Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatikstrategieorgan Bund ISB
Informatiksicherheit SEC

Rolf Oppliger

22.6.2020

Technologiebetrachtung

Elliptische Kurven

1 Einführung

Die asymmetrische Kryptografie auf der Basis von elliptischen Kurven wird häufig eingesetzt, um z.B. die Elgamal-Verschlüsselung, die Signierung gemäss dem Digital Signature Algorithm (DSA) oder den Diffie-Hellman Schlüsselaustausch zu verbessern. Dabei stellt sich die Frage, welche elliptischen Kurven man hierfür einsetzen soll. In den «IKT-Sicherheitsempfehlungen für den Grundschutz V1.2- Kryptografische Verfahren: Algorithmen und Protokolle» [1] werden diesbezüglich die Kurven M-221, E-222, Curve1174, Curve25519, E-382, M-383, Curve383187, Curve41417, Ed448-Goldilocks, M-511 und E-521 oder eine Brainpool-Kurve mit einer Schlüssellänge von mindestens 224 Bit vorgeschlagen.

In dieser Technologiebetrachtung wird erläutert, weshalb die Kurvenwahl aus sicherheitstechnischer Sicht relevant ist, und welche Überlegungen zu diesen Empfehlungen geführt haben. Insofern ist dieses Dokument als Vertiefung von [1] zu verstehen. Es setzt mathematische Grundkenntnisse über Gruppen voraus.

2 Kryptografische Grundlagen

Viele asymmetrische Kryptosysteme basieren auf dem diskreten Logarithmusproblem (DLP) in einer zyklischen Gruppe G. «Zyklisch» bedeutet hier, dass es ein Element g (Generator) gibt, welches die Gruppe erzeugt, d.h. für jedes Element h aus G gibt es eine natürliche Zahl $n \in \mathbf{N}$, so dass $h = g^n$ gilt. Das DLP besteht nun darin, für ein beliebiges Element h aus der Gruppe ein $n \in \mathbf{N}$ mit $g^n = h$ zu finden. Im einfachsten Fall handelt es sich bei der Gruppe G um die multiplikative Gruppe eines Primkörpers, also um $\mathbf{Z}_p^*$ für Primzahl p. Hier gibt es genau die Elemente 1,…,p-1. Das DLP besteht darin, für ein solches Element h eine natürliche Zahl n zu suchen, so dass $h = g^n \bmod p$ gilt.

Für die Lösung des DLP gibt es für eine generische zyklische Gruppe nur Algorithmen, die bezogen auf die Eingabelänge eine exponentielle Laufzeit[1] haben und damit im Sinne der Komplexitätstheorie ineffizient sind. Konkret ist die Laufzeit dieser Algorithmen proportional zur Quadratwurzel der Anzahl Gruppenelemente, d.h. wenn eine Gruppe z.B. 2^{256} Elemente hat, dann ist die Laufzeit eines solchen Algorithmus von der Grössenordnung $2^{256/2} = 2^{128}$. Wenn die zyklische Gruppe allerdings spezielle Eigenschaften aufweist, gibt es manchmal effizientere Algorithmen zur Lösung des DLP. Die multiplikative Gruppe $\mathbf{Z}_p^*$ ist eine solche

[1] Die Laufzeit ist exponentiell, wenn sie sich für ein konstantes c wie $c^{\log n}$ verhält, wobei n für die Eingabe und log n für deren Länge steht.

Gruppe, und die Algorithmen zur Lösung des DLP haben für diese Gruppe eine subexponentielle Laufzeit[2]. Aufgrund dieser Tatsache benötigt man in $\mathbf{Z}_p^*$ Schlüssel von mehreren Tausend Bit Länge, obwohl – wie oben erwähnt - im allgemeinen Fall 256 Bit ausreichen müssten, um ein Sicherheitsniveau von 2^{128} zu erreichen.

Vor diesem Hintergrund ist es sinnvoll, als zyklische Gruppe nicht die multiplikative Gruppe $\mathbf{Z}_p^*$ zu verwenden, sondern eine Gruppe, in der nur exponentielle Algorithmen zur Lösung des DLP bekannt sind. Der DSA verwendet dazu z.B. eine Untergruppe der multiplikativen Gruppe $\mathbf{Z}_p^*$. Eine andere, in den späten 1980er-Jahren vorgeschlagene Möglichkeit besteht in Punktegruppen auf elliptischen Kurven über einem endlichen Körper **K**. Die Elemente dieser Gruppe bestehen aus den Punkten (x,y) aus $\mathbf{K^2}$, die meist als Kurvengleichung der Form $y^2 = x^3 + ax + b$ mit $a,b \in \mathbf{K}$ und $4a^3 + 27b^2 \neq 0$ beschrieben werden, zusammen mit dem neutralen Element *O* der dazugehörigen Gruppenoperation. Diese Operation kann grafisch gedeutet und algebraisch definiert werden. In beiden Fällen beschreibt sie die Addition (+) von zwei Elementen (Punkten) P und Q der Gruppe (P+Q) bzw. eines Punktes P mit sich selbst (2·P). Natürlich kann ein Punkt auch mehrfach mit sich addiert und entsprechend n·P für ein $n \in \mathbf{N}$ gebildet werden. Alle Kurvenpunkte zusammen mit dem neutralen Element *O* und der so definierten Addition bilden zusammen eine zyklische Gruppe, in der wiederum ein Element (Punkt) als Generator G festgelegt wird. Auch hier gilt, dass i·G für i = 1,…,n alle Gruppenelemente erzeugt, wobei n die Ordnung der Gruppe ist (diese Ordnung entspricht in etwa der Ordnung des Körpers **K**).

Eine so definierte elliptische Kurve über **K** wird als *E*(**K**) bezeichnet. Sie umfasst die Kurvenpunkte und das neutrale Element *O* als Elemente, sowie die Addition als Gruppenoperation. In *E*(**K**) kann ein Elliptisches-Kurven-DLP (ECDLP) folgendermassen definiert werden: Gegeben sind *E*(**K**), ein Generator G und ein weiterer Kurvenpunkt $H \in E(\mathbf{K})$. Wie oft muss nun G zu sich selbst addiert werden, so dass H resultiert, d.h. man sucht die natürliche Zahl n, so dass H = n·G gilt. Für die Lösung dieses Problems gibt es bis heute für eine generische Kurve nur Algorithmen, die eine exponentielle Laufzeit haben. Wenn aber die Algorithmen zur Lösung des ECDLP ineffizient sind, bedeutet das im Umkehrschluss, dass man mit kürzeren Schlüsseln arbeiten kann. In der Tat kann man im Bereich der Kryptografie auf der Basis von elliptischen Kurven mit Schlüsseln der Länge 256 arbeiten und trotzdem ein gewünschtes Sicherheitsniveau von 2^{128} erreichen.

3 Standardisierung

Will man die Kryptografie auf der Basis von elliptischen Kurven nutzen, muss man zunächst einmal eine zyklische Gruppe festlegen. Konkret heisst das, dass man **K**, a, b und G so festlegen muss, dass eine hinreichend starke Gruppe resultiert, d.h. eine Gruppe, in der keine Algorithmen bekannt sind, die eine praktikable Laufzeit haben. Weil das nicht ganz einfach ist, bietet sich eine Standardisierung an und verschiedene Organisation haben sich dieser Aufgabe angenommen.

Zunächst einmal hat das U.S. amerikanische National Institute of Standards and Technology (NIST) Kurven für die elliptische-Kurven-Variante des DSA, d.h. den Elliptic Curve DSA (ECDSA), 15 Kurven vorgeschlagen, von denen sich in der Praxis vor allem die Kurven über Primkörpern und dabei vor allem die Kurve P-256 durchgesetzt haben. Die NIST-Kurven sind teilweise im Rahmen von ISO/IEC 1488831, IEEE 1363-2000 und ANSI X9.62 übernommen worden. Die Standards for Efficient Cryptography Group (SECG) ist ein industrielles Konsortium, das ähnliche Kurven festgelegt hat, wobei die beiden Kurven secp256k1 und

[2] Die Laufzeit ist subexponentiell, wenn sie zwar besser als exponentiell aber immer noch nicht polynomial (effizient) ist.

secp256r1 in etwa P-256 entsprechen. Die Kurve secp256k1 hat insbesondere aufgrund ihres Einsatzes für Signaturen im Rahmen von Bitcoin grosse praktische Relevanz erreicht.

Unter dem Strich gibt es heute viele Standards, die für den Einsatz der Kryptografie auf der Basis von elliptischen Kurven eingesetzt werden können. Allerdings basieren sie alle mehr oder weniger stark auf den Vorarbeiten des NIST. Eine diesbezügliche Ausnahme stellen die Kurven dar, die 2005 von einer Arbeitsgruppe namens Brainpool unter der Leitung des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) erarbeitet und spezifiziert worden sind. Die entsprechenden Brainpool-Kurven sind in vielen Standards der IETF übernommen und erfreuen sich insbesondere im Bereich der Internet-Sicherheitsprotokolle grosser Beliebtheit (entsprechend ist ihr Einsatz in vielen RFCs vorgesehen).

4 Hintertüren

Aufgrund der Tatsache, dass man für den Einsatz der Kryptografie auf der Basis von elliptischen Kurven wie oben erwähnt viele Parameter festlegen und bis zu einem gewissen Punkt auch standardisieren muss, hat es schon immer die Befürchtung gegeben, dass derartige Standards auch Hintertüren enthalten können. 2007 wurde erstmals gezeigt, dass ein vom NIST standardisierter und ebenfalls auf elliptischen Kurven basierender Pseudozufallsgenerator namens Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) eine Hintertür enthalten kann. Die Möglichkeit besteht, weil im Standard zwei Kurvenpunkte P und Q vorgesehen sind, dabei aber nicht klar ist, ob diese Punkte zufällig gewählt oder gemäss $Q = d \cdot P$ konstruiert sind. Im zweiten Fall lässt sich aus der Kenntnis von d eine Hintertür konstruieren, mit der der Pseudozufallsgenerator grundsätzlich kompromittierbar d.h. vorhersehbar wird. Leider sind die beiden Fälle a priori nicht unterscheidbar, d.h. es ist nicht klar, ob die Hintertür absichtlich oder versehentlich ermöglicht worden ist. Aufgrund der Enthüllungen von Edward Snowden nimmt man ersteres an, d.h. man geht von einer absichtlich im Standard platzierten Hintertür aus. Das eigentliche Problem, das die Platzierung der Hintertür erst ermöglicht hat, ist die nicht offengelegten Entwurfsprinzipien für die Konstruktion des Dual_EC_DRBG Pseudozufallsgenerators.

Seit dem Dual_EC_DRBG-Vorfall ist die internationale Gemeinschaft der in der Kryptografie Forschenden sehr skeptisch gegenüber Standards, die von staatlichen Behörden und namentlich dem NIST vorgeschlagen worden sind bzw. vorgeschlagen werden. In der Tat ist ein Projekt namens SafeCurves (https://safecurves.cr.yp.to) gestartet worden, im Rahmen dessen aktuell eingesetzte Kurven im Hinblick auf ihre kryptografische Stärke untersucht und neue Kurven vorgeschlagen werden. Dabei ist die Transparenz der Entwurfsprinzipien entscheidend. Die wichtigsten Vorschläge neuer Kurven sind Curve25519, Ed448-Goldilocks und E-521. Insbesondere Curve25519 wird in vielen End-zu-End verschlüsselnden Messengers, wie z.B. Signal (bzw. WhatsApp) und Threema, sowie TLS 1.3-Implementationen eingesetzt.

5 Schlussfolgerungen und Empfehlungen

Aufgrund dieser Ausgangslage wird in [1] empfohlen, in der Praxis entweder die im Rahmen des SafeCurves-Projektes als sicher eingestuften Kurven (siehe oben) oder die Brainpool-Kurven ab einer gewissen Stärke zu verwenden. Nicht empfohlen sind dementsprechend sowohl selbst konstruierte Kurven als auch die Vorschläge des NIST und davon abgeleitete Kurven.

Referenzen

[1] FUB ZEO KRYPT, IKT-Sicherheitsempfehlungen für den Grundschutz V1.2- Kryptografische Verfahren: Algorithmen und Protokolle, 13.12.2019

Abkürzungen

ANSI	American National Standards Institute
BSI	Bundesamt für Sicherheit in der Informationstechnik
DLP	diskretes Logarithmusproblem
DSA	Digital Signature Algorithm
ECDLP	Elliptic Curve DLP
ECDSA	Elliptic Curve Digital Signature Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISB	Informatiksteuerungsorgan Bund
NIST	National Institute of Standards and Technology
RFC	Request for Comments