fhwedel
UNIVERSITY OF APPLIED SCIENCES

Seminararbeit Wahlbereich IT

SoSe 2018

Rechnen mit Punkten auf einer elliptischen Kurve und das „Elliptische Kurven Kryptosytem“ (ECC)

Erarbeitet von: Nino Sziedell (WIng101527)

im 7. Semester Wirtschaftsingenieurwesen

Betreuender Dozent: Prof. Dr. Michael Anders

Abgabe am: 24.06.2018

Gliederung

1. Einführung in das Thema

Wer kennt das Problem nicht: Man möchte einen Text oder eine kurze Nachricht an eine oder mehrere spezielle Personen schreiben, die von allen Außenstehenden aber nicht gelesen werden darf. Schon mit jungen Jahren gab es bei vielen Menschen erste Versuche dieses Problem auf verschiedenste Weisen zu lösen, so dass eine Art Geheimsprache entsteht.

Dabei gibt es zwei grundlegende Arten der Geheimsprache. Die Steganographie ist die eine, bei der eine Nachricht z.B. auf ein Blatt Papier geschrieben wird und im Anschluss dann so verdeckt wird, dass eine unbefugte Person nicht in der Lage ist, die Schrift zu erkennen. Ein Beispiel dafür ist die Zaubertinte, bei der mit einer unsichtbaren Farbe geschrieben wird, die dann nur durch eine bestimmte andere Farbe oder eine Art von Material zum Vorschein gelangt.

Die andere Art der Geheimschrift ist die Kryptologie, bei der die Nachricht tatsächlich zu sehen ist, der Sinn jedoch für einen Unwissenden nicht gegeben ist. Ein Beispiel hierfür ist ein Text, bei dem jeder Buchstabe durch den jeweils nächsten im Alphabet ersetzt wird. Die Kryptologie lässt sich wiederum noch in die Kryptographie, bei der es um die Entwicklung neuer Systeme und Verfahren geht, und die Kryptoanalyse, die für die Überwachung der implementierten Verfahren zuständig ist, unterteilen.

Im Folgenden wird die Kryptographie betrachtet, bei der es also darum geht, neue und möglichst sichere Verschlüsselungsverfahren zu entwickeln. Auch diese Verfahren lassen sich noch einmal in drei Gruppen einteilen.

Als Erstes gibt es die symmetrischen Verfahren. Dabei wird sowohl bei der Ver- als auch bei der Entschlüsselung nur ein einziger Schlüssel gebraucht, wie also z.B. die Information, dass jeder Buchstabe durch den jeweils nächsten im Alphabet ersetzt wurde. Dies ist zwar sehr einfach und kann innerhalb kurzer Zeit durchgeführt werden, beinhaltet aber ein sehr hohes Risiko. Der so wichtige Schlüssel muss durch einen sicheren Kanal ausgetauscht werden, ohne dass ein potentieller Angreifer diesen in die Hände bekommt. Dieser sichere Kanal ist heutzutage – mit Ausnahme des persönlichen Austausches – nur noch sehr schwer zu finden.

Des Weiteren gibt es die Gruppe der asymmetrischen Verschlüsselungsverfahren, bei dem jeder Teilnehmer für die Ver- und Entschlüsselung zusätzlich zu einem privaten Schlüssel, der geheim gehalten wird, auch noch einen öffentlichen Schlüssel besitzt, der ohne Probleme an die Öffentlichkeit gegeben werden kann. Diese Kombination hat sich seit einigen Jahren bewährt und wird in der heutigen Zeit sehr häufig als Verschlüsselung eingesetzt.

Die dritte und letzte Variante ist das hybride Verschlüsselungsverfahren, welches nichts anderes ist als eine Kombination aus dem symmetrischen und dem asymmetrischen Verfahren und dabei auch die Vorteile aus beiden Verschlüsselungsarten vereint. Der Ablauf ist dabei im Groben so, dass die zu schützenden Daten symmetrisch verschlüsselt werden und diese symmetrische Verschlüsselung dann noch einmal asymmetrisch verschlüsselt wird, also eine doppelte Sicherheit darstellt.

Nun sind die Grundlagen bekannt, um im weiteren Verlauf das „Elliptische Kurven Kryptosystem“ zu betrachten.

2. Einleitung

Das „Elliptische Kurven Kryptosystem“ – im Folgenden nur ECC genannt – gehört zur Gruppe der asymmetrischen Verschlüsselungsverfahren. Es wurde 1985 sowohl von Neal Koblitz (University of Washington) als auch von Victor S. Miller (IBM) unabhängig voneinander vorgeschlagen. Seitdem gewann das System immer mehr an Bedeutung bis es dann letztendlich 2005 auch von der NSA vorgeschlagen wurde und somit seit diesem Zeitpunkt mehr und mehr angewandt wird.

Wie der Name schon sagt, ist das ECC ein Kryptosystem. Das bedeutet, dass es nur in Verbindung mit anderen Verfahren zur Geltung kommen kann, da es kein eigenes Verschlüsselungsverfahren darstellt. In welche Verfahren dieses System hauptsächlich implementiert wird, wird später gezeigt (siehe Thema 8).

Der größte Unterschied zu anderen Kryptosystemen liegt darin, dass beim ECC nicht ausschließlich mit reellen Zahlen gerechnet werden. Stattdessen werden elliptische Kurven herangezogen, auf denen mit Punktoperationen gerechnet wird. Es werden also Punktadditionen und Punktmultiplikationen an Stelle der bekannten Operationen mit reellen Zahlen verwendet.

Auf den folgenden Seiten wird das ECC oft mit dem RSA und dem El-Gamal Kryptoverfahren verglichen. Beides sind ebenfalls beliebte asymmetrische Verfahren, bei denen mit reellen Zahlen gerechnet wird.

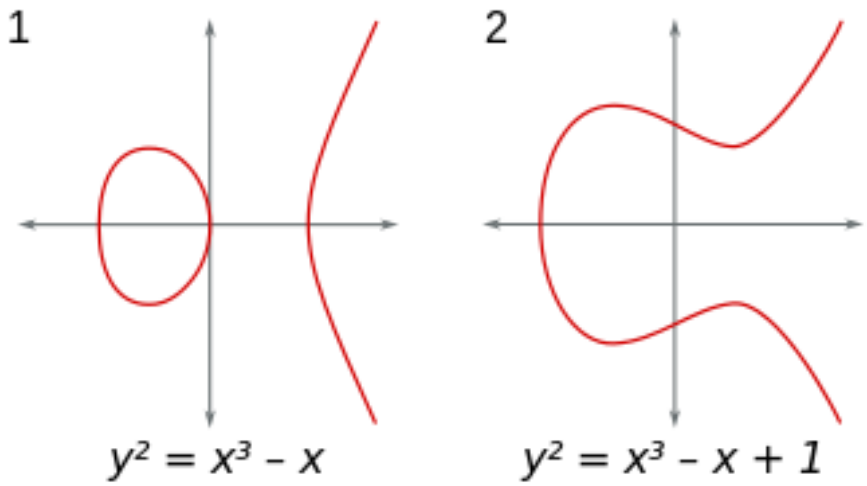
3. Elliptische Kurven

3.1 Definition

Um das Prinzip des ECC zu verstehen, ist es erst einmal wichtig zu wissen was elliptische Kurven überhaupt sind und wie sie aussehen. Und zwar sind dies Funktionen in einem Koordinatensystem mit x-Achse und y-Achse – also wie auch z.B. eine Parabel oder eine lineare Funktion aus der Mathematik. Jede elliptische Kurve ist eine Parabel, bei der immer die Gleichung $y^2 = x^3 + ax + b$ gilt.

Anhand des y^2 auf der linken Seite der Formel ist bereits zu erkennen, dass jede Kurve an der x-Achse gespiegelt ist. Denn egal welchen Zahlenwert man auf der rechten Seite erlangt, es wird am Ende immer noch einmal die Wurzel gezogen, wodurch zwei betragsmäßig gleiche Werte für y herauskommen. Einer davon ist dann positiv (über der x-Achse) und einer negativ (unter der x-Achse).

Durch das Einsetzen von Zahlenwerten für die Variablen a und b entstehen verschiedene elliptische Kurven. Auch wenn diese Werte kaum variieren, also z.B. der Wert b nur um 1 erhöht wird, ist schon ein großer Unterschied zu erkennen. Dies ist noch einmal anhand des folgenden Bildes zu sehen:



3.2 Merkmale

Elliptische Kurven können grundlegend über jeder Art von Körpern definiert werden. Für den Zusammenhang mit der Kryptographie werden jedoch nur Kurven über endlichen Körpern verwendet. Diese endlichen Körper besitzen zwei wichtige Eigenschaften, die hier etwas genauer betrachtet werden sollen.

Zum einen sind sie – wie der Name schon sagt – endlich. Die Anzahl an Werten ist also nicht unendlich groß, sondern ist definiert als Gruppe des Körpers. Während bei dem Rechnen mit reellen Zahlen diese Gruppe aus einer großen Anzahl an Zahlen besteht, enthält sie hier in unserem Fall die Anzahl der Punkte der definierten elliptischen Kurve inklusive eines Punktes U, der den Punkt der Unendlichkeit darstellt. Wieso dieser Punkt auch mit zur Gruppe gehört, wird in einem späteren Abschnitt erklärt.

Zum anderen gelten auf endlichen Körpern die gleichen Rechenregeln wie man das aus der Grundschule mit reellen Zahlen kennt. Diese Regeln möchte ich nun im Folgenden anhand von Punkten nochmals erläutern. P, Q und R sollen dabei Punkte auf der elliptischen Kurve sein, n ist eine reelle Zahl.

Kommutativ-Gesetz: $P+Q=Q+P$

Das Kommutativ-Gesetz besagt, dass egal ist ob man P zu Q dazu addiert oder Q zu P, beides ergibt am Ende den gleichen Punkt als Ergebnis.

Assoziativ-Gesetz: $(P+Q)+R=P+(Q+R)$

Bei einer Addition von mehreren Punkten ist es dank des Assoziativ-Gesetzes unerheblich, welche beiden Punkte man zuerst verrechnet, solange keine andere Rechenoperation dazwischen erfolgt.

Distributiv-Gesetz: $n\cdot(P+Q)=n\cdot P+n\cdot Q$

Das Distributiv-Gesetz – auch bekannt als „Ausklammern“ – besagt, dass wenn eine Zahl mit einer Punktaddition in einer Klammer multipliziert werden soll, genau so gut die Zahl mit den Punkten jeweils einzeln multipliziert werden kann und die Addition dann am Ende erfolgt.

Neben den bereits genannten Aspekten besitzen elliptische Kurven noch ein weiteres Merkmal, das vor allen Dingen für das Rechnen mit Punkten auf der Kurve (siehe Thema 6) sehr wichtig ist. Egal wie die Kurve aussieht (welche Werte also für a und b gewählt wurden), schneidet jede Gerade, die man in das Koordinatensystem hineinlegen könnte, genau drei Punkte der Kurve. Egal wie sehr man diese Gerade also verschiebt, es wird sich nie etwas daran ändern.

4. Prinzip

Da nun bekannt ist was eine elliptische Kurve ist und was sie ausmacht, können wir uns angucken, wie das System des ECC überhaupt funktioniert.

Wie bei den anderen Kryptosystemen der asymmetrischen Kryptographie geht es auch beim ECC darum, einen privaten Schlüssel mit einem Generator zu verknüpfen und daraus einen öffentlichen Schlüssel zu erhalten, der dann ohne Probleme an die Öffentlichkeit gelangen kann.

Sowohl bei dem Diffie-Hellman Schlüsselaustausch als auch bei El-Gamal und RSA wird die Formel $s = g^k \cdot mod\ p$ verwendet. Dabei ist g eine Zahl und gleichzeitig der Generator; das heißt ein öffentlicher Wert, der vor dem Prozess von allen Parteien festgelegt wird. Die Zahl p stellt das Primmodul dar. Was das genau ist und inwiefern es gebraucht wird, wird zu einem späteren Zeitpunkt vertieft (siehe Thema 5.1), für das eigentliche Prinzip ist es jedoch nicht entscheidend.

Die Werte k und s sind ebenfalls reelle Zahlen. k stellt dabei den privaten Schlüssel dar, den jeder Nutzer für sich selbst definiert und der niemals in irgendeiner Form an andere Personen weitergegeben werden darf. Durch die Potenzrechnung aus g und k entsteht dann s als Ergebnis – der öffentliche Schlüssel. Während also k komplett versteckt wird, kann s als Ergebnis ins Netz gestellt werden, ohne dass einer der Teilnehmer der Verschlüsselung schlimme Befürchtungen haben muss.

Man kann also festhalten, diese Art der asymmetrischen Kryptographie beinhaltet ausschließlich Zahlen, die miteinander verrechnet werden.

Wie bereits erwähnt gibt es beim System mit elliptischen Kurven die gleichen Elemente, jedoch in einer anderen Form. Anstatt der Potenzformel verwendet man hier die Formel

$$n \cdot P = Q$$

Diese Formel legt den Grundstein für das ECC und wird auf den kommenden Seiten noch das ein oder andere Mal vorkommen.

Wie bereits bekannt ist, wird hier nicht nur mit reellen Zahlen gerechnet, sondern vor allen Dingen mit Punkten im Koordinatensystem. Sowohl das P als auch das Q in der Formel stellen Punkte dar – genauer genommen Punkte der Gruppe des endlichen Körpers, also in der Regel auf der elliptischen Kurve.

P ist dabei der Generator-Punkt. Er wird also noch vor dem eigentlichen Verschlüsselungsvorgang festgelegt, direkt nachdem eine elliptische Kurve definiert wurde. Der Punkt Q auf der rechten Seite der Gleichung stellt den öffentlichen Schlüssel dar.

Das letzte Element der Formel, das jetzt somit noch fehlt, ist n. n ist im Gegensatz zu P und Q kein Punkt, sondern eine Zahl und gleichzeitig der private Schlüssel. Man kombiniert also auch hier wieder den privaten Schlüssel mit einem Generator um den öffentlichen Schlüssel zu errechnen.

Nun ist es aber so, dass der Punkt P nicht einfach mit Zahl n multipliziert werden kann und Q sofort feststeht, da diese Rechnung ja auf einer Kurve im Koordinatensystem stattfindet und nicht einfach z.B. mit Hilfe eines Taschenrechners errechnet werden kann. Dies wird so gehandhabt, dass die Multiplikation von n und P in mehrere Additionen und/oder Verdoppelungen aufgeteilt wird, da diese auch wirklich durchführbar sind.

Mal angenommen, als privater Schlüssel wurde n = 8 definiert. Daraus entsteht dann die Gleichung $8 \cdot P$, wobei die genauen Koordinaten von P hier keine Rolle spielen. Nun möchte man also diese $8 \cdot P$ in Additionen und Verdopplungen aufteilen und es ist schon relativ leicht zu erkennen, dass dies durch drei Verdopplungen möglich gemacht werden kann. Somit folgt also $2 \cdot (2 \cdot (2 \cdot P))$. In diesem Beispiel sind also keine Additionen notwendig, könnten aber genauso gut z.B. durch $2 \cdot P + P + P + P + P$ eingebaut werden. Egal wie die Formel letztendlich aufgeteilt wird, das Endergebnis ist immer das gleiche – der Punkt Q.

$$Q = 8 \cdot P = 2 \cdot (2 \cdot (2 \cdot P))$$

Als weiteres Beispiel betrachten wir $23 \cdot P$, hier wurde somit n = 23 als privater Schlüssel definiert. Natürlich wäre es hier auch möglich mit 23 aufeinanderfolgenden Additionen zu arbeiten, jedoch ist es aufwändiger je mehr Operationen durchgeführt werden müssen. Die einfachste Aufteilung ist eine Kombination aus mehreren Additionen und Verdopplungen.

$$Q = 23 \cdot P = 2 \cdot (2 \cdot (2 \cdot (2 \cdot P) + P) + P) + P$$

In der Realität werden sehr viel größere Zahlen als private Schlüssel verwendet, da es sonst zu einfach ist den privaten Schlüssel zu erraten. Das Prinzip bleibt aber natürlich das gleiche, auch wenn die Länge der Formel ein sehr hohes Ausmaß annimmt.

Wie genau es weiter geht, also wie überhaupt diese Verdopplungen und Additionen auf der elliptischen Kurve funktionieren, wird an anderer Stelle (siehe Thema 6) erklärt.

5. Diskreter-Logarithmus-Problem

5.1 Definition

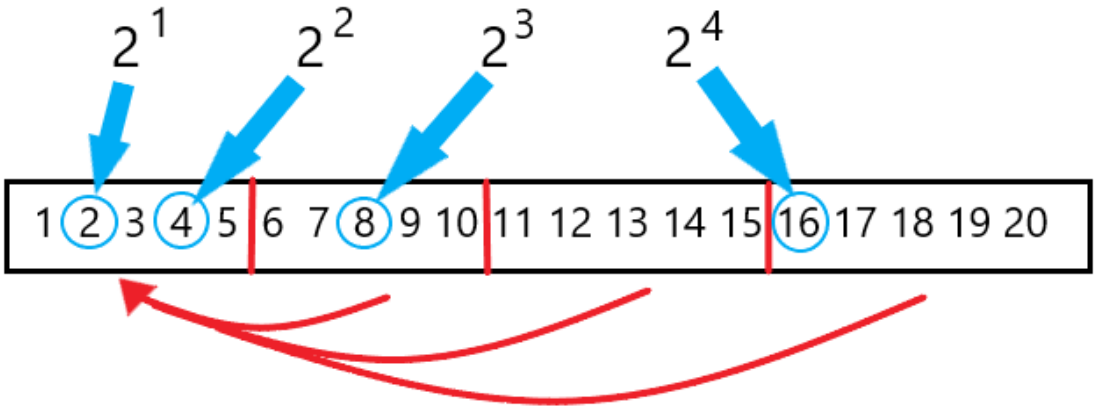
Bevor es weitergeht mit der graphischen Darstellung des Rechnens mit Punkten auf der Kurve, soll erst einmal auf einen Faktor der Sicherheit von asymmetrischen Kryptosystemen eingegangen werden, der vor allem bei dem ECC eine sehr große Rolle spielt.

Das sogenannte Diskreter-Logarithmus-Problem – kurz DLP – ist kein Problem für das System selbst, sondern für einen vermeintlichen Angreifer, der versucht das System zu umgehen. Der Name kommt ursprünglich wieder aus den anderen asymmetrisch verschlüsselten Systemen wie RSA und El-Gamal. Wie nun bekannt rechnen diese mit einer Potenzformel, bei der der private Schlüssel k im Exponenten steht. s und g sind öffentlich und damit bekannt. Da k somit der einzige Wert in der Rechnung ist, der geheim gehalten wird, muss er auch besonders geschützt werden und darf nie in die Hände anderer Personen kommen.

Möchte ein Angreifer nun also an diesen privaten Schlüssel kommen, müsste er den Logarithmus ziehen um die Formel so aufzulösen, dass die Lösung für k ermittelt werden kann. Dies ist im Grunde erstmal sehr einfach möglich, deswegen verwendet man in der Kryptographie einen Vorgang, der sich Modulbildung nennt.

Diese Modulbildung funktioniert so, dass die Werte für den öffentlichen Schlüssel – hier also s – nicht in der gewohnten Reihenfolge betrachtet werden, sondern immer nach einer bestimmten Anzahl p „abgeschnitten“ werden und über die anderen Werte gelegt werden.

Hier einmal ein Beispiel mit dem Generator g = 2 und p = 5:



Durch Modulbildung:

16	2	8	4

Vor der Modulbildung wäre es sehr einfach, den Exponenten durch Annäherung genau zu bestimmen. Hinterher lässt sich die Regelmäßigkeit deutlich schwerer erkennen.

Der Wert von p nennt sich Primmodul und wird auch im ECC verwendet. Er wird in jedem System von einer sehr hohen Primzahl dargestellt, um die Regelmäßigkeit für einen möglichen Angreifer so wenig erkennbar wie möglich zu machen. Bei RSA und El-Gamal findet man diesen Wert am Ende der Formel wieder als mod (Modul) p.

Vor allen Dingen mit Hilfe dieser Modulbildung macht man es einem Eindringling schwer bis unmöglich, an den so wertvollen privaten Schlüssel zu kommen. Dabei definiert man den privaten Schlüssel als diskreten Logarithmus. Je schwerer es also ist den diskreten Logarithmus zu ermitteln, desto sicherer ist das Kryptosystem.

5.2 Verbindung zu ECC

Da bei dem ECC ja mit der Formel $n \cdot P = Q$ gerechnet wird und n der private Schlüssel ist, sollte n auch möglichst schwer heraus zu finden sein. Man spricht hier davon, dass n der diskrete Logarithmus von Q zur Basis P ist.

Das DLP sagt hier also folgendes aus: Auf der einen Seite ist es einfach für einen Teilnehmer der Verschlüsselung, den öffentlichen Schlüssel mit Hilfe seines privaten Schlüssels und des Generator Punktes zu errechnen. Auf der anderen Seite ist es jedoch deutlich schwerer für einen Angreifer n zu erraten bzw. zu errechnen, selbst wenn P und Q bekannt sind.

Auch die Modulbildung wird im ECC übrigens verwendet. Es gibt zwar keine eindeutige Reihenfolge der Zahlen, aber die Sicherheit steigt trotzdem noch einmal deutlich an durch diese Methode.

6. Rechnen mit Punkten auf einer elliptischen Kurve

6.1 Graphisch

6.1.1 Addition

Mit dem Wissen des grundlegenden Prinzips des ECC fehlt jetzt nur noch das Verständnis des tatsächlichen Rechnens mit den Punkten auf der elliptischen Kurve.

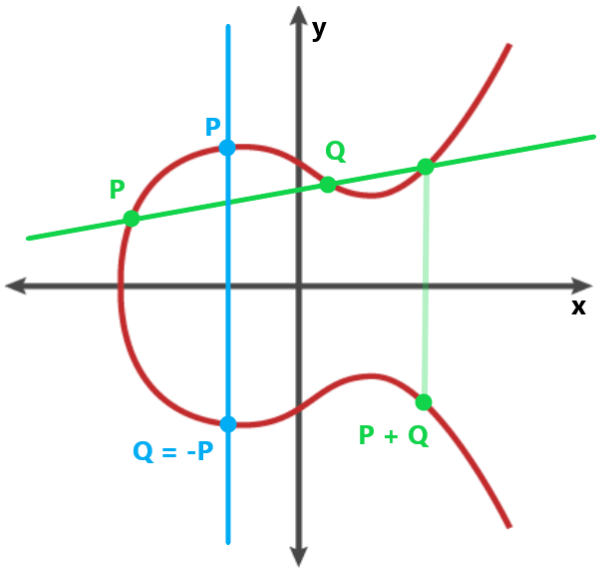
Angefangen mit der Addition von zwei Punkten P und Q. Sind also sowohl die Koordinaten der beiden Punkte als auch die zu verwendende Kurve bekannt, kann losgelegt werden. Als erstes werden die beiden Punkte im Koordinatensystem gekennzeichnet und es wird eine Gerade durch diese Punkte hindurch gezogen.

Wie ja bereits bekannt ist (siehe Thema 2) schneidet jede Gerade genau 3 Punkte der Kurve, sodass es neben den bereits bekannten Punkten P und Q noch einen dritten Punkt R gibt, der einen Schnittpunkt der Geraden mit der Kurve darstellt. Egal wo dieser Punkt R liegt, muss er nun an der x-Achse gespiegelt werden. Man bekommt einen Punkt -R, der gleichzeitig das Ergebnis aus der Addition von P und Q ist.

Möchte man also zwei Punkte miteinander addieren, sucht man den dritten Schnittpunkt mit der Kurve und spiegelt diesen an der x-Achse. Dies ist der Regelfall.

Es gibt auch noch einen Sonderfall, bei dem dieses Prinzip nicht angewandt werden kann. Dieser tritt ein, wenn P und Q die gleichen Punkte sind, nur dass sie an der x-Achse gespiegelt sind. Q ist also in diesem Fall -P. Wenn man nun eine Gerade durch diese beiden Punkte zieht, gibt es keinen dritten Schnittpunkt mit der elliptischen Kurve. Aus diesem Grund wird dann als Ergebnis der Punkt U (Punkt der Unendlichkeit) festgelegt. Dies ist auch der Grund wieso der Punkt U Teil der Gruppe des endlichen Körpers ist, über dem die Kurve definiert wurde.

Im Folgenden ist noch einmal sowohl der Regelfall (grün) als auch der Sonderfall (blau) in einer Grafik dargestellt:



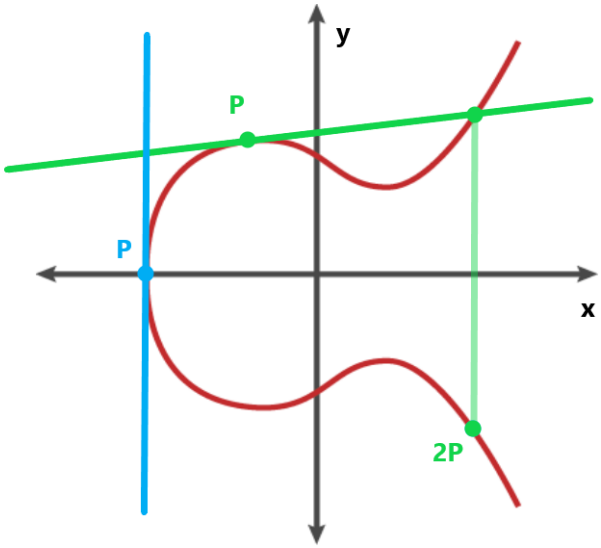
6.1.2 Verdopplung

Kommen wir nun zur Verdopplung eines Punktes P. Diese ist nichts anderes als eine Addition des Punktes P zu sich selbst, weshalb der Ablauf sehr ähnlich zu dem der Addition ist.

Der einzige Unterschied ist, dass natürlich keine Gerade durch zwei Punkte möglich ist, da nur ein Punkt bekannt ist. Stattdessen verwendet man hier die Tangente am Punkt P. Der Punkt P zählt dann als zwei Punkte, da man ihn zu sich selber addiert, und somit schneidet die Tangente wieder einen dritten Punkt der Kurve, den Punkt R. Dieser dritte Punkt wird dann wie üblich an der x-Achse gespiegelt und man bekommt das Ergebnis aus der Verdopplung des Punktes P.

Auch hier gibt es wieder einen Sonderfall. Dieser ist sehr ähnlich mit dem der Addition und tritt ein, wenn der Punkt P so liegt, dass seine Tangente genau senkrecht verläuft. Auch hier ist es so, dass dann das Ergebnis dieser Verdopplung der Punkt U definiert wird.

Hier dann auch einmal die grafische Übersicht des Regelfalls (grün) und des Sonderfalls (blau) bei der Verdopplung:



6.1.3 Beispiele

Nachdem nun alles Wichtige zum Rechnen mit Punkten auf einer elliptischen Kurve gesagt wurde, wird dies hier noch einmal anhand von zwei Beispielen verdeutlicht.

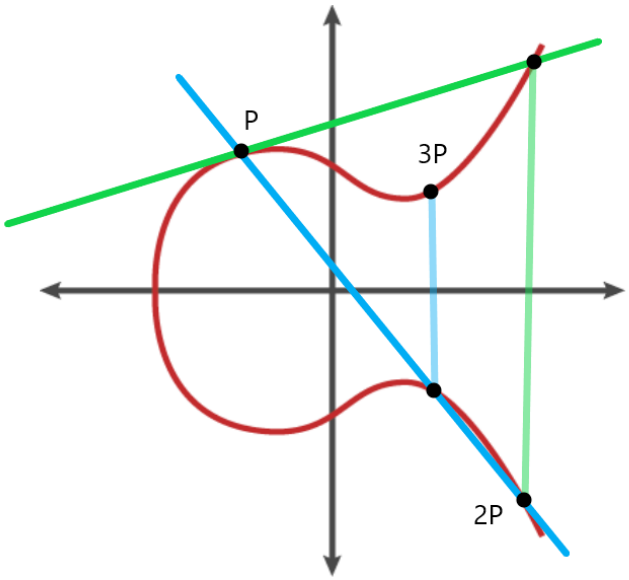
Im ersten Beispiel benutzen wir einen privaten Schlüssel n = 3, der öffentliche Schlüssel Q wird also folgendermaßen berechnet:

$Q = 3 \cdot P = 2 \cdot P + P$

Es fällt hier also eine Verdopplung und eine Addition an. Durch die Rechenregel „Punkt vor Strich“ wird mit der Verdopplung angefangen. Es wird also eine Tangente an den Punkt P gelegt und der dritte Schnittpunkt wird wie bekannt an der x-Achse gespiegelt.

Man bekommt den Punkt 2P. Da man diesen nun zu P dazu addieren möchte, legt man eine Gerade durch die Punkte 2P und P und bekommt natürlich wieder einen dritten Schnittpunkt. Spiegelt man diesen nun mit der x-Achse, bekommt man den Punkt 3P als endgültiges Ergebnis, dessen Koordinaten dann den öffentlichen Schlüssel darstellen.

Hier die dazugehörige Grafik:



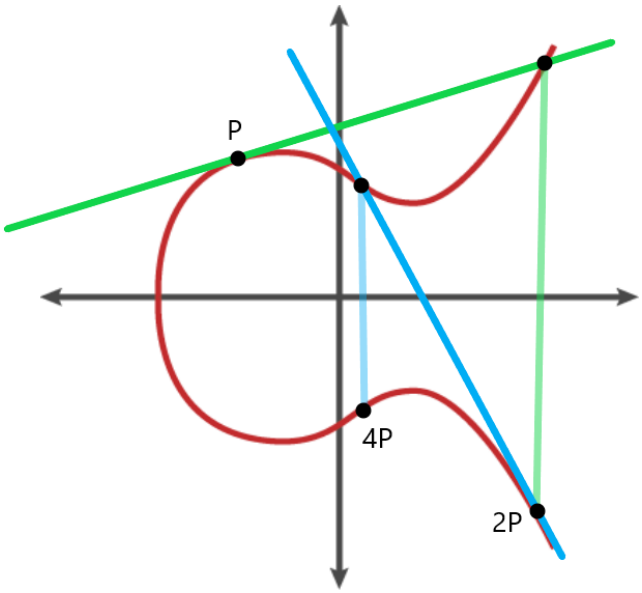
Im zweiten Beispiel benutzen wir den gleichen Punkt P wie zuvor und den privaten Schlüssel n = 4 und bekommen damit

$Q = 4 \cdot P = 2 \cdot (2 \cdot P)$

Hier wird der öffentliche Schlüssel somit über zwei Verdopplungen errechnet. Wie im vorangegangenen Beispiel wird hier zunächst eine Verdopplung von P ausgeführt. Man bekommt also wieder den Punkt 2P als Ergebnis.

Da dieser nun wieder verdoppelt werden soll, wird wieder eine Tangente an den Punkt 2P gelegt. Der dritte Schnittpunkt wird dann wie üblich an der x-Achse gespiegelt und man bekommt den Punkt 4P als öffentlichen Schlüssel.

Im Folgenden die grafische Darstellung:



Wie in den beiden Grafiken gut zu erkennen ist, liegen der Punkt 3P und der Punkt 4P nicht einmal im Ansatz beieinander, obwohl nur dieser Unterschied von 1 im privaten Schlüssel gegeben ist. Es lässt sich also keine Ordnung erkennen – 4P liegt ja beispielsweise zwischen P und 2P.

6.2 Rechnerisch

In der Realität ist die Art der graphischen Berechnung nicht wieder zu finden. Sie würde viel zu viel Zeit in Anspruch nehmen und wäre auch sonst viel zu umständlich. Die Computerprogramme heutzutage benutzen ausschließlich Formeln zur Codierung.

Alle Formeln lassen sich mit etwas Nachdenken aus der graphischen Darstellung ableiten, das Prinzip bleibt also genau das gleiche. Um nun die einzelnen Formeln zu verstehen, muss man sich noch einmal ein Paar Dinge klar machen.

Als Grundformel dient $P+Q=R$. Es werden also zwei Punkte addiert um einen dritten Punkt zu ermitteln. Bei dem Fall der Verdopplung gilt die gleiche Formel, nur dass P und Q

natürlich gleich sind. Aufgrund der Tatsache, dass hier mit Punkten gerechnet wird, hat jeder Punkt auch seine x- und seine y-Koordinate.

x_R → x-Koordinate des Punktes R

y_R → y-Koordinate des Punktes R

➔ Dementsprechend für die anderen Punkte

Es gelten folgende Gleichungen:

$x_R = s^2 - x_P - x_Q$

$y_R = s \cdot (x_P - x_R) - y_P$

Der Wert s ist die Steigung der beiden zu addierenden Punkte und wird folgendermaßen berechnet:

$s = \frac{x_Q - x_P}{y_Q - y_P}$

➔ Für normale Addition ($P \neq Q$¿

$s = \frac{3x^2 + a}{2y}$

➔ Für Verdopplung ($P = Q$¿

Der Faktor a ist der Wert aus der Formel für die elliptische Kurve und wird vor dem Verschlüsseln festgelegt, also zu dem Zeitpunkt wo eine bestimmte Kurve definiert wird.

7. Stärken & Schwächen

7.1 Stärken

Um das ECC beurteilen zu können, wird seine Sicherheit mit der der anderen asymmetrischen Kryptosysteme verglichen, bei denen mit reellen Zahlen gerechnet wird. Vor allen Dingen El-Gamal und RSA stellen echte Konkurrenten des ECC dar. Betrachtet werden dabei zuerst die Vorteile des ECC, die – schon einmal vorweggenommen – deutlich überwiegen.

7.1.1 Diskrete Logarithmen

Die erste große Stärke des ECC liegt in der unmöglichen Ermittlung der diskreten Logarithmen. Wie bereits in den Beispielen der Punktberechnung (siehe Thema 6.1.3) zu erkennen war, liegen die Punkte sehr verstreut auf der elliptischen Kurve. Es lässt sich also unmöglich ein Muster erkennen, in dem die Punkte angeordnet sind.

Im Gegensatz zu den Varianten mit reellen Zahlen, bei denen selbst bei Verwendung der Modulbildung noch eine gewisse Restordnung zu sehen ist, gibt es im System der elliptischen Kurven keine Möglichkeit irgendeine regelmäßige Anordnung der Punkte zu erkennen.

Die einzige Alternative, die es dann noch gibt ist das Raten. Wählt man jedoch eine elliptische Kurve, auf der genügend Punkte liegen, geht die Trefferquote dabei gegen 0 und ein korrekter Rateversuch ist so gut wie unmöglich.

Aus diesem Grund wird das ECC als sehr sicher angesehen. Außerdem ist vor allen Dingen bei höheren Sicherheitsniveaus die Verschlüsselungszeit sehr gering, wodurch die ganze Verschlüsselung sehr viel flexibler ablaufen kann.

Des Weiteren ist durch den komplett unregelmäßigen Verlauf der Punkte eine deutlich kürzere Schlüssellänge notwendig bei gleichem Sicherheitsniveau. Dies zeigt die folgende Tabelle besonders gut, bei der ein Vergleich der Schlüssellängen von ECC mit denen von RSA und Diffie-Hellman dargestellt wird:

Symmetrische Schlüssellänge (in bits)	RSA und Diffie-Hellman Schlüssellänge (in bits)	Elliptische-Kurven Schlüssellänge (in bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Tabelle: NIST empfohlene Schlüssellängen

7.1.2 Gruppenordnung

Nach dem ersten großen Vorteil der diskreten Logarithmen gibt es noch eine weitere Stärke des ECC. Diese hängt zusammen mit der Gruppenordnung q, also der Anzahl der Elemente in der Gruppe des verwendeten Körpers.

Bei dem Rechnen mit reellen Zahlen ist q immer definiert als $p-1$. p ist das Primmodul, also die Anzahl der Elemente, nach denen ein Modul abgeschnitten wird und über die anderen gelegt wird (siehe Thema 5.1). Da p immer eine Primzahl ist, also eine ungerade Zahl, ist q demnach immer gerade und somit niemals eine Primzahl.

Aus diesem Grund lässt sich die eigentliche Gruppenordnung durch Teilen in eine kleinere Untergruppe zerlegen. Diese Untergruppe beinhaltet dann nur noch eine höchstens halb so große Anzahl an Elementen und vereinfacht es einem potentiellen Angreifer damit den richtigen Wert heraus zu finden.

Im Falle des ECC ist q ja die Anzahl der Punkte auf der elliptischen Kurve mit einem zusätzlichen Punkt U. Diese hängt von der Art der Kurve ab und ist somit nicht von dem Primmodul abhängig. Man wählt dann einfach eine Kurve aus, bei der q ebenfalls eine Primzahl ist und somit keine Untergruppen möglich sind.

7.2 Schwachstellen

Wie in jedem System gibt es auch im ECC Schwachstellen. Jedoch hat man bis heute die anomalen Kurven und die supersingulären Kurven als einzige Schwächen erkannt. Beides sind eine besondere Art der elliptischen Kurve, auf die hier nicht weiter eingegangen werden soll.

Im Allgemeinen erleichtern beide Varianten die Erkennung der Regelmäßigkeit und lassen somit einen Angreifer deutlich einfacher in das System eindringen. Vor allen Dingen bei den anomalen Kurven gab es schon Fälle, bei denen Unbefugte an den privaten Schlüssel gekommen sind.

Im Großen und Ganzen sind diese Schwachstellen aber leicht zu umgehen. Bevor man eine elliptische Kurve für die Verschlüsselung definiert, sollte man sich darüber informieren, was supersinguläre und anomale Kurven sind und wie sie aussehen, um klar zu stellen, dass sie auf keinen Fall verwendet werden.

Ist dies geschehen, gibt es eigentlich keine Risiken mehr, da es die einzigen Schwachstellen sind, die bis zum heutigen Tage gefunden wurden.

8. Arten des ECC

Wie bereits in der Einleitung (siehe Thema 2) erläutert, ist das ECC nur ein Kryptosystem und kein eigenes Verfahren. Es funktioniert also nur in Kombination mit einer Reihe von bekannten Kryptoverfahren.

Die bekanntesten Verfahren, bei denen das ECC zugrunde liegt, sind die Folgenden:

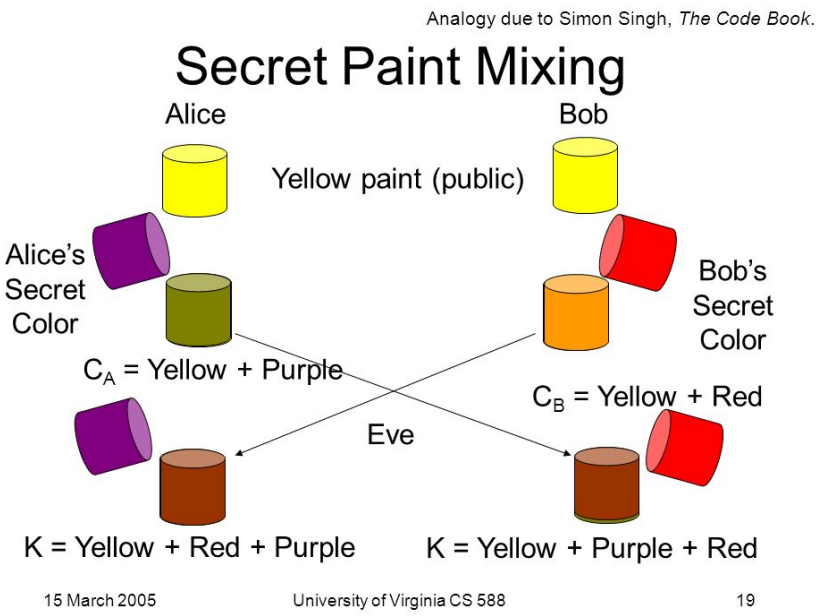
- Elliptic Curve Diffie-Hellman (ECDH)
  - Auf Grundlage des Diffie-Hellman Schlüsselaustausches
- Elliptic Curve El-Gamal (EC El-Gamal)
  - Auf Grundlage des El-Gamal Verschlüsselungsverfahrens
- Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Digitale Signatur
- Elliptic Curve Integrated Encryption Scheme (ECIES)
  - Hybrides Verschlüsselungsverfahren

Von diesen 4 Verfahren werden die ersten beiden – also ECDH und EC El-Gamal – hier einmal näher erläutert.

8.1 Elliptic Curve Diffie-Hellman (ECDH)

8.1.1 Diffie-Hellman Prinzip

Um den Diffie-Hellman Schlüsselaustausch zu verstehen, hier einmal das Prinzip anhand eines Beispiels des Farbmischens:



Erst einmal ist es wichtig zu wissen, dass in diesem Verfahren nur ein Austausch eines Schlüssels passiert und keine konkrete Nachricht verschlüsselt wird.

Nun stellen wir uns also zwei Personen, Alice und Bob, vor, die einen geheimen Schlüssel austauschen möchten. Dafür müssen insgesamt 5 Schritte durchlaufen werden:

Schritt 1: Gemeinsame Startfarbe definieren

Alice und Bob überlegen sich zuerst eine Farbe, die für beide und auch alle Außenstehenden bekannt ist. Dies ist hier Gelb.

Schritt 2: Persönliche Farbe definieren

Sowohl Alice als auch Bob überlegen sich jeweils für sich eine geheime Farbe, die sie an niemanden weitergeben und die von keiner anderen Person herausgefunden werden darf. In diesem Fall ist das Lila bei Alice und Rot bei Bob.

Schritt 3: Mischung der geheimen Farbe mit der Startfarbe

Alice nimmt ihr Lila und mischt es mit dem vorher definierten Gelb und bekommt Grün während Bob sein Rot mit dem Gelb mischt und Orange bekommt.

Schritt 4: Austausch der Farben

Sowohl das Lila als auch das Orange sind nun wieder öffentlich zugänglich und müssen nicht mehr verheimlicht werden. Beide Farben werden nun also an die jeweils andere Person übergeben.

Schritt 5: Gewinnen der fertigen Farbe

Alice benutzt das Orange von Bob, mischt es wiederum mit ihrem Lila und bekommt Braun als endgültige Farbe. Bob macht das Gleiche, indem er das Grün von Alice nimmt, dies mit seinem persönlichen Rot vermischt und ebenfalls Braun bekommt. Man sieht also, dass Alice und Bob erfolgreich eine Farbe ausgetauscht haben, die keiner anderen Person bekannt ist und somit sicher ist.

8.1.2 Anwendung auf elliptische Kurven

Genau mit dem gleichen Prinzip und mit dem gleichen 5 Schritten funktioniert das ECDH. Nur wird hier natürlich wie bekannt mit Punkten gerechnet anstatt Farben zu mischen.

Schritt 1: Elliptische Kurve und gemeinsamen Startpunkt definieren

Als Erstes muss die elliptische Kurve definiert werden, die in den nächsten Schritten verwendet werden soll. Dafür benutzt man heutzutage sehr häufig die Methode der Zufallskurven. Das bedeutet, dass die Faktoren a und b der Formel $y^2 = x^3 + ax + b$ solange per Zufall neu erzeugt werden bis die Kurve ausreichend sicher ist.

Woher weiß man nun also, ob die Kurve ausreichend sicher ist? Die Antworten auf diese Frage wurden mehr oder weniger bereits in vorherigen Kapiteln gegeben. Zum einen sollte man darauf achten, dass keine supersingulären oder anomalen Kurven verwendet werden (siehe Thema 7.2). Zum Anderen muss die Gruppenordnung eine Zahl sein, die ausreichend groß ist (i.d.R. höher als 2^{160}) und dazu noch eine Primzahl darstellt, um die Möglichkeit der Untergruppen zu vermeiden (siehe Thema 7.1.2).

Sobald also die elliptische Kurve eine hohe Sicherheit hat, muss nun noch ein gemeinsamer Startpunkt P definiert werden, der öffentlich bekannt ist.

Schritt 2: Privaten Schlüssel definieren

Nun geht es für Alice und Bob jeweils darum, eine Zahl zu bestimmen, die den privaten Schlüssel darstellt und geheim gehalten wird. Dies ist n_A für Alice und n_B für Bob.

Schritt 3: Berechnung des öffentlichen Schlüsselpunktes

Sowohl Alice als auch Bob benutzen jeweils ihren eigenen, privaten Schlüssel und multiplizieren diesen mit dem Punkt P um den jeweiligen öffentlichen Schlüsselpunkt zu erhalten. Wie das funktioniert, ist ja mittlerweile bekannt. Es gilt dann also $Q_A = n_A \cdot P$ für Alice und $Q_B = n_B \cdot P$ für Bob.

Schritt 4: Austausch der öffentlichen Schlüsselpunkte

Beide tauschen ihre öffentlichen Schlüsselpunkte aus bzw. machen diese im Internet öffentlich. Dadurch erhält Alice Q_B von Bob und Bob erhält Q_A von Alice.

Schritt 5: Gewinnen des gemeinsamen Schlüsselpunktes

Als letzten Schritt benutzt Alice den öffentlichen Schlüsselpunkt von Bob und verrechnet diesen mit ihrem privaten Schlüssel, um den gemeinsamen, geheimen Schlüsselpunkt R zu erhalten. Bob macht das genau Gegenteilige, er benutzt den öffentlichen Schlüsselpunkt von Alice und multipliziert diesen mit seinem privaten Schlüssel. Er erhält ebenfalls R, da gilt:

$$R = n_A \cdot Q_B = n_B \cdot Q_A = n_A \cdot n_B \cdot P$$

Wie also gut zu erkennen ist, rechnen beide mit der selben Formel, nur in umgekehrter Reihenfolge. Diese Formel enthält dabei jeweils einen privaten Schlüssel von Alice und Bob und damit sind sie die einzigen Personen, die diesen gemeinsamen Schlüsselpunkt R kennen. Da R ja nur ein Schlüsselpunkt ist, muss noch der eigentliche Schlüssel daraus ermittelt

werden. Dies geschieht normalerweise ganz einfach durch das Ablesen der x-Koordinate des Punktes R.

Dadurch, dass sowohl bei der Berechnung des öffentlichen Schlüsselpunktes als auch bei der Berechnung des gemeinsamen Endpunktes diskrete Logarithmen enthalten sind, und zusätzlich die Gruppenordnung noch eine Primzahl ist, kann man dieses System als sehr sicher bezeichnen.

8.2 Elliptic Curve El-Gamal

Da hier das Gleiche wie bei dem ECDH passiert, nur mit einer zeitlichen Versetzung, sparen wir uns hier die Erläuterung des Prinzips und gehen direkt in das Rechnen mit dem ECC über.

Das EC El-Gamal ist im Gegensatz zu dem Elliptic Curve Diffie-Hellman ein Verschlüsselungsverfahren, bei dem tatsächlich auch eine Nachricht verschlüsselt wird. Es gibt ganze 8 Schritte.

Schritt 1: Elliptische Kurve und Startpunkt definieren

Es wird genau gleich vorgegangen wie im ECDH, außer dass hier nur Alice allein die elliptische Kurve und den Punkt bestimmt, da Bob erst später dazu stößt.

Schritt 2: Alice bestimmt ihren privaten Schlüssel

Alice denkt sich eine Zahl als privaten Schlüssel (n_A) aus. Normalerweise wird solch ein privater Schlüssel nur einmalig also für einen Durchlauf benutzt. Hier ist der Schlüssel von Alice jedoch permanent, d.h. er kann für beliebig viele Verschlüsselungen verwendet werden.

Schritt 3: Veröffentlichung des öffentlichen Schlüsselpunktes

Alice benutzt ihren privaten Schlüssel n_A, multipliziert diesen mit dem Startpunkt P und bekommt ihren öffentlichen Schlüsselpunkt Q_A. Diesen permanenten Schlüsselpunkt veröffentlicht sie dann im Internet, sodass beliebig viele Leute ihn benutzen und weiterverwenden können.

Schritt 4: Bob bestimmt seinen privaten Schlüssel

Nun kommt also Bob ins Spiel. Er möchte Alice eine Nachricht zukommen lassen und definiert sich dafür erst einmal seinen eigenen privaten Schlüssel n_B, der einmalig existiert.

Schritt 5: Bob berechnet seinen öffentlichen Schlüsselpunkt und den Schlüsselpunkt R

Mithilfe seines eigenen Schlüssels n_B und des Punktes P berechnet sich Bob seinen öffentlichen Schlüsselpunkt Q_B. Außerdem verwendet er den veröffentlichen Schlüsselpunkt von Alice, verrechnet diesen auch mit seinem privaten Schlüssel n_B und bekommt R als Ergebnis. Aus R gewinnt er dann den Schlüssel, mit dem er seine Nachricht verschlüsseln möchte.

Schritt 6: Verfassen und Verschlüsseln einer Nachricht

Bob verfasst nun also seine Nachricht, die er Alice zukommen lassen möchte. Diesen Text verschlüsselt er anschließend mit dem Schlüssel, den er aus R gewonnen hat.

Schritt 7: Verschicken der verschlüsselten Nachricht

Bob sendet eine Mitteilung mit der verschlüsselten Nachricht und seinem öffentlichen Schlüsselpunkt Q_B an Alice.

Schritt 8: Entschlüsseln der Nachricht

Alice erhält die Mitteilung von Bob und möchte diese nun entschlüsseln. Dies erreicht sie, indem sie ihren privaten Schlüssel n_A mit dem gerade erhaltenen öffentlichen Schlüsselpunkt Q_B von Bob multipliziert und damit R erhält, aus welchem dann der Schlüssel zum Entschlüsseln gewonnen werden kann.

Da hier genau die gleichen Formeln gelten wie bei dem ECDH, gilt die Sicherheit des Verfahrens im gleichen Sinne.

9. Anwendung

Das ECC wird aufgrund seiner geringen Schlüssellänge vor allen Dingen bei Medien mit geringer Rechen- oder Speicherkapazität (z.B. Smartcards) verwendet.

Außerdem findet es Anwendung in vielen wichtigen Systemen. Angefangen mit dem Messenger-Dienst WhatsApp, an dem inzwischen kaum noch ein Weg vorbeiführt. Dort werden die Ende-zu-Ende Verschlüsselungen der Chats genau mit diesem Kryptosystem gesichert.

Zwei weitere Beispiele sind die kryptographischen Protokolle in den neueren Betriebssystemen von Windows und der Zugriff auf den Chip des neuen Personalausweises. Auch hier wird das ECC verwendet, was zeigt welch hohen Stellenwert dieses System in der heutigen Zeit hat.

10. Literaturverzeichnis

(1) Elliptic Curve Cryptography – An implementation tutorial

http://www.infosecwriters.com/text_resources/pdf/Elliptic_Curve_AnnopMS.pdf

(2) Koblitz, N. – Elliptic Curve Cryptosystems – 1987

https://pdfs.semanticscholar.org/c7c5/47ede2da32aba645edb11e33f1d32af735e2.pdf

(3) Jonas, T. – Elliptische-Kurven-Kryptographie, 2016, e-follows.net stipendiat wissen, Band 2059

(4) Wagnon, J. – Elliptic Curve Cryptography Overview – 2015

https://www.youtube.com/watch?v=dCvB-mhkT0w

(5) Sullivan, N. – A (relatively easy to understand) primer on elliptic curve cryptography – 2013

https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

(6) Hainz, C. – Kryptographie und elliptische Kurven – 2001

https://homepages.thm.de/~hg10013/Lehre/MMS/SS01_WS0102/Elyps/

(7) Anders, M. – Kryptographie mit elliptischen Kurven (ECC) – 2015

https://www.youtube.com/watch?v=N1WBehM9rPk

(8) Anders, M. – Diffie-Hellman Schlüsselaustausch mit ECC Algebra – 2015

https://www.youtube.com/watch?v=aC05R9xqbgE&t=1466s

(9) Rouse, M. – Elliptische-Kurven-Kryptographie (Elliptic Curve Cryptography, ECC)

https://www.searchsecurity.de/definition/Elliptische-Kurven-Kryptografie-Elliptic-Curve-Cryptography-ECC

Der letzte Zugriff der URLs erfolgte am 23.06.2018.