Kryptographie mit elliptischen Kurven

Florian Heß (TU Berlin)

1 Einleitung

Die besondere Bedeutung elliptischer Kurven in der Kryptographie hat im wesentlichen zwei Ursachen. Zum einen bietet das diskrete Logarithmus Problem (DLP) hier nach gegenwärtigem Kenntnisstand größtmögliche Schwierigkeit im Bezug zur Gruppengröße, wodurch ein sehr gutes Verhältnis von Effizienz und Sicherheit bewirkt wird. Zum anderen finden die Tate- und Weilpaarungen auf elliptischen Kurven Anwendung in der paarungsbasierten Kryptographie, einem sehr aktuellen Gebiet der Kryptographie. Die mit diesen beiden Aspekten verbundenen Vorteile können allerdings nicht simultan genutzt werden.

Im vorliegenden Artikelsollen die wesentlichen mathematisch-algorithmischen Aspekte dieser beiden Anwendungen elliptischer Kurven in der Kryptographie dargestellt werden.

2 Generische Komplexität

In der DL-basierten Kryptographie verwendet man zyklische Gruppen G von Primzahlordnung ℓ, und in der paarungsbasierten Kryptographie betrachtet man zusätzlich bilineare, nicht ausgeartete Abbildungen $e : G_1 \times G_2 \to G_T$ solcher Gruppen.

Die Sicherheit von kryptographischen Verfahren wie Verschlüsselung oder digitale Signaturen wird auf die Komplexität gewisser Berechnungsprobleme zurückgeführt. Die wichtigsten Vertreter sind das DLP, das Diffie-Hellman Problem (DHP) und das Entscheidungs-Diffie-Hellman Problem (DDHP). Sei g ein Erzeuger von G. Beim DLP soll zu $y \in G$ ein $x \in \mathbb{Z}$ mit $y = g^x$ berechnet werden. Beim DHP soll zu $g^a, g^b \in G$ das Element g^{ab} berechnet werden (a, b unbekannt). Beim DDHP soll zu $g^a, g^b, h \in G$ entschieden werden, ob $h = g^{ab}$ gilt. Beim bilinearen Diffie-Hellman Problem soll aus g^a, g^b, g^c der Wert $e(g, g)^{abc}$ berechnet werden.

Verwendet man nur die Gruppenoperationen und keine weiteren Informationen über eine konkret vorliegende Gruppe G, so können das DLP, DHP und DDHP mit den Pollardmethoden [8] in einer Laufzeit von $O(\ell^{1/2})$ gelöst werden. Nach [39] ist dies auch bestmöglich, es ergibt sich die generische Komplexität dieser Probleme von $\Theta(\ell^{1/2})$. Die Quantenkomplexität hingegen ist polynomiell in $\log(\ell)$ [38].

Legt man die generische Komplexität für ein konkret gegebenes G zugrunde, so werden in der heutigen Praxis Primzahlen ℓ von ungefähr 160 bis 230 Bit verwendet. Gewisse Reduktionen zwischen dem DLP, DHP und DDHP und paarungsbezogenen Problemen sind bekannt [5, 28, 24, 42].

3 Elliptische Kurven

Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik $p > 3$. Eine elliptische Kurve über $\mathbb{F}_q$ wird durch eine Gleichung

$$E : Y^2 = X^3 + aX + b$$

mit $a, b \in \mathbb{F}_q$ und $4a^3 + 27b^2 \neq 0$ gegeben. Die Menge der $\mathbb{F}_q$-rationalen Punkte von E ist definiert als $E(\mathbb{F}_q) = \{(x, y) \,|\, x, y \in \mathbb{F}_q,\, y^2 = x^3+ax+b\} \cup \{\mathcal{O}\}$, wobei $\mathcal{O}$ der Punkt „im unendlichen“ ist. Nach dem Satz von Hasse-Weil gilt $\#E(\mathbb{F}_q) = q + 1 - t$ mit $t \in \mathbb{Z}$ und $|t| \leq 2\sqrt{q}$. Man kann $E(\mathbb{F}_q)$ in eine abelsche Gruppe mit dem neutralen Element $\mathcal{O}$ machen. Das Gruppengesetz wird üblicherweise additiv geschrieben. Für die Addition zweier Punkte $P_1, P_2 \in E(\mathbb{F}_q)$ gibt es explizite Formeln, die die Koordinaten von $P_1 + P_2$ als rationale Funktionen der Koordinaten von P_1 und P_2 und a, b darstellen.

Für $p = 2, 3$ gelten analoge Aussagen, nur daß die Gleichung für die Kurve andere Formen annimmt. Die obige Bedingung an a, b stellt sicher, daß $x^3 + ax + b$ keine mehrfachen Nullstellen besitzt und die Kurve damit glatt ist.

Für kryptographische Zwecke verwendet man elliptische Kurven E, für die $\#E(\mathbb{F}_q) = c\ell$ mit einem großen Primfaktor ℓ und einem kleinen Kofaktor c (beispielsweise $c < 10$) gilt. Gehört die elliptische Kurve dann nicht einem der unten aufgeführten Spezialfälle an, so sind die effizientesten bekannten Verfahren zum Lösen des DLP, DHP und DDHP die Pollardmethoden. Es ergibt sich eine Laufzeit von $\Theta^{\sim}(\ell^{1/2})$. Elliptische Kurven können damit, anders als die multiplikativen Gruppen endlicher Körper, nach gegenwärtigem Kenntnisstand im wesentlichen die maximale Komplexität für das DLP, DHP und DDHP in Abhängigkeit der Bitlänge der Darstellungen der Gruppenelemente erreichen.

Will man elliptische Kurven in der Praxis verwenden, so sind ergeben sich drei grundlegende Fragestellungen: Wie bestimmt man $\#E(\mathbb{F}_q)$? Welches sind die unsicheren Spezialfälle? Welches sind die bezüglich Effizienz, Bandbreite und Sicherheitsaspekten besten Algorithmen für $E(\mathbb{F}_q)$? Im folgenden soll kurz auf die ersten beiden Fragenstellungen eingegangen werden. Für die dritte Fragestellung verweisen wir auf [8].

Bestimmung der Ordnung von $E(\mathbb{F}_q)$. Die Berechnung von $\#E(\mathbb{F}_q)$ wird auch „Punktezählen“ genannt. Der Schoof-Elkies-Atkin (SEA) Algorithmus berechnet $\#E(\mathbb{F}_q)$ in einer heuristischen Laufzeit von $O^{\sim}(\log(q)^{4+\varepsilon})$. Die sogenannten p-adischen Methoden berechnen $\#E(\mathbb{F}_q)$ in einer Laufzeit von $O^{\sim}(\log(q)^2)$, sofern für die Charakteristik $p \in O(1)$ gilt [35]. Mit diesen Algorithmen ist es bei den in der Kryptographie verwendeten Größen von q möglich, die Ordnung $\#E(\mathbb{F}_q)$ ausreichend schnell zu berechnen. In der Praxis würde man zufällige elliptische Kurven durchprobieren und abbrechen, wenn eine Kurve mit einem hinreichend großen Primfaktor ℓ gefunden wurde. Erwartungsgemäß sind nach dem Primzahlsatz hierfür ungefähr $\log(q)$ Versuche erforderlich.

Eine andere Methodik setzt sich zum Ziel, elliptische Kurven mit bekannter Ordnung zu konstruieren [32, 26, 7, 25]. Insbesondere die Konstruktionen mit Hilfe der Theorie der komplexen Multiplikation spielen wegen der Effizienz der genannten Verfahren zum Punktezählen hauptsächlich nur noch für die Berechnung „paarungsfreundlicher“ elliptischer Kurven eine Rolle.

Unsichere Spezialfälle. Wir gehen davon aus, daß $\#E(\mathbb{F}_q)$ einen hinreichend großen Primfaktor ℓ von mindestens 160 Bit mit kleinem Kofaktor enthält. Dann gibt es prinzipiell vier Möglichkeiten, daß DLP mit Hilfe spezieller Eigenschaften von E anzugreifen.

Der multiplikative Transfer (MOV und FR Angriff) verwendet die Weil- oder Tatepaarung, um ein DLP in $E(\mathbb{F}_q)$ in ein DLP in $\mathbb{F}_{q^k}^{\times}$ abzubilden [29, 13]. Es muß ein hinreichend kleines k mit $\ell | (q^k - 1)$ geben, damit der Angriff schneller als die Pollardmethoden ist. Für supersinguläre elliptische Kurven gilt stets $k \leq 6$. Für zufällig gewählte Kurven ist die Wahrscheinlichkeit der Existenz eines kleinen k allerdings sehr gering [1].

Der additive Transfer kann angewendet werden, wenn $\ell = p$ gilt [37, 41, 36, 33]. Mit Hilfe des p-adischen Logarithmus oder allgemeiner logarithmischen Differentialen kann das DLP in $E(\mathbb{F}_q)$ in die additive Gruppe von $\mathbb{F}_p$ abgebildet werden. Der gesamte Angriff ist polynomiell in $\log(q)$.

Angriffe mittels Weil Abstieg oder Überlagerungsangriffe konstruieren mit Hilfe von Galoistheorie oder spezieller Artin-Schreier und Kummertheorie Überlagerungskurven C von E, welche über Teilkörpern K_0 von $\mathbb{F}_q$ definiert werden können [19, 9] (ein Übersichtsartikel mit weiteren Referenzen ist [21]). Das DLP wird dann von $E(\mathbb{F}_q)$ nach $\mathrm{Pic}(C)(K_0)$ abgebildet und kann dort unter Umständen leichter gelöst werden. Ist der Erweiterungsgrad $[\mathbb{F}_q : \mathbb{F}_p]$ gleich 1 oder eine Primzahl, aber nicht von der Form $2^d - 1$ und ungleich 5, so ist dieser Angriff nicht erfolgreich. Andere Erweiterungsgrade und Bedingungen für einen Ausschluß dieses Angriffs sind auch möglich, allerdings aufwendiger zu beschreiben.

Angriffe mittels Indexcalculus für elliptische Kurven sind bisher eher theoretischer Natur. Ist E über $\mathbb{F}_{q^n}$ definiert, führt man auf $E(\mathbb{F}_{q^n})$ ein Größenmaß ein, so daß sich beliebige Punkte mit einer gewissen Wahrscheinlichkeit als Summe ei-

ner kleinen Anzahl „kleiner“ Punkte darstellen lassen, und wendet die üblichen Strategien von Indexcalculus oder Relationenverfahren an. Die Berechnung der Summenzerlegung eines Punkts benötigt Verfahren zum Lösen multivariater Gleichungssysteme über $\mathbb{F}_q$. Für n fest und $q \to \infty$ kann das DLP mit dieser Methode nach [18] in $O(q^{2-2/n})$ anstelle von $O(q^{n/2})$ mit den Pollardmethoden gelöst werden. Für $n \approx \log(q)$ kann das DLP nach [10] vermutlich sogar mit einer gewissen subexponentiellen Laufzeit gelöst werden. Dieser Angriff ist jedoch nicht möglich, wenn der Erweiterungsgrad $[\mathbb{F}_{q^n} : \mathbb{F}_p]$ gleich 1 oder eine Primzahl ist.

Will man möglichst wenig Struktur in einer elliptischen Kurve haben, um etwaigen, noch zu entdeckenden Angriffen keine Angriffsmöglichkeit zu bieten, sollte man zufällig gewählte elliptische Kurven über großen Primkörpern $\mathbb{F}_p$ verwenden und gegebenenfalls zusätzlich testen, daß die Endomorphismenringe zu imaginär quadratischen Zahlkörpern mit ausreichend großer Diskriminante gehören.

4 Paarungen

Im folgenden sei E eine elliptische Kurve über $\mathbb{F}_q$. Die Punktemengen $E(\mathbb{F}_{q^k})$ sind abelsche Gruppen. Mit $E(\mathbb{F}_{q^k})[\ell]$ bezeichnen wir die Untergruppe der Punkte der Ordnung ℓ. Wir nehmen wie im vorigen Abschnitt an, daß $\#E(\mathbb{F}_q)$ einen hinreichend großen Primteiler $\ell \neq q$ besitzt. Sei $k \in \mathbb{Z}^{\geq 1}$ minimal mit $\ell | (q^k - 1)$. Wir nehmen zusätzlich an, daß $k \geq 2$ gilt und $q^k - 1$ von ℓ nur in einfacher Potenz geteilt wird. Die Zahl k heißt Einbettungsgrad von E. Unter diesen Voraussetzungen gilt $E(\mathbb{F}_{q^k})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ und die Gruppe der ℓ-ten Einheitswurzeln μ_ℓ ist in $\mathbb{F}_{q^k}$ enthalten.

Die Tatepaarung

$$\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^\ell$$

wird wie folgt definiert. Für jedes $P \in E(\mathbb{F}_{q^k})$ und $n \in \mathbb{Z}$ bezeichnen wir mit $f_{n,P} \in \mathbb{F}_{q^k}(E)$ eine rationale Funktion auf E mit $(f_{n,P}) = n((P) - (\mathcal{O})) - ((nP) - (\mathcal{O}))$, wobei (P) der durch P bestimmte Primdivisor auf E ist [40]. Seien nun $P \in E(\mathbb{F}_{q^k})[\ell]$ und $Q \in E(\mathbb{F}_{q^k})$. Wir wählen $R \in E(\mathbb{F}_{q^k})$ mit $\{Q + R, R\} \cap \{P, \mathcal{O}\} = \emptyset$ und definieren

$$\langle P, Q + \ell E(\mathbb{F}_{q^k}) \rangle_\ell = f_{\ell,P}(Q + R) / f_{\ell,P}(R) \cdot (\mathbb{F}_{q^k}^\times)^\ell.$$

In den Anwendungen betrachtet man anstelle der eben definierten Tatepaarung der Einfachheit halber die reduzierte Tatepaarung

$$t_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \to \mu_\ell,$$
$$t_\ell(P, Q) = \langle P, Q + \ell E(\mathbb{F}_{q^k}) \rangle_\ell^{(q^k-1)/\ell}.$$

Die Tatepaarung und die reduzierte Tatepaarung sind bilinear und nicht ausgeartet [13, 14, 20].

Auf die Weilpaarung gehen wir hier nicht weiter ein und verweisen auf [14, 30, 40].

Typen 1-3. Um diese Paarungen in der Kryptographie zu Einsatz zu bringen, werden gewisse Untergruppen von $E(\mathbb{F}_{q^k})$ mit günstigen Eigenschaften verwendet.

Sei π_q der Frobeniusendomorphimus von E mit $(x, y) \mapsto (x^q, y^q)$. Es gibt Punkte P, Q mit $E(\mathbb{F}_{q^k})[\ell] = \langle P \rangle \times \langle Q \rangle$ und $\pi_q(P) = P$, $\pi_q(Q) = qQ$. Speziell gilt also $P \in E(\mathbb{F}_q)$. Für diese Untergruppen ergibt sich $\langle P, P \rangle_\ell = \langle Q, Q \rangle_\ell = 1$ und $\langle P, Q \rangle_\ell \neq 1$, analoges gilt für die Weilpaarung. Der Endomorphismus $\mathrm{Tr} = c \sum_{i=0}^{k-1} \pi_q^i$ mit $kc \equiv 1 \bmod \ell$ liefert eine surjektive Projektion $\langle P \rangle \times \langle Q \rangle \to \langle P \rangle$ mit Kern $\langle Q \rangle$ (auch Spur-Null Gruppe genannt).

Eine Distortionsabbildung für $T = \lambda P + \mu Q \neq 0$ ist ein Endomorphimsmus ψ von E mit $\psi(T) \notin \langle T \rangle$. Sind λ und μ ungleich Null, so ist Tr eine Distortionsabbildung für T. Man kann zeigen, daß es eine Distortionsabbildung für $T = P, Q$ genau dann gibt, wenn E supersingulär ist [42, 17].

Anhand dieser mathematischen Daten ergeben sich drei Typen von Paarungen $e : G_1 \times G_2 \to \mu_\ell$, die in der Kryptographie Verwendung finden [34]. Typ 1 verwendet supersinguläre elliptische Kurven, eine Distortionsabbildung ψ sowie $Q = \psi(P)$. Hier gilt also $G_1 = G_2 = \langle P \rangle$. Typ 2 verwendet eine ordinäre elliptische Kurve mit $G_1 = \langle P \rangle$ und $G_2 = \langle \lambda P + \mu Q \rangle$ mit $\lambda, \mu \neq 0$. Hier gilt $G_1 \neq G_2$ und Tr liefert einen Einwegisomorphismus $G_2 \to G_1$. Typ 3 verwendet eine ordinäre elliptische Kurve mit $G_1 = \langle P \rangle$ und $G_2 = \langle Q \rangle$. Hier gilt $G_1 \neq G_2$ und es gibt (vermutlich) keinen effizient berechenbaren Isomorphismus zwischen G_1 und G_2.

Konstruktionen. Der für die Sicherheit beziehungsweise Effizienz wichtigste Parameter ist der Einbettungsgrad. Die Komplexitäten des DLP in $E(\mathbb{F}_q)$ und $(\mathbb{F}_{q^k})^\times$ betragen ungefähr $\exp(1/2 \log q)$ beziehungsweise $\exp((k \log q)^{1/3})$. Um diese Komplexitäten zu balancieren, muß k also für wachsendes q ebenfalls wachsen.

Mit supersingulären Kurven kann man die Einbettungsgrade $k \in \{2, 3, 4, 6\}$ erreichen [29]. Für größere k müssen ordinäre elliptische Kurven geeignet konstruiert werden. Folgende Bedingungen an q, ℓ, $t = q + 1 - \#E(\mathbb{F}_q)$ und k sind dabei zu beachten (ϕ_k ist das k-te Kreisteilungspolynom):

1. $q + 1 - t = c\ell$.
2. $\phi_k(q) \equiv 0 \bmod \ell$.
3. q ist Primzahlpotenz, ℓ ist Primzahl, $|t| \leq 2\sqrt{q}$.
4. $4q - t^2 = Df^2$ mit D klein.
5. $\rho = \log(q)/\log(\ell) \approx 1$.

Bedingung 2 impliziert $\ell | (q^k - 1)$. Bedingung 3 ist erforderlich, damit die elliptische Kurve mit Hilfe der Theorie der komplexen Multiplikation in vertretbarer Zeit berechnet werden kann. Bedingung 5 besagt, daß c wie zuvor möglichst klein sein soll.

Lösungen der Bedingungen 1-5 können für beliebiges k relativ einfach mit einer geeigneten Suchstrategie von C. Cox und R. Pinch gefunden werden, sofern man $\rho \approx 2$ erlaubt [14]. Dies führt jedoch zu ineffizienten Systemen. Man kann auf der anderen Seite zeigen, daß Lösungen für $\rho \approx 1$ in gewissem Sinn sehr selten auftreten [27] und daher schwierig zu finden sind.

Konstruktionen von ordinären elliptischen Kurven mit $\rho = 1$ wurden bisher für die Einbettungsgrade $k \in \{3, 4, 6\}$, $k = 10$ und $k = 12$ gefunden [31, 4, 12]. Für Konstruktionen mit $\rho > 1$ siehe beispielsweise [6, 11, 16]. Zu gegebenem k können Lösungen zu den Bedingungen 1-5 häufig in parametrisierter Form $q = q(z)$ und $\ell = \ell(z)$ für $z \in \mathbb{Z}$ angegeben werden.

Als Beispiel betrachten wir die Kurven aus [4]. Seien $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$, $t(z) = 6z^2 + 1$ und $\ell(z) = p(z) + 1 - t(z)$. Dann gilt $\phi_{12}(p(z)) \equiv 0 \bmod \ell(z)$ und $4p(z) - t(z)^2 = 3(6z^2 + 4z + 1)^2$. Die Konstruktion der zugehörigen Kurven geschieht wie folgt:

Algorithmus.

1. Finde $x \in \mathbb{Z}$, so daß $p(x)$ und $\ell(x)$ Primzahlen sind.
2. Teste $\#E(\mathbb{F}_p) = \ell(x)$ für zufällig gewählte Kurven $E : y^2 = x^3 + b$, $b \in \mathbb{F}_p$.
3. Falls der Test in Schritt 2 positiv ausfällt, gib E zurück.

Bei näherer Betrachtung fällt auf, wie erstaunlich diese Konstruktion eigentlich ist. Die berechneten Kurven erfüllen automatisch die Bedingungen 1-5 für $k = 12$, auf die Konstruktion von E mittels der Theorie der komplexen Multiplikation kann vollständig verzichtet werden. Der Test in Schritt 2 fällt nach 6 erwarteten Versuchen positiv aus, so daß der Algorithmus sehr effizient ist.

Effiziente Berechnung. Die effiziente Berechnung der Tatepaarung wurde in einigen Arbeiten untersucht, unter anderem in [15, 3, 2]. Die zur Zeit effizienteste Variante, die Atepaarung, wurde in [22] eingeführt. Wir wollen auf zwei wesentliche Aspekte dieser Paarung eingehen.

Wir betrachten die reduzierte Tatepaarung t_ℓ und die Erzeuger P, Q der Eigenräume G_1 und G_2 wie oben beschrieben. Dann kann man $t_\ell(P, Q) = f_{\ell,P}(Q)^{(q^k-1)/\ell}$ und $t_\ell(Q, P) = f_{\ell,Q}(P)^{(q^k-1)/\ell}$ zeigen. Die Paarung t_ℓ eingeschränkt auf $G_1 \times G_2$ beziehungsweise auf $G_2 \times G_1$ wird also bereits durch diese vereinfachten Ausdrücke definiert.

Es ist jedoch möglich, den Ausdruck für die Paarung im zweiten Fall weiter zu vereinfachen. Dies führt auf eine neue, bilineare und nicht ausgeartete Paarung: Sei $T = t - 1$, wobei $\#E(\mathbb{F}_q) = q + 1 - t$, und gelte $T^k \neq 1$. Die Atepaarung [22] wird durch

$$\hat{t}_\ell : G_2 \times G_1 \to \mu_\ell,$$
$$\hat{t}_\ell(Q, P) = f_{T,Q}(P)^{(q^k-1)/\ell}$$

definiert. Der wesentliche Punkt hier ist, daß die Funktion $f_{T,Q}$ den Grad $T+1$ besitzt, welcher ungefähr zwischen $\ell^{1/\phi(k)}$ und $q^{1/2}$ liegt, wohingegen der Grad der Funktionen $f_{\ell,P}$ und $f_{\ell,Q}$, die für die Tatepaarung verwendet werden, gleich $\ell \approx q$ ist. Dies führt zu einer deutlichen Effizienzsteigerung in der Berechnung der Paarung.

Mit der Theorie der Twists [40] kann der Speicheraufwand für G_2 verringert sowie eine weite-

re Effizienzsteigerung erzielt werden. Eine elliptische Kurve E' über $\mathbb{F}_q$ heißt Twist vom Grad d von E, wenn es einen Isomorphismus $\psi : E' \to E$ gibt, der über $\mathbb{F}_{q^d}$ mit d minimal definiert ist. Ist E ordinär, $k = ed$ und besitzt E einen Twist über $\mathbb{F}_{q^e}$ vom Grad $d > 1$, so können E' und ψ so gewählt werden, daß $E'(\mathbb{F}_{q^e})[\ell] = \langle \psi^{-1}(Q) \rangle$ gilt. Wir setzen dann $Q' = \psi^{-1}(Q)$, $G_2' = \langle Q' \rangle$ und erhalten die modifizierte Atepaarung

$$\hat{t}'_\ell : G_2' \times G_1 \to \mu_\ell,$$
$$\hat{t}'_\ell(Q', P) = \hat{t}_\ell(\psi(Q'), P).$$

Im Fall der oben erwähnten Kurven mit $k = 12$ aus [4] ergibt sich beispielsweise das folgende. Es gilt $E : y^2 = x^3 + b$ mit $b \in \mathbb{F}_p$ und $p \equiv 1 \bmod 6$. Seien $\lambda \in \mathbb{F}_{p^2} \backslash (\mathbb{F}_{p^2})^3$ und $\mu \in \mathbb{F}_{p^2} \backslash (\mathbb{F}_{p^2})^2$. Die Kurve $E' : \mu y^2 = \lambda x^3 + b$ ist ein Twist von E vom Grad 6 und $\psi : E' \to E$, $\psi(x, y) = (\lambda^{1/3} x, \mu^{1/2} y)$ ist der zugehörige Isomorphismus. In diesem Beispiel ist der Grad von $f_{T,Q}$ ungefähr $\ell^{1/2}$, und durch Verwendung von Q' und E' über $\mathbb{F}_{p^2}$ gegenüber Q und E über $\mathbb{F}_{p^{12}}$ ergibt sich ein um den Faktor von 6 verringerter Speicheraufwand.

5 Einsatz von CAS

Computeralgebrasysteme wie zum Beispiel Kash und Magma spielen bei der Behandlung der durch die Kryptographie aufgeworfenen mathematischen Fragestellungen aus Algebra, Zahlentheorie und algebraischer Geometrie eine bedeutende Rolle und werden als wichtiges Werkzeug für die Forschung angesehen. Die folgenden Einsatzarten und -gebiete können dabei unterschieden werden:

1. Untersuchungen von Eigenschaften mathematischer Objekte und Algorithmen, Testen von Hypothesen, interaktives Arbeiten.

2. Analyse von Algorithmen zum Lösen der kryptographischen Verfahren unterliegenden mathematischen Berechnungsprobleme.

3. Erzeugung mathematischer Objekte für kryptographische Verfahren, Implementierung von Prototypen kryptographischer Verfahren.

Die relevanten Merkmale eines Computeralgebrasystems sind dabei vor allem Funktionsumfang und Benutzerfreundlichkeit.

Im ersten und zweiten Einsatzgebiet geht es darum, mit den verschiedenen mathematischen Objekten und Algorithmen konkret arbeiten und Ideen ausprobieren zu können, da Berechnungen von Hand schnell zu aufwendig werden. Der Frage nach der Existenz weiterer parametrischer Lösungen der Bedingungen 1-5 auf Seite 4 könnte man beispielsweise in einem ersten Schritt durch eine Suche mit dem Computer nachgehen. Oder man könnte das Verhalten von neuen Algorithmen zur Berechnung des DLP untersuchen, falls diese von gewissen heuristischen Annahmen abhängen oder nur eine heuristische Laufzeitabschätzung zulassen.

Gegenüber dem ersten und zweiten spielt das dritte Einsatzgebiet wohl eher eine untergeordnete Rolle. Während der relativ große Funktionsumfang von Computeralgebrasystemen genutzt werden kann, um beispielsweise Algorithmen für die Berechnung kryptographisch geeigneter elliptischer Kurven zu implementieren, ist die Verwendung von Computeralgebrasystemen für die kryptographischen Verfahren an sich wenig sinnvoll. Hier werden in der Regel sehr spezielle, hoch optimierte und kleine Stand-alone Programme benötigt. Nichtsdestotrotz kann es hilfreich sein, diese Programme mit Hilfe von Computeralgebrasystemen auf ihre korrekte Funktionsweise hin zu überprüfen.

Literatur

[1] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), no. 2, 141–145.

[2] P. Barreto, S. Galbraith, C. O'hEigeartaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, To appear in Designs, Codes and Cryptography, 2005.

[3] P. Barreto, H. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, CRYPTO 2002.

[4] P. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, SAC 2005.

[5] D. Boneh and R. Lipton, *Algorithms for black-box fields and their application to cryptography*, CRYPTO 1996.

[6] F. Brezing and A. Weng., *Elliptic curves suitable for pairing based cryptography.*, Designs, Codes and Cryptography **37** (2005), 133–141.

[7] R. Bröker, *Constructing elliptic curves of prescribed order*, PhD Thesis, Leiden University, 2006.

[8] H. Cohen and G. Frey, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall, London, 2006.

[9] C. Diem, *The GHS-attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2002), no. 1, 1–32.

[10] ———, *On the discrete logarithm problem in elliptic curves over non-prime finite fields*, Preprint, 2004.

[11] P. Duan, S. Cui, and C. Chan, *Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems*, Preprint, 2005.

[12] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree 10*, ANTS VII.

[13] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[14] S. Galbraith, *Pairings* (book chapter), in I. Blake et al. [23].

[15] S. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate-pairing*, ANTS V.

[16] S. Galbraith, J. McKee, and P. Valenca, *Ordinary abelian varieties having small embedding degree*, CRM Barcelona, 2005.

[17] S. Galbraith and V. Rotger, *Easy decision Diffie-Hellman groups*, LMS J. Comput. Math. **7** (2004), 201–218.

[18] P. Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, Preprint, 2004.

[19] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46.

[20] F. Hess, *A note on the Tate pairing of curves over finite fields*, Arch. Math. **82** (2004), 28–32.

[21] ———, *Weil descent attacks* (book chapter), in I. Blake et al. [23].

[22] F. Hess, N. Smart, and F. Vercauteren, *The eta pairing revisited*, Accepted at IEEE Transactions on Information Theory, 2006.

[23] I. Blake, G. Seroussi, and N. Smart (eds.), *Advances in elliptic curve cryptography*, Cambridge University Press, Cambridge, 2005.

[24] A. Joux and K. Nguyen, *Separating Decision Diffie–Hellman from Diffie–Hellman in cryptographic groups*, J. Cryptology **16** (2003), 239–248.

[25] D. Kohel, *Rational groups of elliptic curves suitable for cryptography*, Progr. Comput. Sci. Appl. Logic **20** (2001), 69–80.

[26] G. Lay and H. Zimmer, *Constructing elliptic curves with given group order over large finite fields*, ANTS I.

[27] F. Luca and I. Shparlinski, *Elliptic curves with low embedding degree*, To appear in J. Cryptology, 2006.

[28] U. Maurer, *Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms*, CRYPTO 1994.

[29] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.

[30] V. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), 235–261.

[31] A. Miyaji, M. Nakabayashi, and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundamentals **E84** (2001), 1234–1243.

[32] F. Morain, *Building cyclic elliptic curves modulo large primes*, EUROCRYPT 1991.

[33] H.-G. Rück, *On the discrete logarithm in the divisor class group of curves*, Math. Comput. **68** (1999), no. 226, 805–806.

[34] K. Paterson S. Galbraith and N. Smart, *Pairings for cryptographers*, Preprint, 2006.

[35] T. Satoh, *On p-adic point counting algorithms for elliptic curves over finite fields*, ANTS V.

[36] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Commentarii Mathematici Universitatis Sancti Pauli **47** (1998), 81–92.

[37] I. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. **67** (1998), 353–356.

[38] P. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, 1994, pp. 124–134.

[39] V. Shoup, *Lower bounds for discrete logarithms and related problems*, EUROCRYPT 1997.

[40] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[41] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, J. Cryptology **12** (1999), 193–196.

[42] E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), 277–296.