Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K24: Der Schoof-Algorithmus

Stichworte: Modularitätsmuster ~> Taniyama-Shimura-Vermutung = Modularitätssatz, Frey-Kurven, großer Fermatscher Satz, Schoof-Algorithmus zur Bestimmung von $\#E(\mathbb{F}_{p^n})$ in der Praxis für eine gegebene elliptische Kurve mit Koeff. $\in \mathbb{Z}$

24.1. Einleitung: Wir erläutern ein Modularitätsmuster für elliptische Kurven, das im Zusammenhang mit dem großen Fermatsche Satz steht. Weiter behandeln wir den Schoof-Algorithmus.

24.2. Für elliptische Kurven mit Koeffizienten $\in \mathbb{Z}$ wurde ein Modularitätsmuster gefunden, welches sehr unerwartet und ungewöhnlich ist, dass es kaum vorstellbar ist, dass dieses überhaupt gefunden werden konnte. Es handelt sich (in voller Allgemeinheit) um die Taniyama-Shimura-Vermutung von 1957, welche von A. Wiles et. al. 1995 komplett bewiesen wurde und als Baustein des Beweises des großen Fermatschen Satzes diente (Vgl. ZT I, Z1).

24.3. Im Spezialfall der Kurve $E: y^2 = x^3 - 4x^2 + 16$ z.B. lautet diese Vermutung, dass folgendes "Modularitätsmuster" für die Defekte a_p gilt:
Man betrachte die Potenzreihe $\Theta(T) \in \mathbb{Z}[T]$, welche durch Ausmultiplizieren des unendlichen Produkts

$$\Theta(T) := T\cdot\left((1-T)(1-T^{11})\right)^2\cdot\left((1-T^2)(1-T^{22})\right)^2\cdot\left((1-T^3)(1-T^{33})\right)^2\cdot\left((1-T^4)(1-T^{44})\right)^2\cdot\ldots$$

entsteht, sie beginnt mit $\Theta(T) = T - 2T^2 - T^3 + 2T^4 + T^5 + 2T^6 - 2T^7 - 2T^9 - 2T^{10} + T^{11} - 2T^{12} + 4T^{13} + 4T^{14} - T^{15} - 4T^{16} - 2T^{17} + -\ldots$

Im Vergleich die Defekte von E: $a_2 = 0$, $a_3 = -1$, $a_5 = 1$, $a_7 = -2$, $a_{11} = 1$, $a_{13} = 4$, $a_{17} = -2, \ldots$,
d.h. bis auf a_2 ist a_p genau der Koeffizient vor T^p in $\Theta(T)$, $p \geq 3$ prim.

24.4. Ein derartiges Muster vermuteten Taniyama/Shimura für jede elliptische Kurve mit Koeffizienten $\in \mathbb{Z}$, genauer: jede elliptische Kurve ist "modular".

24.5. Der große Satz von Fermat besagt, dass die Gleichung $A^n + B^n = C^n$ für $n \geq 3$ keine Lösungen in $\mathbb{Z} \setminus \{0\}$ besitzt.
Fermat formulierte diese Aussage im 17. Jahrhundert und ihr Beweis galt bis 1995 als eines der größten ungelösten Probleme der Mathematik. Die Bemühungen vieler Mathematiker um diese Vermutung brachten die Mathematik, speziell die algebraische Zahlentheorie, bis heute weit voran. Die Lösung durch A. Wiles stellte 1995 einen riesigen Durchbruch dar.

24.6. Bis 1980 wurden Lösungsversuche durch Faktorisierungstechniken vorgenommen.
Im Jahr 1986 schlug G. Frey eine Verbindung zwischen Fermats großem Satz und elliptischen Kurven vor, auf der die weiteren Erfolge beruhten:
Zu einer angenommenen, nichttrivialen Lösung A, B, C des großen Fermat-Satzes zu einem primen Exponenten $n = p$ betr. man die zugehörige elliptische Kurve
$$E_{A,B} : y^2 = x(x + A^p)(x - B^p),$$
ihre Diskriminante ist $\Delta(E_{A,B}) = 16(ABC)^{2p}$, was unwahrscheinlich erscheint.

Die Idee ist, z.B., dass eine solche Kurve nicht modular sein kann, d.h. der Taniyama-Shimura-Vermutung widerspricht. Im Jahr 1986 konnte dies gezeigt werden von K. Ribet. Davon inspiriert verbrachte A. Wiles die nächsten 6 Jahre damit, die Taniyama-Shimura-Vermutung zumindest für sogenannte semistabile elliptische Kurven zu zeigen, was ihm gelang.
Da Frey-Kurven $E_{A,B}$ semistabil sind, reichte dies zum Beweis des großen Fermatschen Satzes aus.

24.7. Mittlerweile wurde die (volle) Taniyama-Shimura-Vermutung bewiesen durch C. Breuil, B. Conrad, F. Diamond und R. Taylor (2001) und heißt heute Modularitätssatz. Heute wird der Modularitätssatz als Spezialfall der allgemeineren Serre-Vermutung über Galoisdarstellungen angesehen, welche aufbauend auf den Arbeiten von A. Wiles, inzwischen (im Jahr 2006) von C. Khare, J.-P. Wintenberger und M. Kisin bewiesen wurde.

24.8. Wir behandeln im folgenden noch den Schoof-Algorithmus:
Für die kryptographie-Anwendungen ist ein praktischer Weg, die Anzahl $N_{p^r} = \#E(\mathbb{F}_{p^r})$ der Punkte auf einer elliptischen Kurve über einem endlichen Körper $\mathbb{F}_{p^r}$ zu bestimmen, von Bedeutung. Dies leistet der Schoof-Algorithmus, den wir jetzt besprechen.

24.9. Vor.: Sei $p > 2$ und $E(\mathbb{F}_{p^r})$ geg. durch $y^2 = x^3 + ax + b$, wo $a, b \in \mathbb{F}_{p^r}$ ist.
Der Algorithmus bestimmt $t := a_{p^r} = p^r + 1 - \#E(\mathbb{F}_{p^r})$ nur modulo der ersten Primzahlen $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$ bis damit a_{p^r} bestimmt werden kann.

24.10. Für die ersten s Primzahlen $p_1, \ldots, p_s$ vermittelt der CRS durch die Restklassenabbildung $\mathbb{Z} \longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$
eine Bijektion $\mathbb{Z}_{p_1 \cdots p_s} \xrightarrow{\cong} \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$.

Gilt $|t| < \frac{1}{2} p_1 \cdots p_s$, ist $t \bmod p_1 \cdots p_s$ durch die Restklassen $(t \bmod p_1, \ldots, t \bmod p_s)$ eindeutig bestimmt. Da nach dem Satz von Hasse $|t| < 2\sqrt{p^r}$ gilt, genügt es, s mit $p_1 \cdots p_s > 4\sqrt{p^r}$ zu wählen. Die Bestimmung von $t \bmod p_1, \ldots, t \bmod p_s$ reicht dann also zur Bestimmung von t laut CRS.

24.11. 1. Schritt: Bestimmung von t mod 2.

Da $t \equiv \#E(\mathbb{F}_{p^r}) \bmod 2$, muss die Parität von $\#E(\mathbb{F}_{p^r})$ bestimmt werden, d.h. ob $\#E(\mathbb{F}_{p^r})$ gerade oder ungerade ist.

- Für festes $x \in \mathbb{F}_{p^r}$ mit $x^3+ax+b \neq 0$ in $\mathbb{F}_{p^r}$ hat $y^2 = x^3+ax+b$ keine oder 2 Lsgn. y, d.h. die $\#$ Lsgn. (x,y) mit $y \neq 0$ ist gerade und zählen mod 2 daher nicht.

- Es bleiben $\mathcal{O}$ und die $(x_0,0) \in E(\mathbb{F}_{p^r})$ zu zählen. Über $\overline{\mathbb{F}}_{p^r}$ faktorisiert x^3+ax+b zu $x^3+ax+b = (x-x_0)(x-x_1)(x-x_2)$ mit $x_1, x_2 \in \overline{\mathbb{F}}_{p^r}$. Da E nicht-singulär, sind x_0, x_1, x_2 p.w.v. Wegen $x_0+x_1+x_2 = 0$ ($\hat{=}$ Koeff. vor x^2) folgt
a) $x_1, x_2 \in \mathbb{F}_{p^r}$ oder b) $x_1, x_2 \in \overline{\mathbb{F}}_{p^r} \setminus \mathbb{F}_{p^r}$.

- Im Fall a) gibt es 3 Punkte $(x_i, 0) \in E(\mathbb{F}_{p^r})$, im Fall b) nur einen Punkt, so dass $t \equiv \#E(\mathbb{F}_{p^r}) \equiv 0\ (2)$ folgt (wegen $\mathcal{O}$), sofern $(x_0,0) \in E(\mathbb{F}_{p^r})$ existieren. Gibt es keine solchen Punkte, folgt (wegen $\mathcal{O}$) dann $t \equiv \#E(\mathbb{F}_{p^r}) \equiv 1\ (2)$.

- Ob $(x_0,0) \in E(\mathbb{F}_{p^r})$ existieren, kann durch Überprüfen von $x-x_0 \mid x^3+ax+b$ für alle $x_0 \in \mathbb{F}_{p^r}$ getestet werden; wegen $x^{p^r}-x = \prod_{x_0 \in \mathbb{F}_{p^r}} (x-x_0)$ also effektiv durch Überprüfen von
$\operatorname{ggT}(x^3+ax+b,\ x^{p^r}-x) = 1$ im Polynomring $\mathbb{F}_{p^r}[x]$ mit dem euklidischen Algorithmus.

Erläuterung zu $x^{p^r}-x \overset{!}{=} \prod_{x_0 \in \mathbb{F}_{p^r}} (x-x_0)$: $\forall\, b \in \mathbb{F}_{p^r}$ ist $b^{p^r-1} = 1$, d.h. $b^{p^r} = b$ bzw. $b^{p^r}-b = 0$, denn p^r-1 ist die Gruppenordnung von $(\mathbb{F}_{p^r}^*, \cdot)$. ⌟

24.12. 2. Schritt: Bestimmung von $t \bmod p_i \geq 3$.

Dies ist deutlich schwieriger, hier nur die Grundidee:

- Der Frobenius $\Phi: E(\overline{\mathbb{F}}_{p^r}) \to E(\overline{\mathbb{F}}_{p^r}), [x:y:z] \mapsto [x^{p^r}:y^{p^r}:z^{p^r}]$ genügt der Gleichung
$\Phi^2(P) - t \cdot \Phi(P) + p^r \cdot P = \mathcal{O}$ für alle $P \in E(\overline{\mathbb{F}}_{p^r})$,
da t die "Spur" des Frobenius ist. [ohne Beweis]
Zu bestimmen ist eine Zahl $\tau \in \{0, \dots, p_i - 1\}$, die dieser Glg. (an Stelle t) für jeden Punkt $P \in E[p_i] := \{P \in E(\overline{\mathbb{F}}_{p^r}); \underbrace{\operatorname{ord}(P) \mid p_i}_{\Leftrightarrow p_i \cdot P = \mathcal{O}}\}$ genügt.

⌜Denn für so ein τ muss $(t - \tau)\Phi(P) = \mathcal{O}$ für jedes $P \in E[p_i] \setminus \mathcal{O}$ sein.
Da $\Phi(P) \in E[p_i] \setminus \mathcal{O}$ ist, ist $\operatorname{ord}(\Phi(P)) = p_i$ in $E[p_i]$,
es folgt $p_i = \operatorname{ord}(\Phi(P)) \mid t - \tau$, also $t \equiv \tau \bmod p_i$.⌟

- Die Bestimmung von τ mit $\Phi^2(P) - \tau\Phi(P) + p^r \cdot P = \mathcal{O}$ für alle $P \in E[p_i]$ kann mittels der expliziten Formeln in eine Polynomgleichung übersetzt werden, für die der Reihe nach für $\tau = 0, 1, \dots, p_i - 1$ getestet wird, ob sie gilt, bis man auf die Lösung stößt. □

24.13. Der Schoof-Algorithmus hat eine Laufzeit von nur $\mathcal{O}(\log^8(p^r))$, ein naiver Algorithmus zur Bestimmung von $\#E(\mathbb{F}_{p^r})$ hat eine Laufzeit von $\mathcal{O}(p^{r/4+\epsilon})$. Damit kann $\#E(\mathbb{F}_{p^r})$ mit dem Schoof-Algorithmus effektiv und schnell bestimmt werden, wenn p^r groß ist. Mithilfe von $\#E(\mathbb{F}_{p^r}) \in \mathbb{N}$ kann dann entschieden werden, ob die (meist zufällig gewählte) elliptische Kurve kryptographisch geeignet ist oder nicht. Das behandeln wir im nächsten Kapitel/K25 der Vorlesung.