- 1 -

EllKK V20

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

---

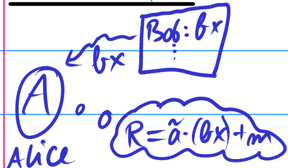
§4.2 ElGamal für elliptische Kurven

1.) Erinnerung an das allgemeine ElGamal-Verschlüsselungsverfahren für eine beliebige abelsche Gruppe G aus V6:

Alice möchte eine geheime Botschaft $m \in G$ an Bob schicken.

2.) Das Verfahren geht wie folgt:

Schritt (1.) Alice wählt eine Zufallszahl $\tilde{a} \in \{1, \ldots, n-1\}$ und berechnet $\tilde{a} \cdot x$.
Alice besorgt sich Bobs öffentlichen Schlüssel bx
und berechnet $R = \tilde{a} \cdot (bx) + m$.



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

$$\text{Alice } \xrightarrow{\tilde{a}x,\, R} \text{ Bob}$$

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

3.) 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 V19, 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 Klartext als einen Punkt auf der elliptischen Kurve kodiert und wieder zurückerhält (etwa wie in V17 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:
   Ⓐlice: $a \in \mathbb{N}$ (geheim) und $a \cdot P$ (öffentlich),
   Ⓑob: $b \in \mathbb{N}$ (geheim) und $b \cdot P$ (öffentlich).

Danach kann das ElGamal-Verfahren wie oben beschrieben durchgeführt werden.

4) <u>Bsp.:</u> Man lege das Alphabet $\Sigma = \{A, B, \ldots, Z\}$ zugrunde und nehme die elliptische Kurve $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$ (in der Rolle von $x \in G$) mit $p = 6833$, $A = 5984$, $B = 1180$ und den Basispunkt $P = (1, 2631)$.

- Teilnehmer Ⓑob wählt den geheimen Schlüssel $b = 2465 \in \mathbb{N}$ und macht $Q = 2465 \cdot P = (4748, 2021)$ öffentlich.
- Teilnehmerin Ⓐlice schickt den geheimen Text "INSTITUT" etwa in der folgenden Form (Streckungsfaktor 10, $\tilde{a}$ = Zufallszahl) an Bob:

Text	IN	ST	IT	UT
w	$(8,13)_{(26)} = 221 \rightsquigarrow 2210$	$(18,19)_{(26)} = 487 \to 4870$	$(8,19)_{(26)} = 227 \rightsquigarrow 2270$	$(20,19)_{(26)} = 539 \rightsquigarrow 5390$
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 Ⓐlice an Ⓑob verschickt.
Ⓑob entschlüsselt mit $\tilde{a}Q + M_w - b\tilde{a}P = M_w$, da $Q = bP$,
die x-Koordinate x von $M_w \in E(\mathbb{F}_p)$ ergibt dann mit $\lfloor \frac{x}{10} \rfloor = w$ den Textblock.

§ 4.3 ECDSA-Signaturen

5.) ECDSA ist das DSA-Verfahren (elektronische Unterschrift) auf elliptischen Kurven. Ⓐlice möchte dabei ein Dokument $m \in \mathcal{M}$ an Ⓑob schicken und signieren.

6.) <u>Schritt 1.):</u> Zuerst müssen sich die Teilnehmer Ⓐlice und Ⓑob darauf einigen, auf welcher elliptischen Kurve gearbeitet werden soll.

- Gewählt werden ein Grundkörper $\mathbb{F}_p$ (aber auch $\mathbb{F}_{2^r}$ 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 $\mathbb{F}_{2^r}$ 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 $n := \operatorname{ord}(P) \in \mathbb{N}$. Verlangt wird außerdem, dass n prim ist mit $n > 2^{160}$ und $n > 4\sqrt{p}$. Weiter soll n kein Teiler von $p-1, p^2-1, \ldots, p^{30}-1$ sein und $n \neq p$ gelten.

7) **Bem.:** • Die Bedingung $n > 2^{160}$ sorgt dafür, dass das DL-Problem in $\langle P \rangle$ nicht mit Pollard-ς 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.

8) **Schritt 2.):** Ⓐlice wählt eine Zufallszahl $a \in \{0, \dots, n-1\}$ 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 $H(m) = \sum_{i=0}^{N-1} a_i 2^{N-1-i} \leq 2^N - 1$ interpretiert.

Schritt 3.): Ⓐlice wählt eine Zufallszahl $\hat{a} \in \{1, \dots, n-1\}$ $(\hat{a} \neq 0)$ und berechnet den Punkt $\hat{a}P = (u, v)$ sowie den Rest $\Psi(\hat{a}P) \equiv u \mod n$.
(Die Funktion $\Psi : \langle P \rangle \to \{0, 1, \dots, n-1\}$ ist zwar nicht bijektiv, die Urbildmenge eines u ist aber klein genug, so dass unwahrscheinlich ist, dass $\Psi(R) = \Psi(kP)$ gilt, ohne dass $R = kP$ gilt. Das reicht in der Praxis.)

Schritt 4.): Ⓐlice berechnet $\hat{a}^{-1} \mod n$ und die Restklasse

$$\underline{s = \hat{a}^{-1}\left(H(m) - \Psi(\hat{a}P)\, a\right)} \mod n.$$

Falls $s \equiv 0 \mod n$, muss ein neues $\hat{a}$ gewählt werden $\rightsquigarrow$ zurück zu Schritt 3.), da Ⓑob bei der Prüfung der Unterschrift s invertieren wird.

Schritt 5.): Ⓐlice schickt das Dokument $m \in \mathcal{M}$ zusammen mit ihrer Unterschrift $\underline{\underline{(\Psi(\hat{a}P), s)}}$ an Ⓑob.

9.) Bob überprüft die Unterschrift wie folgt:

1. Schritt: er testet, ob $\Psi(\hat{a}P), s \in \{0, 1, \dots, n-1\}$.

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

er berechnet $s^{-1} \bmod n$ Alices öffentl. Schlüssel

und den Punkt $R := s^{-1}(H(m)P - \Psi(\hat{a}P) \cdot aP) \in E(\mathbb{F}_p)$.

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 $x = \Psi(\hat{a}P)$ ist, sonst nicht.

10.) Begründung der Korrektheit dieser Verifikation:

Denn wenn die Unterschrift von Alice stammt, ist

$$s = \hat{a}^{-1}(H(m) - \Psi(\hat{a}P)a) \bmod n,$$

also gilt $s^{-1}\hat{a}^{-1}(H(m) - \Psi(\hat{a}P)a) \equiv 1 \bmod n$,

d.h. $s^{-1}(H(m) - \Psi(\hat{a}P)a) \equiv \hat{a} \bmod n$

und somit $R = s^{-1}(H(m)P - \Psi(\hat{a}P)aP) = s^{-1}(H(m) - \Psi(\hat{a}P)a)P = \hat{a}P$,

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