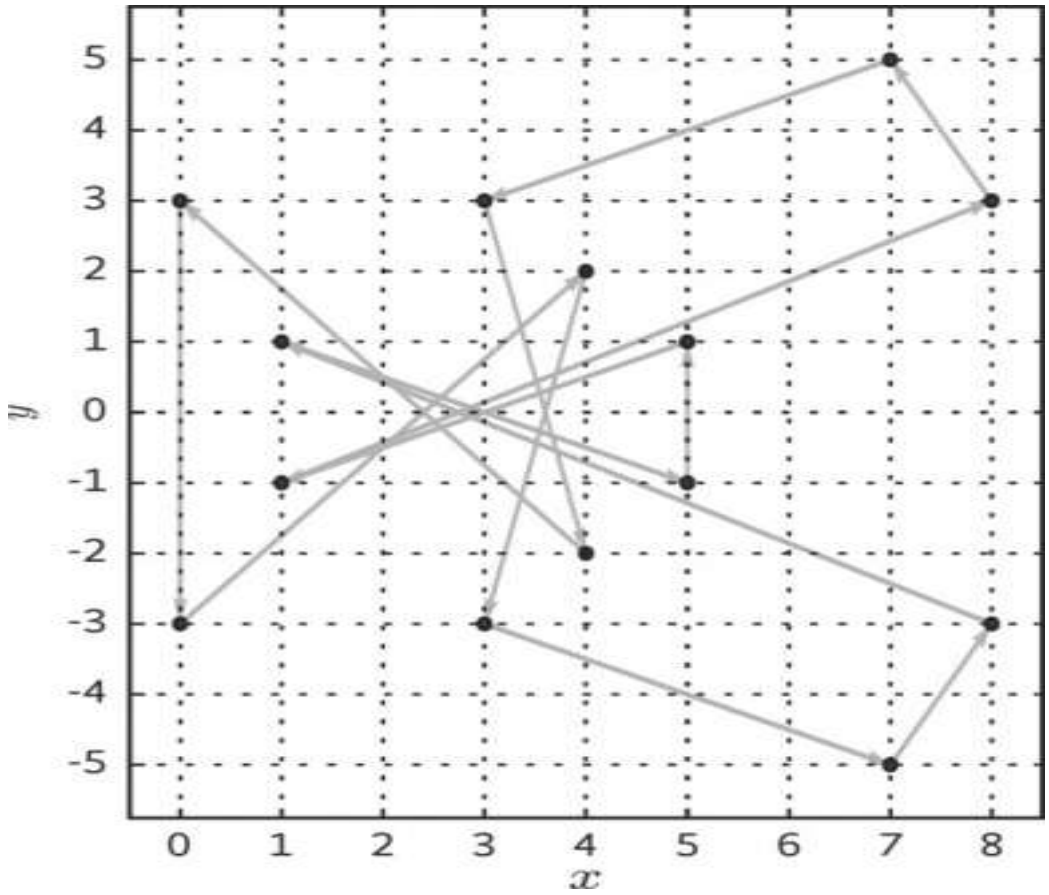
Elliptic Curve Diffie-Hellman (ECDH)

- wurde Mitte der 1980er Jahre von Victor S. Miller und Neal Koblitz unabhängig voneinander vorgeschlagen
- Jedes Verfahren, das auf dem diskreten Logarithmus in endlichen Körpern basiert, lässt sich in einfacher Weise auf elliptische Kurven übertragen und somit zu einem Elliptic-Curve-Kryptosystem umformen
- dabei werden die eingesetzten Operationen (Multiplikation und Exponentiation) auf dem endlichen Körper ersetzt durch Punktaddition und Skalarmultiplikation+ auf elliptischen Kurven
- Das n-fache Addieren eines Punktes P zu sich selbst (also die Multiplikation mit dem Skalar n) wird mit nP bezeichnet und entspricht einer Exponentiation

$$n^p$$

im ursprünglichen Verfahren

Geheimer Schlüsseltausch



Elliptische Kurven bestehen aus Punktmengen, deren Koordinaten auf einer „Kurve“ liegen.

$$yx + ax + bmodp$$

Nimmt man als Generator den Punkt (5,1), erhält man durch

Schlüsselaustausch

A erzeugt eine Zufallszahl r und sendet r·P0 an B

B erzeugt eine Zufallszahl s und sendet s·P0 an A

B berechnet s·(r·P0) =r·s·P0

A berechnet r·(s·P0) =r·s·P0

Beide verfügen dann mit dem Punkt

$$rsP0$$

über ein gemeinsames Geheimnis.

Signaturerzeugung

A erzeugt eine Zufallszahl k ,

berechnet R=k·P0

und setzt r= xR mod q (4)

Zur Signaturprüfung werden von B folgende Schritte ausgeführt:

1. berechne s·PA=(k·rH(m)) ·P0
2. berechne t= r1 mod q
3. berechne t· (s·PA+H(m) ·P0) =S
4. **Die Signatur ist gültig, falls xS mod q=r**

Angriffe auf ECC

der Minerva Angriff auf Smartcards
Werden Implementierungen kryptographischer Signaturen mit elliptischen Kurven nicht vor Timing-Angriffen geschützt,kann ein Angreifer unter Umständen den privaten Schlüssel berechnen

- angegriffen wird ein Nonce-Wert, ein Zahlenwert, der einmalig sein muss und den ein Angreifer nicht kennen darf
- Mit einigen Hundert bis einigen Tausend beobachteten Signaturen lässt sich ein Angriff durchführen
- Damit ein solcher Angriff funktionieren kann, muss man die Zeit, die eine Signaturoperation benötigt, sehr genau messen können

Angriffe auf ECC

der Känguruh Angriff Annahme:ich habe einige Teile eines privaten Diffie-Hellman-Schlüssels abgefangen

$$x = nmodr$$

- Beim ECDH-Problem über

  $$E(Fp)$$

  versuchen wir zu lösen

  $$y = xG \tag{6}$$

- wo **G** ein Basispunkt ist für die Gruppe
- Mit dem privaten Schlüssel, den ich bisher habe, habe ich die folgende Transformation:

  $$x = nmodrßx = n + mr$$

y=(n+mr)G=nG mrG
(7)

Sicherheit von ECC

- Die Forschung im Bereich der elliptischen Kurven wird seit ca. 150 Jahren betrieben. Seit ungefähr 1985 ist bekannt, dass das Eliptische Kurven DL-Problem für die Kryptographie genutzt werden kann. Kein führender Mathematiker hat bis heute eine bemerkenswerte Schwachstelle entdeckt.
- Es muss jedoch beobachtet werden, dass es Klassen von ungeeigneten Kurven gibt, und zwar sind sogenannte **supersinguläre Kurven**, so wie auch sogenannte **anomale Kurven** nicht geeignet. Die Attacken auf die Letzteren wurden unabhängig von einander von Semaev, Smart, Satoh und Araki, und für den allgemeinen Fall von Rück gefunden.
- Ansonsten bietet ein System, das auf elliptischen Kurven mit einem Modulus von 160 Bit basiert, die gleiche kryptographische Sicherheit wie ein RSA-System mit einem 1024 Bit Modulus. Ein 256 Bit ECC-Schlüssel ist mit einer 3072 Bit RSA-Verschlüsselung vergleichbar und eine ECC-Schlüssellänge von 512 Bit bietet dieselbe Sicherheit wie ein utopischer 15000 Bit RSA-Schlüssel.

Schwache elliptische Kurven

Singuläre Elliptische Kurve
Eine Kurve, definiert über dem Körper K durch eine Gleichung

$$F(X, Y) = 0$$

(wobei F(X,Y) irreduzibel über dem algebraischen Abschluss K^{-} von K ist) heisst singulär in einem Punkt (x0, y0) (auf der Kurve), falls beide Ableitungen in dem Punkt verschwinden, d.h.

$$F(x0, y0) = 0, Fx(x0, y0) = 0 und Fy(x0, y0) = 0$$

Eine Kurve heisst nichtsingulär, wenn

$$in K kein Punkt (x0, y0) A2(K)$$

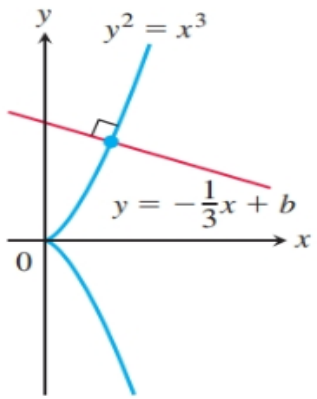
existiert für den beide Ableitungen verschwinden. Eine Gleichung obiger Form nennt man Weierstrass-Gleichung

supersinguläre Kurven

Eine “supersinguläre” Kurve ist eine Kurve, für die die Anzahl der Punkte genau p+1 ist. *(Jedenfalls, wenn man modulo einer Primzahl p5 rechnet.)* Für supersinguläre Kurven gibt es den MOV-Algorithmus2, der in subexponentieller Zeit entschlüsselt.

Beispiele

The graph of $y^2 = x^3$ is called a **semicubical parabola** and is shown in the accompanying figure. Determine the constant b so that the line $y = -\frac{1}{3}x + b$ meets this graph orthogonally.



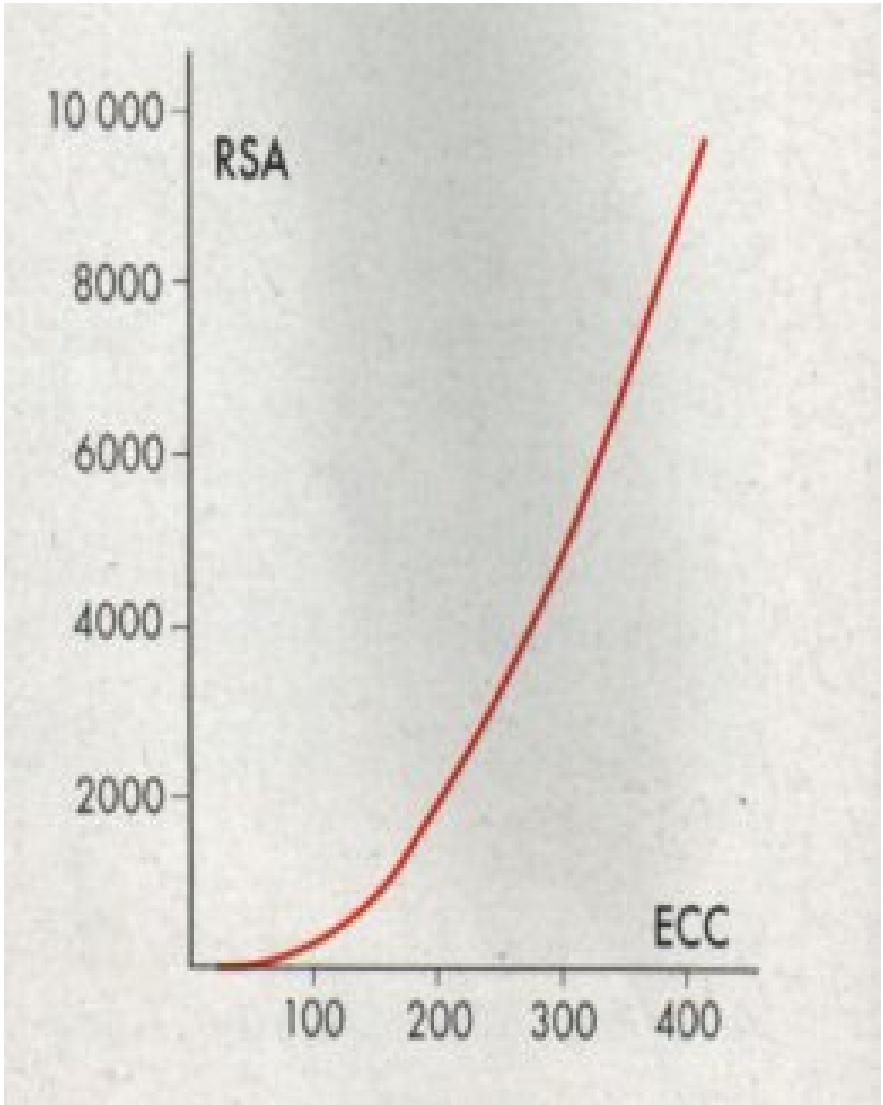
Der MOV Algorithmus

Der MOV-Algorithmus benutzt die Weil-Paarung, um die Berechnung diskreter Logarithmen in E(F) auf die (etwas einfachere) Berechnung diskreter Logarithmen in der multiplikatven Gruppe Fx zurückzuführen.

Reine anomale Kurven:

Eine “anomale” elliptische Kurve ist eine Kurve, für die die Anzahl der Punkte genau p ist.
Für anomale Kurven gibt es den SSSA-Algorithmus, der in subexponentieller Zeit entschlüsselt.

ECC vs. RSA Schlüssel



Curve25519

- wird durch die Funktion

$$y^2 = x^3 + 486662x^2 + x$$

  n einem endlichen Körper modulo der Primzahl

$$2^{255} - 19$$

  definiert
- wurde 2005 von dem Kryptographen Daniel J. Bernstein entwickelt
- handelt sich um eine sogenannte Montgomery-Kurve
- erlaubt die Verwendung von Algorithmen, die immun gegen Timing-Seitenkanalangriffe sind

secp256k1 bitcoin

Bitcoin verwendet kein RSA, sondern eine elliptische Kurve der Art

$$y^2 = x^3 + a * x + b \tag{10}$$

a und b sind fest, darüber hinaus gibt es einen Punkt G und eine Primzahl p, auf die man sich geeinigt hat (die Primzahl liegt in der Größenordnung von

$$2^256$$

).

- secp256k1 bietet ein Sicherheitsniveau von 128 Bits
- secp256k1 bietet das selbe Sicherheitsniveau wie RSA mit einer Schlüssellänge von 3072 Bits
- Die Wahrscheinlichkeit, dass man direkt die Adresse mit den 92000 BTCs generiert, liegt bei

  $$1/2^128$$

  Die Wahrscheinlichkeit im Lotto zu gewinnen liegt bei

  $$1/139838160$$

  , d.h. es ist wahrscheinlicher vier mal hintereinander im Lotto zu gewinnen,

Kurve Ed448-Goldilocks

- Während X25519 ungefähr 128-Bit-Sicherheit bietet, können wir dies mit Curve 448 verbessern, das ungefähr 224-Bit-Sicherheit implementiert und eine Primzahl von Folgendem verwendet:

$$2 - 2 - 1$$

- 2014 hat Mike Hamburg, Kryptoexperte am MIT, Goldilocks

$$(x2 + y21 - 39081x2y2mod2448 - 2224 - 1)$$

  beschrieben

Fazit: Mit Quantencomputern könnten alle elliptischen Kurven angegriffen werden, , je mehr Bit, desto länger müssen aber auch die rechnen

Wie sicher sind elliptische Kurven?

1. Beim Implementieren muss man äußerst sorgfältig vorgehen, um keine Fehler zu machen.
2. die Standard-Kurven der NIST oder bspw. auch des deutschen BSI sind anfällig gegen Seitenkanal-Angriffe auf der Basis von Timing- oder anderen Meta-Informationen
3.

Fazit Verschlüsselung auf Basis elliptischer Kurven ist nur dann sicher, wenn die verwendete Kurve sehr sorgfältig ausgesucht wurde.

Übersicht: ECC-Verfahren

- ECDH - Elliptic Curve Diffie-Hellman (Schlüsselaustausch)
- ECMQV - Elliptic Curve Menezes-Qu-Vanstone (Schlüsselaustausch)
- ECDSA - Elliptic Curve Digital Signature Algorithm (Signaturverfahren)
- EC-NR - Elliptic Curve Nyberg-Rueppel (Signaturverfahren)
- EC-KCDSA - Elliptic Curve Korean Certificate-based Digital Signature Algorithm (Signaturverfahren)
- ECGDSA - Elliptic Curve German Digital Signature Algorithm (Signaturverfahren)

Quellenverzeichnis

- https://www.secorvo.de/publikationen/elliptische-kurven-fox-2002.pdf
- https://ldapwiki.com/wiki/Elliptihttps://en.wikipedia.org/wiki/MQV c
- https://homepages.thm.de/ hg10013/Lehre/MMS/SS01$_W$S0102/*Elyps*/*index*.
//*www*.*heise*.*de*/*select*/*ix*/2017/3/1487529933065685
- http://2014.kes.info/archiv/heft/abonnent/04-3/04-3-052.htm
- https://eprint.iacr.org/2004/093.pdf
- https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/

Danke für Ihre Aufmerksamkeit

Fragen?