

K26: El Gamal für elliptische Kurven, ECDSA

Stichworte: El Gamal für elliptische Kurven mit Beispiel,
ECDSA: elektronische Unterschriften mit elliptischen Kurven

26.1. Einführung: Wir behandeln das El Gamal-Verfahren bei Verwendung elliptischer Kurven-Gruppen, speziell das ECDSA-Verfahren.

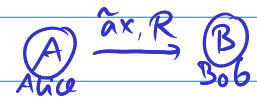
26.2. Erinnerung an das allgemeine El Gamal-Verschlüsselungsverfahren für eine beliebige abelsche Gruppe G aus K5.3:
Alice möchte eine geheime Botschaft $m \in G$ an Bob schicken.

26.3. Das Verfahren geht wie folgt:

Schritt (1.) Alice wählt eine Zufallszahl $\tilde{a} \in \{1, \dots, r-1\}$ und berechnet $\tilde{a} \cdot x$.

Alice besorgt sich Bobs öffentlichen Schlüssel b_x und berechnet $R = \tilde{a} \cdot (b_x) + m$.

Schritt (2.) Alice sendet $\tilde{a}x$ und R an Bob.



Schritt (3.) Bob berechnet $b \cdot (\tilde{a}x) = \tilde{a} \cdot (bx)$ und die Nachricht durch $R - b \cdot (\tilde{a}x) = m$.

26.4. Ist nun G die abelsche Gruppe einer kryptographisch geeigneten elliptischen Kurve, kann dieses Verfahren als sicher angesehen werden.
Eine Umsetzung ist wie folgt möglich:

1. Man wählt eine kryptographisch geeignete elliptische Kurve $E(\mathbb{F}_p): y^2 = x^3 + ax + b$, d.h. eine Primzahl p und natürliche Zahlen $0 \leq a, b < p$ (und prüft die Sicherheit gemäß K25, so dass das DL-Problem schwer ist), sowie ein $P \in E(\mathbb{F}_p)$ mit großer Ordnung als Basispunkt.
2. Ⓐ und Ⓑ einigen sich, wie man Klartext¹ als einen Punkt auf der elliptischen Kurve kodiert und wieder zurückerhält (etwa wie in K23 beschrieben).
3. Jeder Teilnehmer wählt eine Zahl $k \in \mathbb{N}$ als privaten Schlüssel und gibt $Q = kP \in E(\mathbb{F}_p)$ als öffentlichen Schlüssel bekannt:
 - Ⓐ Alice: $a \in \mathbb{N}$ (geheim) und $a \cdot P$ (öffentlich),
 - Ⓑ Bob: $b \in \mathbb{N}$ (geheim) und $b \cdot P$ (öffentlich).
 Danach kann das ElGamal-Verfahren wie oben beschrieben durchgeführt werden.

- 26.5. Bsp.: Man lege das Alphabet $\Sigma = \{A, B, \dots, Z\}$ zugrunde und nehme die elliptische Kurve $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$ (in der Rolle von $x \in \mathbb{G}$) mit $p = 6833$, $A = 5984$, $B = 1180$ und den Basispunkt $P = (1, 2631)$.
- Teilnehmer Ⓑ Bob wählt den geheimen Schlüssel $b = 2465 \in \mathbb{N}$ und macht $Q = 2465 \cdot P = (4748, 2021)$ öffentlich.
 - Teilnehmerin Ⓐ Alice schickt den geheimen Text "INSTITUT" etwa in der folgenden Form (Streckungsfaktor 10, $\tilde{a} = \text{Zufallszahl}$) an Bob:

Text	IN	ST	IT	UT
w	$(8, 13)_{(16)} = 221 \rightarrow 2210$	$(18, 19)_{(26)} = 487 \rightarrow 4870$	$(8, 19)_{(26)} = 227 \rightarrow 2270$	$(20, 19)_{(26)} = 539 \rightarrow 5390$
M_w	$(2211, 556)$	$(4872, 3315)$	$(2270, 2994)$	$(5392, 959)$
\tilde{a}	6794	3035	3508	2765
$\tilde{a}P$	$(687, 171)$ }	$(1211, 2731)$ }	$(2714, 2389)$ }	$(6818, 2527)$ }
$\tilde{a}Q + M_w$	$(3327, 5675)$ }	$(2260, 17)$ }	$(357, 1247)$ }	$(1333, 6617)$ }

Die Folge der Punktepaare $(\tilde{a}P, \tilde{a}Q + M_w)$ wird von Alice an Bob verschickt.
 Bob entschlüsselt mit $\tilde{a}Q + M_w - b \cdot \tilde{a}P = M_w$, da $Q = bP$,
 die x-Koordinate x von $M_w \in E(\mathbb{F}_p)$ ergibt dann mit $\lfloor \frac{x}{\lambda_0} \rfloor = w$ den Text block.

ECDSA - Signaturen

26.6. ECDSA ist das DSA-Verfahren (elektronische Unterschrift) auf elliptischen Kurven.
 Alice möchte dabei ein Dokument $m \in M$ an Bob schicken und signieren.

26.7. Schritt 1.: Zuerst müssen sich die Teilnehmer Alice und Bob darauf einigen, auf welcher elliptischen Kurve gearbeitet werden soll.

- Gewählt werden ein Grundkörper \mathbb{F}_p (aber auch \mathbb{F}_{2^k} möglich) mit $p > 3$ prim,
 $A, B \in \mathbb{F}_p$ für die elliptische Kurve $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$
 (im Fall \mathbb{F}_{2^k} nimmt man die Glg. $y^2 + xy = x^3 + Ax^2 + B$),

so dass $E(\mathbb{F}_p)$ eine kryptographisch geeignete elliptische Kurve ist.

- Gewählt wird ein Basispunkt $P = (x, y) \in E(\mathbb{F}_p)$ mit $n := \text{ord}(P) \in \mathbb{N}$.
 Verlangt wird außerdem, dass n prim ist mit $n > 2^{160}$ und $n > 4\sqrt{p}$. Weiter
 soll n kein Teiler von $p-1, p^2-1, \dots, p^{30}-1$ sein und $n \neq p$ gelten.

26.8. Bem.: • Die Bedingung $n > 2^{160}$ sorgt dafür, dass das DL-Problem in $\langle P \rangle$
 nicht mit Pollard-S angreifbar ist. Ist n kein Teiler von $p^k - 1$, $k \leq 30$,
 kann man den MOV-Algorithmus nicht einsetzen. Wegen $n \neq p$ greift
 auch der SSSA-Algorithmus nicht.

- Es reicht, die Bedingungen an P zu erfüllen; die Kurve ist dann "von selbst"
 kryptographisch geeignet: Letztlich arbeitet man mit der Untergruppe $\langle P \rangle \subseteq E(\mathbb{F}_p)$.
- Dass die Kurve zufällig erzeugt wird per Zufallsgenerator für $p, A, B, P = (x, y)$,
 sorgt für zusätzliche Sicherheit; die zufällige Erzeugung sollte in der Praxis
 idealerweise überprüfbar sein, um auszuschließen, dass kryptographisch
 Schwache Kurven durch Betrüger eingeschleust werden.

26.9. Schritt 2.): Alice wählt eine Zufallszahl $a \in \{0, \dots, m-1\}$ als privaten Schlüssel, der Punkt $aP \in E(\mathbb{F}_p)$ gibt sie als öffentlichen Schlüssel bekannt.

Für ihr zu unterschreibendes Dokument $m \in \mathcal{M}$ berechnet sie $h(m) \in \{0, 1\}^N$ für eine vorher festgelegte geeignete Hashfunktion; der Bitstring $(a_0, a_1, \dots, a_{N-1})$ wird dann als $H(m) = \sum_{i=0}^{N-1} a_i \cdot 2^{N-1-i} \leq 2^N - 1$ interpretiert.

Schritt 3.): Alice wählt eine Zufallszahl $\tilde{a} \in \{1, \dots, m-1\}$ ($\tilde{a} \neq 0$) und berechnet den Punkt $\tilde{a}P = (u, v)$ sowie den Rest $\mathcal{F}(\tilde{a}P) \equiv u \pmod{m}$.

(Die Funktion $\mathcal{F}: \langle P \rangle \rightarrow \{0, 1, \dots, m-1\}$ ist zwar nicht bijektiv, die Urbildmenge eines u ist aber klein genug, so dass unwahrscheinlich ist, dass $\mathcal{F}(R) = \mathcal{F}(kP)$ gilt, ohne dass $R = kP$ gilt. Das reicht in der Praxis.)

Schritt 4.): Alice berechnet $\tilde{a}^{-1} \pmod{m}$ und die Restklasse

$$s = \tilde{a}^{-1} (H(m) - \mathcal{F}(\tilde{a}P) a) \pmod{m}.$$

Falls $s \equiv 0 \pmod{m}$, muss ein neues \tilde{a} gewählt werden \leadsto zurück zu Schritt 3.), da Bob bei der Prüfung der Unterschrift s invertieren wird.

Schritt 5.): Alice schickt das Dokument $m \in \mathcal{M}$ zusammen mit ihrer Unterschrift $(\mathcal{F}(\tilde{a}P), s)$ an Bob.

26.10. Bob überprüft die Unterschrift wie folgt:

1. Schritt: er testet, ob $\mathcal{F}(\tilde{a}P), s \in \{0, 1, \dots, m-1\}$.

2. Schritt: er berechnet $H(m) \in \mathbb{N}$,

er berechnet $s^{-1} \pmod{m}$

und den Punkt $R := s^{-1} (H(m)P - \mathcal{F}(\tilde{a}P) \cdot \overset{\text{@lies öffentl. Schlüssel}}{aP}) \in E(\mathbb{F}_p)$.

3. Schritt: Für $R = \mathcal{O}$ ist die Unterschrift ungültig.

Für $R = (x, y) \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ ist die Unterschrift gültig,

wenn $x = \underline{\underline{\mathcal{F}(\tilde{a}P)}}$ ist, sonst nicht.

26.11. Begründung der Korrektheit dieser Verifikation:

Denn wenn die Unterschrift von Alice stammt, ist

$$s = \tilde{a}^{-1} (H(m) - \mathcal{F}(\tilde{a}P)a) \pmod{m},$$

$$\text{also gilt } s^{-1} \tilde{a}^{-1} (H(m) - \mathcal{F}(\tilde{a}P)a) \equiv 1 \pmod{m},$$

$$\text{d.h. } s^{-1} (H(m) - \mathcal{F}(\tilde{a}P)a) \equiv \tilde{a} \pmod{m}$$

$$\text{und somit } R = s^{-1} (H(m)P - \mathcal{F}(\tilde{a}P)aP) = s^{-1} (H(m) - \mathcal{F}(\tilde{a}P)a)P = \tilde{a}P,$$

so dass die x-Koordinaten der Punkte R und $\tilde{a}P$ übereinstimmen müssen.