

K25: Sichere Kryptographie mit elliptischen Kurven

Stichworte: Bekannte Angriffe auf das DL-Problem bei speziellen elliptischen Kurven, supersinguläre/anomale Kurven, Vergleich mit konventionellen Kryptoverfahren

---

25.1. Einführung: Wir geben einen Überblick zu bekannten Angriffen auf das DL-Problem, insbesondere auf elliptischen Kurven, vgl. K11.3. Die Sicherheit des ElGamal- und ECDSA-Verfahrens beruht auf der Schwierigkeit des DL-Problems auf elliptischen Kurven. Allerdings gibt es bestimmte Arten elliptischer Kurven, bei denen das DL-Problem algorithmisch schnell lösbar ist, so dass sich diese Kurven als kryptographisch schwach bzw. ungeeignet erweisen. Auch die Wahl eines Punktes  $P$  mit großer Ordnung ist wichtig.

Wir behandeln zur Lösung des DL-Problems zunächst die Verfahren "BSGS" und Silver-Pohlig-Hellman.

Diese beiden Methoden eignen sich zur Lösung des DL-Problems in einer beliebigen abelschen Gruppe  $G$ , also auch zu einer Gruppe  $(E(k), +)$  einer elliptischen Kurve.

25.2. DL-Problem in  $G$ : Geg. sei  $P \in G$  mit  $\text{ord}(P) = m \in \mathbb{N}$ , sowie  $Q \in \langle P \rangle$ .

Gesucht ist  $k \in \{0, \dots, m-1\}$  mit  $kP = Q$ .

25.3. BSGS (= "Baby steps giant steps"): Dieses Verfahren kommt in Frage, wenn  $P$  kleine Ordnung  $n$  hat. Dann kann das DL-Problem wie folgt gelöst werden; der Algorithmus hat einen Zeit- und Platzbedarf der Größenordnung  $O(\sqrt{m})$ :

25.4. Vorüberlegung:

Sei  $m = \lceil \sqrt{n} \rceil = \min \{ l \in \mathbb{N}; l \geq \sqrt{n} \}$ ,

Schreibe  $k = qm + r$ ,  $r \in \{0, 1, \dots, m-1\}$  (Div. mit Rest)

Ziel: Bestimme  $q, r$ .

Da  $Q = kP = qmP + rP$ , folgt  $\underbrace{Q - rP}_{\text{"Baby step"}} = \underbrace{qmP}_{\text{"Giant step"}}$ .

25.5. Idee: Berechne alle möglichen Werte der l.S. = "Baby step" und nach und nach die möglichen Werte der r.S. = "Giant step". Trifft man auf eine Übereinstimmung, sind  $r$  und  $q$  gefunden.

25.6. 1. Schritt: Berechne die Liste der "Baby steps"  $B = \{ (Q - rP, r); 0 \leq r \leq m \}$ .

25.7. 2. Schritt:

- Ist für eines der  $r$  die Glg.  $Q - rP = \mathcal{O}$  erfüllt, ist  $k = r$ . ✓
- Sonst teste für den ersten "Giant step"  $R = mP$ , ob  $R$  in der Baby step liste  $B$  schon vorkommt. Falls ja:  $k = m + r$ . ✓
- Teste so alle "Giant steps"  $2R, 3R, 4R, \dots, (m-1)R$ , ob diese in  $B$  vorkommt, wenn ja, gibt die 2. Komponente  $r$  mit  $k = qm + r$ . ✓

25.8. Silver-Pohlig-Hellman-Verfahren:

Dieses Verfahren löst das DL-Problem in einer abelschen Gruppe  $G$ , wenn die Ordnung  $n = \text{ord}(P)$  aus nur kleinen Primfaktoren  $p_i$  zusammengesetzt, d.h. glatt ist.

25.9. Def.: Sei  $B \in \mathbb{R}_{>0}$ . Dann heißt  $m \in \mathbb{N}$  B-glatt, falls  $\forall p|m: p \leq B$ .

25.10. Die Bestimmung von  $k$  in  $\langle P \rangle$  wird auf Untergruppen von  $\langle P \rangle$  der Ordnungen  $p_i|m$  zurückgeführt.

Sei  $\text{ord}(P) = m = \prod_{i=1}^t p_i^{\lambda_i}$  mit  $p_1, \dots, p_t$  p.w.v. prim,  $\lambda_i \in \mathbb{N}$ .  
 Der Algorithmus hat dann eine Laufzeit von  $\underline{\underline{O\left(\sum_{i=1}^t (\lambda_i (\log(m + \sqrt{p_i})))\right)}}$ .

25.11. Vorbereitung:

• Zur Bestimmung von  $k$  mit  $kP = Q \in \langle P \rangle$  berechnen wir alle Restklassen  $k \bmod p_1^{\lambda_1}, k \bmod p_2^{\lambda_2}, \dots, k \bmod p_t^{\lambda_t}$ . Denn laut CRS ist  $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{\lambda_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_t^{\lambda_t}\mathbb{Z}$ , so dass damit dann auch die Restklasse von  $k \bmod m$  bestimmt werden kann.

• Betr. daher jedes  $p = p_i, \lambda = \lambda_i$  mit  $1 \leq i \leq t$ .

Gesucht:  $z \in \{0, \dots, p^{\lambda} - 1\}$  mit  $z \equiv k \bmod p^{\lambda}$ . ( $\leadsto z \equiv k \equiv z_0(p)$ )

Schreibe  $z = z_0 + z_1 p + \dots + z_{\lambda-1} p^{\lambda-1}$ , die  $z_i \in \{0, \dots, p-1\}$ ,

in der  $p$ -adischen Entwicklung; bestimme die  $z_0, \dots, z_{\lambda-1}$ .

25.12. 1. Schritt: Sei  $R := \frac{m}{p} \cdot P$ , dann ist  $\frac{m}{p} Q = \frac{m}{p} kP = kR$  und  $pR = O$ .

Also ist  $kR = zR = z_0 R$ , d.h.  $z_0 R = \frac{m}{p} \cdot Q$ .

Somit muss man in der Untergruppe  $\langle R \rangle$  der (kleinen) Ordnung  $p$  ein DL-Problem lösen, um  $z_0$  zu bestimmen — etwa mit BSGS.

25.13. 2. Schritt: Seien  $z_0, \dots, z_{j-1}$  schon (rekursiv) bestimmt, wo  $j \leq \lambda - 1$  ist.

Berechne dann  $Q_j := \frac{m}{p^{j+1}} (Q - (z_0 + z_1 p + \dots + z_{j-1} p^{j-1}) P)$ .

Da  $nP = O$ , ist  $\frac{m}{p^{j+1}} \cdot p^j P = O$ , da  $z \equiv k \bmod p^{\lambda}$  ist  $k = z + sp^{\lambda}$ ,  $s \in \mathbb{Z}$ ,

$$\text{also } \frac{m}{p^{j+1}} Q = \frac{m}{p^{j+1}} kP = \frac{m}{p^{j+1}} zP + \underbrace{\frac{m}{p^{j+1}} \cdot s p^{\lambda} P}_{=O} = \frac{m}{p^{j+1}} zP$$

$$\text{und somit } Q_j = \frac{m}{p^{j+1}} (z_j p^j + \dots + z_{\lambda-1} p^{\lambda-1}) P = \frac{m}{p} z_j P = z_j R.$$

$\leadsto$  Zur Bestimmung von  $z_j$  ist wieder ein DL-Problem in der Untergruppe  $\langle R \rangle$  der Ordnung  $p$  zu lösen — etwa mit BSGS.

25.14. Bem.: Ist die Gruppenordnung glatt, ist der Algorithmus also sehr schnell.

### Verfahren "Pollard-S" und "Pollard-λ":

25.15. Der Pollard-S-Algorithmus ist von der Laufzeit her vergleichbar mit BSGS, ist aber speicherplatztechnisch günstiger und löst sich gut parallelisieren. Mit  $m$  Prozessoren wird der Algorithmus so um den Faktor  $m$  schneller.

25.16. Der Pollard-λ-Algorithmus ist ähnlich, i.o. eher langsamer als Pollard-S. Er liefert gute Ergebnisse, wenn der diskrete Logarithmus  $k$  in einem hinreichend kleinen Intervall liegt. Auch Pollard-λ ist gut parallelisierbar. (Die genannten Verfahren können in der Fachliteratur nachgeschlagen werden.)

### Verfahren MOV und SSSA:

25.17. Beim MOV-Verfahren [Autoren: Menezes, Okamoto, Vanstone] wird das DL-Problem für eine elliptische Kurve  $E(\mathbb{F}_{p^r})$  auf das in der Gruppe  $(\mathbb{F}_{p^{r\ell}}^*, \cdot)$  für ein  $\ell \geq 1$  zurückgeführt. Es ist also speziell nur für elliptische Kurvengruppen konstruiert, nicht für allgemeine abelsche Gruppen. Zeigt sich hier, dass  $\ell \geq 1$  so wählbar ist, dass das DL-Problem in  $(\mathbb{F}_{p^{r\ell}}^*, \cdot)$  leicht, d.h. schnell, zu lösen ist, ist die elliptische Kurve kryptographisch ungeeignet, etwa wenn  $m = \text{ord}(P)$  Teiler von  $p^{r\ell} - 1$  ist.

25.18. Generell lässt sich das DL-Problem in  $(\mathbb{F}_{p^r}^*, \cdot)$  in subexponentieller Zeit schnell lösen (mit sogenannten Index-Calculus-Methoden), so dass Kurven, für die das DL-Problem auf ein schnelleres in einem  $(\mathbb{F}_{p^{r\ell}}^*, \cdot)$  zurückgeführt werden kann, als kryptographisch schwach bzw. ungeeignet angesehen werden.

Das ist etwa bei supersingulären elliptischen Kurven der Fall, bei denen die Gruppenstruktur recht gut bekannt ist.

- 25.19. Def.: Eine elliptische Kurve  $E(\mathbb{F}_{p^r})$  heißt supersingulär, falls  $p = \text{char}(\mathbb{F}_{p^r})$  die Spur des Frobenius teilt, d.h.  $p \mid p^r + 1 - \#E(\mathbb{F}_{p^r})$ .
- 25.20. Bem.: • Um zu testen, ob eine Kurve supersingulär und damit kryptographisch ungeeignet ist, muss die Gruppenordnung  $\#E(\mathbb{F}_{p^r})$  der elliptischen Kurve bestimmt werden – typischerweise mit dem Schoof-Algorithmus.  
• Der Begriff "supersingulär" hat nichts mit singulären Punkten zu tun: elliptische Kurven sind per Definition nicht-singulär.
- 25.21. Bsp.: Die Kurve  $E(\mathbb{F}_2): y^2 + y = x^3 + x + 1$  ist supersingulär, da  $E(\mathbb{F}_2) = \{O\}$ .
- 25.22. Bem.: Supersingularität bleibt bei Übergang zu einem Erweiterungskörper erhalten: Ist  $E(\mathbb{F}_{p^r})$  supersingulär, dann auch  $E(\mathbb{F}_{p^{rl}})$  für alle  $l \geq 1$ .  
[Ohne Bew.]
- 25.23. 1. Kriterium für Supersingularität: Sei  $p \geq 3$ ,  $E(\mathbb{F}_p): y^2 = x^3 + ax^2 + bx + c =: h(x)$  elliptische Kurve. Dann ist  $E(\mathbb{F}_p)$  genau dann supersingulär, wenn der Koeffizient vor  $T^{p-1}$  in  $h(T)^{(p-1)/2} \in \mathbb{F}_p[T]$  gleich 0 ist.
- 25.24. 2. Kriterium für Supersingularität: Sei  $p=2$ ,  $E(\mathbb{F}_{2^r}): y^2 + a_1xy + y = x^3 + a_2x^2 + a_4x + a_6$ .  
Dann ist  $E(\mathbb{F}_{2^r})$  genau dann supersingulär, wenn  $a_1 = 0$ . [Ohne Bew.]
- 25.25. Bsp.: s.o. 25.21, und  $E(\mathbb{F}_p): y^2 = x^3 + x$  ist für  $p \equiv 3(4)$  supersingulär.  
Denn:  $(T^3 + T)^{(p-1)/2} = \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j} T^{3j} T^{(p-1)/2 - j}$   
mit  $\frac{p-1}{2} + 2j = p-1 \Leftrightarrow 2j = \frac{p-1}{2}$ , d.h. wenn  $2 \mid \frac{p-1}{2} \Leftrightarrow p \equiv 1(4)$   
 $\rightarrow$  Koeff. vor  $T^{p-1}$  ist  $\binom{(p-1)/2}{(p-1)/4} \neq 0$  in  $\mathbb{F}_p$ .  
Für  $p \equiv 3(4)$  kommt  $T^{p-1}$  nicht vor  $\rightarrow$  Koeff. = 0.]
- 25.26. Bem.: Der MOV-Algorithmus nutzt bei einer supersingulären Kurve  $E(\mathbb{F}_{p^r})$  aus, dass  $t = p^r + 1 - \#E(\mathbb{F}_{p^r})$  nur einen der Werte  $t \in \{0, \pm\sqrt{p^r}, \pm\sqrt{2p^r}, \pm\sqrt{3p^r}, \pm 2\sqrt{p^r}\}$  annehmen kann.

25.27. Beim SSSA-Verfahren [Autoren: Sato, Smart, Semaev, Araki] handelt es sich um einen schnellen Algorithmus zur Lösung des DL-Problems auf anormalen elliptischen Kurven, welche deswegen kryptographisch ungeeignet sind. Die Grundidee ist, die elliptische Kurve über  $\mathbb{F}_p$  als eine über  $\mathbb{Q}_p$  zu betrachten, dem Körper der  $p$ -adischen Zahlen, und die Logarithmenberechnung auf eine Division in  $\mathbb{Z}_p$  zurückzuführen (was leicht ist).

25.28. Def.: Eine elliptische Kurve  $E(\mathbb{F}_p)$  heißt anormal, wenn  $\#E(\mathbb{F}_p) = p$  ist. Dies lässt sich wieder durch Bestimmung von  $\#E(\mathbb{F}_p)$  mit dem Schoof-Algorithmus leicht überprüfen. Der SSSA-Algorithmus kann auf Kurven über  $\mathbb{F}_p$  übertragen werden. Er hat polynomiale Laufzeit.

25.29. Überblick: geeignete elliptische Kurven und Vergleich mit anderen Public-Key-Verfahren

Eine elliptische Kurve  $E(\mathbb{F}_p): y^2 = x^3 + ax + b$  mit vorgegebener Bitzahl für  $p$  ist leicht zu finden – mit Zufallszahlengenerator und Primzahltest, was auch für große Zahlen mit mehreren hundert Dezimalstellen schnell machbar ist; dafür kennt man ganz gute Algorithmen.

25.30. Man wählt solange die Parameter  $p, a, b$  neu, bis die Diskriminante  $4a^3 + 27b^2$  nicht durch  $p$  teilbar ist und somit eine elliptische Kurve vorliegt. Ziemlich sicher liegt dann eine kryptographisch geeignete Kurve vor. Das testet man nach Berechnender Gruppenordnung  $\#E(\mathbb{F}_p)$  mit dem Schoof-Algorithmus:

- 25.31. • Ist  $\#E(\mathbb{F}_p)$  glatt, d.h. hat  $\#E(\mathbb{F}_p)$  nur kleine Primteiler, ist die Kurve ungeeignet wegen Silver-Pohlig-Hellman.
- Ist  $\#E(\mathbb{F}_p) = p+1$ , d.h. die Kurve supersingulär, ist die Kurve ungeeignet (MOV).
- Ist  $\#E(\mathbb{F}_p) = p$ , d.h. die Kurve anomal, ist die Kurve ungeeignet (SSSA).
- Ob die Kurve supersingulär/anomal ist, kann man <sup>meist</sup> leicht erkennen durch Wahl von Punkten  $P \in E(\mathbb{F}_p)$  und dem Test, ob  $(p+1)P = \mathcal{O}$  bzw  $pP = \mathcal{O}$  gilt.

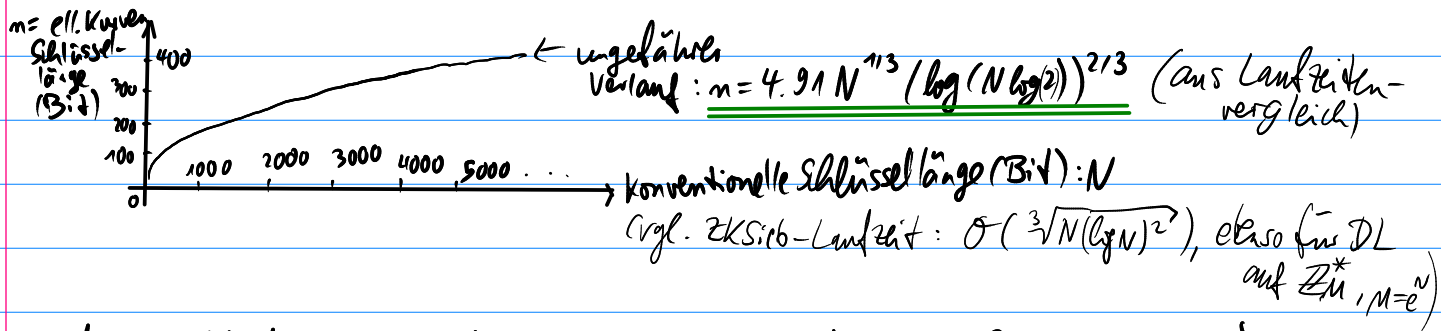
25.32. Die Wahl eines Punktes  $P$  mit nicht zu kleiner Ordnung  $n$  muss dann gewährleistet werden. Speziell darf  $n$  kein Teiler von  $p^t - 1$  sein, wenn das DL-Problem in  $(\mathbb{F}_{p^t}^*, \cdot)$  leicht zu lösen ist, und  $n$  darf auch kein Vielfaches von  $p$  sein (wegen SSSA).

Auch sollte  $n$  nicht glatt sein; man wählt in der Praxis meist Punkte  $P$ , für die  $n = \text{ord}(P)$  eine hinreichend große Primzahl ist; für sie sollte etwa  $n > 2^{60}$  gelten.

25.33. Die für allgemeine elliptische Kurven, die in diesem Sinne als kryptographisch sicher gelten, bekannte Implementierungen des DL-Problems sind alle von exponentieller Komplexität. Ein Kryptographieverfahren wie ElGamal bzw. DSA gilt dann als kryptographisch sicher.

25.34. Für konventionelle Kryptoverfahren (RSA und ElGamal / DSA auf  $(\mathbb{F}_{p^t}^*, \cdot)$ ) gibt es subexponentielle Verfahren zur Lösung des DL-Problems.

Dieser Vergleich schlägt sich in der Wahl der Schlüssellängen (= Bitzahl der Größe des endl. Körpers) nieder: Die Schlüssellänge eines elliptischen Kurven-Systems wächst etwas schneller als die 3. Wurzel der Schlüssellänge eines konventionellen Krypto-Systems mit ähnlicher kryptographischer Sicherheit:



- 25.35
- Man geht davon aus, dass Kurven  $E(\mathbb{F}_p)$  mit  $p \approx 2^{173}$ , wo  $\#E(\mathbb{F}_p)$  einen Primteiler  $\geq 2^{160}$  hat, die gleiche Sicherheit wie ein RSA-System mit 1024 Bit bietet (für 4096 Bit beim RSA nur etwa 313 bei ECC-System!).
  - Durch die geringere Schlüssellänge bei Verfahren mit elliptischen Kurven kann man diese leicht auf Smart-Cards ohne Koprozessor implementieren. Solche Smart-Cards sind wesentlich billiger als Chip-Karten mit Koprozessor.

25.36. Bedenken der elliptische Kurven-Kryptographie:

Die Nichteignung supersingularer/anomaler Kurven kam schnell und überraschend. Es ist unklar, ob noch weitere ungeeignete Kurvenfamilien existieren und mit einem schnellen DL-Algorithmus angreifbar sind.