Matthijs Coster
Ministerie van Defensie
Den Haag
mj.coster@mindef.nl

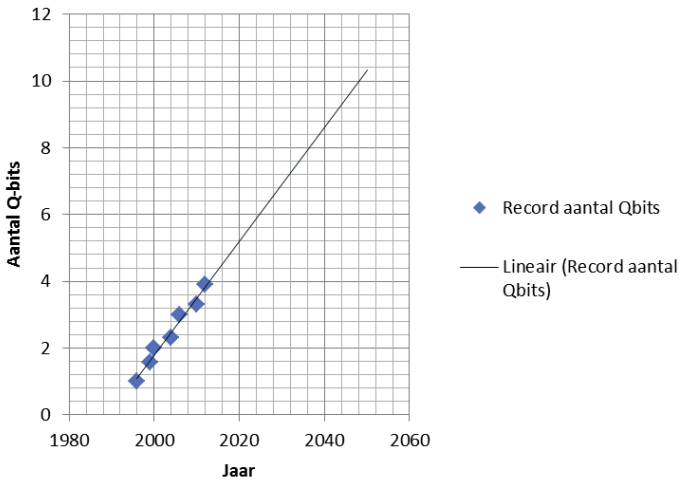
Isogenieën over supersinguliere elliptische krommen

Matthijs Coster is een wiskundig cryptologist werkzaam voor de Nederlandse overheid, maar is ook in zijn vrije tijd actief als redacteur voor het wiskundetijdschrift *Pythagoras*. In dit artikel legt Coster uit hoe een kwantumveilig cryptografisch sleuteluitwisselprogramma gebaseerd kan worden op de isogenieën van elliptische krommen.

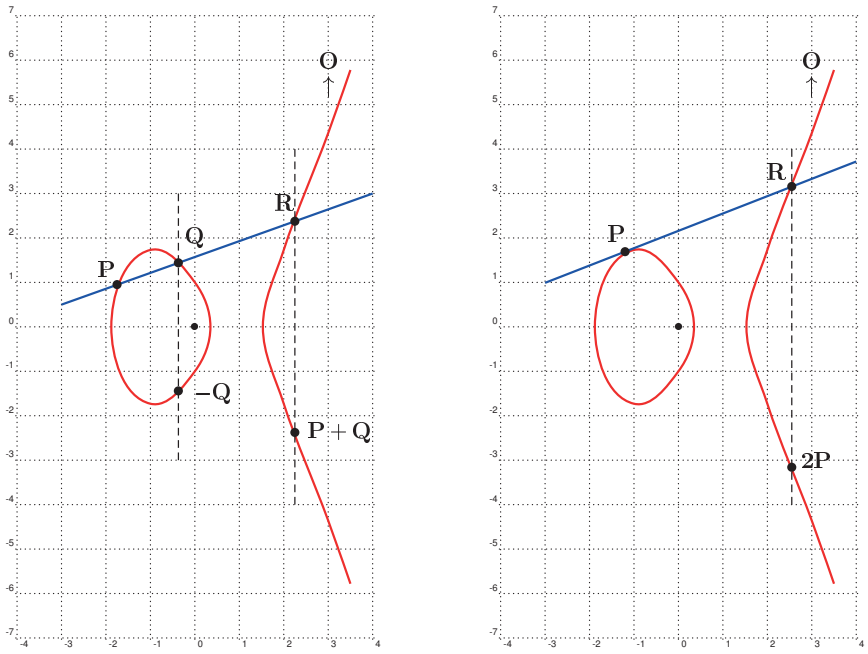
Komen de kwantumcomputers er aan? Afgelopen jaar ben ik intensief bezig geweest met onderzoek naar gevolgen van het gebruik van kwantumcomputers op de veiligheid van cryptografische producten. Bij het beveiligen van verbindingen en vooral data moet je in het hoofd houden dat als iets eenmaal is ontvreemd of geïntercepteerd, dan is dat het geval voor de eeuwigheid. Dat betekent dat als bijvoorbeeld een goed versleutelde laptop wordt ontvreemd, die plotseling met behulp van een kwantumcomputer als nog ontcijferd kan worden (mogelijk jaren na de ontvreemding), dan kan informatie op de laptop als nog worden gelezen. Als zich op de laptop data bevindt die 25 jaar geheim moet blijven, dan moet je er zeker van zijn dat dat de komende 25 jaar ook zo blijft. Er valt op het ogenblik nog niets te zeggen over wanneer de eerste kwantumcomputer in gebruik zal worden genomen. Er wordt van uitgegaan dat dat nog minimaal tien jaar gaat duren, wellicht langer, maar mogelijk is de kwantumcomputer al in gebruik genomen maar hebben we er hier in Nederland geen weet van. In Figuur 1 is een diagram te zien waarin ik een optimale lijn heb getrokken met alle recente doorbraken (jaartallen en logaritme van aantal qbits). Voor het factoriseren van een 1024-bits RSA-modulus zijn met het algoritme, ontwikkeld door Peter Shor (zie [9]) 2048 qbits nodig. Volgens het diagram zou dat pas in 2050 worden behaald. Maar een dergelijk diagram zegt natuurlijk heel weinig!

Ook andere voornamelijk publieke-sleuteluitwisselprogramma's kunnen door vergelijkbare algoritmes met een kwantumcomputer worden ontcijferd.

Kwantumcomputers kunnen extra goed worden ingezet op het moment dat er sprake is van een groep met veel structuur. Dat is het geval bij zowel RSA ($\mathbb{Z}/n\mathbb{Z}$) en de discrete logaritme over priemmachten als de discrete logaritme over elliptische krommen. ($\mathcal{E}/\mathcal{F}_q$, met q een (macht van een) priemgetal. Elliptische krommen worden genoteerd met $\mathcal{E}$. In de volgende paragraaf wordt een definitie gegeven.) Op het ogenblik zijn cryptografen op zoek naar nieuwe publieke-sleuteluitwisselprogramma's, die niet een groep met veel structuur ten grondslag hebben, dus de zogenaamde *post-kwantum*-alternatieven van RSA.



Figuur 1 Aantal qbits uitgezet tegen de tijd. Let op: voor de qbits is een logaritmische schaal gebruikt, dus lees voor 10: $2^{10} = 1024$ qbits.



Figuur 2 Optelling van P en Q op een elliptische kromme (links). Scalaire vermenigvuldiging van P met 2 op een elliptische kromme (rechts).

Onlangs schreven Dan Bernstein en Tanja Lange een overzichtsartikel waarin een aantal alternatieven wordt beschreven (zie [1]). Naast een aantal uitgebreid onderzochte alternatieven zijn de isogenieën over supersinguliere elliptische krommen minder intensief onderzocht. Het idee om isogenieën over elliptische krommen te gebruiken is oorspronkelijk voorgesteld in 2006 door Alexander Rostovtsev en Anton Stolbunov (zie [10]). Het bleek later dat er een aanpassing nodig was door een restrictie op te leggen op de elliptische krommen. Deze restrictie resulteerde in het gebruik van de *supersinguliere elliptische kromme*, maar de motivatie hiervoor noem ik in dit artikel niet. Het voorbeeld dat in dit artikel wordt besproken (conform Luca de Feo, David Jao en Jérôme Plût, zie [5]) bevat een elliptische kromme met $2^{2a}3^{2b}$ punten, met $2^a \approx 3^b \approx 2^{256}$. De discrete logaritme over een dergelijke kromme kan eenvoudig worden gebroken zonder veel rekenkracht. Er wordt vermoed dat isogenieën een vercijferingsschema kunnen opleveren dat lastig te kraken is, maar de motivatie is nog niet overtuigend.

De basis: de elliptische kromme

Voor een gedetailleerde uiteenzetting over elliptische krommen refereer ik naar Andrew Sutherland [12]. Het artikel van Henk van Tilborg uit 2001 in het *Nieuw Archief voor Wiskunde* vormt een uitstekende basis om kennis te maken met elliptische krommen en toepassingen in de cryptografie (zie [13]).

Ik ga uit van een eindig lichaam $k = \mathcal{F}_q$ (karakteristiek $p > 2$, $q = p^n$) en een elliptische kromme $\mathcal{E}/k$ kan worden gerepresenteerd door de *Weierstrass-vergelijking* $y^2 = x^3 + ax + b$, maar deze representatie kan door een willekeurige worden vervangen (bijvoorbeeld Edwards Curve). Voor het aantal punten ($\#\mathcal{E}$) geldt $|\#\mathcal{E} - (q+1)| \leq 2\sqrt{q}$ (Hasse). Vaak is duidelijk over welk lichaam k de elliptische kromme is gedefinieerd, en kan de index k worden weggelaten. Punten P en Q op de kromme kunnen worden opgeteld en scalair worden vermenigvuldigd (zie Figuur 2). We noteren de scalaire vermenigvuldiging met nP. Met $\mathrm{ord}(P)$ (de orde van P) wordt het kleinste positieve geheel getal m bedoeld zo dat $mP = O$. Uiteraard is m een deler van $\#\mathcal{E}$.

Vanzelfsprekend bestaat er dan ook een oorsprong, die ik aanduid met 0 of O en in de literatuur ook wel ∞ (*het punt op oneindig*) genoemd wordt; in *projectieve* coördinaten: $(0{:}1{:}0)$.

Isogenieën tussen de elliptische krommen

Een isogenie is een afbeelding die de onderliggende structuur behoudt (morfisme) tussen twee algebraïsche variëteiten (in ons geval elliptische krommen) die 0 afbeelden op 0. (Vergelijk dit met een homomorfisme in de algebra waarbij de eenheid van de ene groep overgaat naar de eenheid van de andere groep.)

Enkele voorbeelden van isogenieën:

- Op $\mathcal{E}$ is het altijd mogelijk om het *automorfisme* $(x,y) \to (x,-y)$ te definiëren. (In feite is dit de afbeelding $P \to -P$.)
- Voor een positief (of negatief) geheel getal m is $[m]$ (de afbeelding $P \to mP$) een *endomorfisme* van $\mathcal{E} \to \mathcal{E}$.
- Het *Frobenius* endomorfisme, meestal genoteerd met $\pi_{\mathcal{E}}$ is de afbeelding $\mathcal{E}$ die (x,y) afbeeldt op (x^q, y^q). Ik ga er niet diep op in, omdat deze afbeelding geen rol speelt bij het hier besproken sleuteluitwisselprogramma.
- *Onjuist voorbeeld:* Als Q een punt is op $\mathcal{E}$, niet de oorsprong, dan is $P \to P + Q$ een voorbeeld van een morfisme, maar niet een homomorfisme, dus geen isogenie.

De isogenie φ is in feite een functie $\overline{k} \times \overline{k} \to \overline{k} \times \overline{k}$, waarbij $\overline{k}$ de algebraïsche afsluiting is van k. Een typische φ heeft het format $\varphi(x,y) = \left(\frac{u(x)}{v(x)}, cy\left(\frac{u(x)}{v(x)}\right)'\right)$ als $\mathcal{E}$ wordt gerepresenteerd als een Weierstrass-vergelijking. (De isogenie heeft in het algemeen het format $\varphi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$. In de praktijk van dit sleuteluitwisselprogramma kunnen we bovengenoemd simpele format hanteren.) De *kern* van φ is $\{P = (x_0, y_0) \mid v(x_0) = 0\} \cup O$. De *graad* van φ is $\max\{\deg(u(x)), \deg(v(x))\}$.

Voor ons is de stelling van Tate van belang, die zegt dat als $\mathcal{E}$ en $\mathcal{E}'$ twee elliptische krommen zijn, gedefinieerd over k, en bovendien geldt $\#\mathcal{E} = \#\mathcal{E}'$, dan geldt dat er een isogenie bestaat tussen $\mathcal{E}$ en $\mathcal{E}'$. Merk op dat de groepsstructuur niet gelijk hoeft te zijn. Zo kan de ene groep isomorf zijn met $\mathbf{C}_{4N}$ en de andere groep isomorf zijn met $\mathbf{C}_{2N} \times \mathbf{C}_2$. Bovendien zegt deze stelling nog niets over hoe de isogenie eruitziet.

Een andere stelling doet de volgende uitspraak over isogenieën. Laat $\overline{k}$ de algebraïsche afsluiting van k zijn. We bekijken een isogenie $\varphi : \mathcal{E} \to \mathcal{E}'$ over $\overline{k}$. De kern van φ, de punten op $\mathcal{E}$ die op 0 van $\mathcal{E}'$ worden afgebeeld, vormt een ondergroep, zeg G. De stelling zegt nu dat er voor elke $G \subset \mathcal{E}$ een isogenie φ_G en een elliptische kromme $\mathcal{E}'$ bestaan zodanig dat $\varphi_G : \mathcal{E} \to \mathcal{E}'$ kern G heeft. Het blijkt dat de graad van de isogenie φ gelijk is aan het aantal elementen van G. De kromme $\mathcal{E}'$ wordt ook wel genoteerd als $\mathcal{E}/G$.

Het omgekeerde geldt slechts tot op zekere hoogte. Er kunnen meerdere ellip-

tische krommen $\mathcal{E}'$ bestaan zo dat de kern van de isogenie van $\mathcal{E}$ op deze krommen $\mathcal{E}'$ steeds de groep G is. Stel dat $\mathcal{E}'$ en $\mathcal{E}''$ twee dergelijke elliptische krommen zijn (met isogenieën φ en ϕ), dan geldt echter wel dat er een isomorfisme ψ bestaat, $\psi : \mathcal{E}' \to \mathcal{E}''$. In een plaatje hebben we de volgende situatie:

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\varphi} & \mathcal{E} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \psi} \\ & & \mathcal{E}'' \end{array}$$

$\mathcal{E}'$ en $\mathcal{E}''$ zijn niet identiek maar wel isomorf. Dat houdt in dat er ook een inverse bestaat, ofwel dat er een isogenie tussen $\mathcal{E}'$ en $\mathcal{E}''$ bestaat van graad 1. En dat betekent dat beide krommen dezelfde j-*invariant* hebben. De j-invariant kan eenvoudig worden berekend,

$$j(\mathcal{E}) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}.$$

Dankzij het werk van Vélu (1965) kan de isogenie φ_G expliciet worden berekend (zie bijvoorbeeld Sutherland [12, Lecture 6, p. 6]). Deze berekening is echter vrij lastig. Er zijn verbeteringen bedacht door Kohel [8] en Shumow [11] in hun proefschriften. In het kader op de volgende pagina heb ik de door Shumow opgestelde berekening van de isogenie opgeschreven. Het komt er op neer dat je een groep G formuleert (een verzameling van punten) en vervolgens voor elk van deze punten een bepaalde waarde van een bepaalde functie bij elkaar optelt. Dat betekent dat naarmate G groter wordt, de berekening lastiger wordt.

Een andere waardevolle stelling, waarop het gehele sleuteluitwisselprogramma is gebaseerd, zegt dat er een commutatieve eigenschap bestaat voor isogenieën: $\varphi_{G_A} \circ \varphi_{G_B} \cong \varphi_{G_B} \circ \varphi_{G_A}$. Ofwel, het linker- en rechterlid zijn isomorf. Mogelijk (in de praktijk zeer waarschijnlijk) gaat het om verschillende krommen, maar met gelijke j-invariant.

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\varphi_{G_A}} & \mathcal{E}/G_A \\ \downarrow{\scriptstyle \varphi_{G_B}} & & \downarrow{\scriptstyle \psi} \\ \mathcal{E}/G_B & \xrightarrow{\eta} & \mathcal{E}/\langle G_A, G_B \rangle \end{array}$$

Dit diagram blijkt commutatief. Dus door eerst $\mathcal{E}/G_A$ en vervolgens $(\mathcal{E}/G_A)/G_B$ uit te voeren verkrijgen we hetzelfde resultaat als door eerst $\mathcal{E}/G_B$ en daarna $(\mathcal{E}/G_B)/G_A$ uit te voeren.

Het sleuteluitwisselprogramma

Het basisidee van het sleuteluitwisselprogramma is dit commutatieve diagram. Het idee is dat Alice een groep G_A van een speciale vorm bepaalt en daaruit $\mathcal{E}/G_A$ berekent. Evenzo berekent Bob $\mathcal{E}/G_B$. Het idee is verder dat het voor iemand die wil afluisteren, laten we zeggen Eve, qua rekenkracht lastig is om uit $\mathcal{E}/G_A$ de groep G_A te reconstrueren, en evenzo G_B. Alice en Bob wisselen $\mathcal{E}/G_A$ en $\mathcal{E}/G_B$ uit zonder daarbij respectievelijk G_A en G_B prijs te geven. Vervolgens gaat Bob verder met $\mathcal{E}/G_A$ en bepaalt $(\mathcal{E}/G_A)/G_B$. Evenzo bepaalt Alice $(\mathcal{E}/G_B)/G_A$. Beiden vinden ze $\mathcal{E}/\langle G_A, G_B \rangle$.

Hier komen we tot de kern van het reductieprobleem. De wetenschappers die zich met de isogenie bezighouden gaan ervan uit dat Eve hier een forse uitdaging heeft, maar tot op heden is nog niet bekend tot welk probleem deze problematiek kan worden gereduceerd. (De term *reductieprobleem* wordt gebruikt om te bewijzen of een zekere vercijfering veilig is. Als $\mathcal{B}$ veilig is en je kunt bewijzen dat $\mathcal{A}$ kan worden *gereduceerd* tot $\mathcal{B}$, dan is $\mathcal{A}$ eveneens veilig.)

Keuze van p en $\mathcal{E}$

Tot nog toe is er nog niets gezegd over de karakteristiek p, en de grootte van het lichaam $\mathcal{F}_q$.

De keuze van het priemgetal is $p = \lambda \cdot \ell_A^a \cdot \ell_B^b - 1$. Hierin zijn ℓ_A en ℓ_B kleine priemgetallen en λ een kleine factor om te zorgen dat p een priemgetal wordt $\equiv 3 \bmod 4$. Verder geldt $\ell_A^a \approx \ell_B^b$. Het lichaam waarover we werken is $\mathcal{F}_{p^2}$. Dit lichaam kan worden gerepresenteerd door $\mathcal{F}_p[x]/(x^2+1) \cong \mathcal{F}_p(i)$. De elliptische kromme die gekozen wordt is $\mathcal{E} : y^2 = x^3 + 1$. Dit is een *supersinguliere* elliptische kromme. Deze $\mathcal{E}$ bevat $(p+1)^2$ punten, en in het bijzonder geldt dat $\mathcal{E} \cong (\mathbb{Z}/\ell_A^a\mathbb{Z})^2 \times (\mathbb{Z}/\ell_B^b\mathbb{Z})^2$.

Conform het voorstel van de auteurs [5], beschouw ik $\ell_A = 2$ en $\ell_B = 3$. Vanaf nu kiezen we $\lambda = 1$. Heel belangrijk is het om kennis te nemen van het feit dat het berekenen van een willekeurige isogenie weliswaar mogelijk is, maar tevens tijdrovend is. Echter door de structuur van de elliptische kromme en enige kennis van G kan de isogenie aanzienlijk eenvoudiger worden berekend. Zonder in details te treden poneer ik hier dat als $\#G = 2^u 3^v$, dan zijn er u isogenieën φ_i van graad 2 en v isogenieën ϕ_j van graad 3, zodanig dat $\varphi_G = \varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \cdots \circ \varphi_u \circ \phi_1 \circ \phi_2 \circ \phi_3 \circ \cdots \circ \phi_v$, hetgeen het rekenwerk aanzienlijk reduceert.

In concreto

We laten zien hoe Alice en Bob samen een gemeenschappelijke sleutel kunnen construeren die niet door een buitenstaander gevonden kan worden.

1. Kies een priem p van de vorm $p = 2^a \cdot 3^b - 1$, waarbij $2^a \approx 3^b$, en $p \equiv 3 \bmod 4$.
2. Het lichaam waarover we werken is $\mathcal{F}_{p^2}$. Dit lichaam kan worden gerepresenteerd door $\mathcal{F}_p[x]/(x^2+1) \cong \mathcal{F}_p(i)$.
3. Er geldt $\mathcal{E} \cong (\mathbb{Z}/2^a\mathbb{Z})^2 \times (\mathbb{Z}/3^b\mathbb{Z})^2$. Kies punten $\mathsf{P}_A, \mathsf{Q}_A, \mathsf{P}_B, \mathsf{Q}_B$ zodanig dat $\mathrm{ord}(\mathsf{P}_A) = \mathrm{ord}(\mathsf{Q}_A) = 2^a$, $\mathrm{ord}(\mathsf{P}_B) = \mathrm{ord}(\mathsf{Q}_B) = 3^b$ en $\mathcal{E}$ wordt precies voortgebracht door $\mathsf{P}_A, \mathsf{Q}_A, \mathsf{P}_B$ en Q_B.
4. Alice kiest random m_A en $n_A \in \{1, \ldots, 2^a\}$ en berekent $R_A = m_A \cdot \mathsf{P}_A + n_A \cdot \mathsf{Q}_A$. G_A is de groep die wordt voortgebracht door R_A. De groep G_A impliceert de isogenie φ_{G_A}. Alice berekent $\mathsf{P}_{(A)B} = \varphi_{G_A}(\mathsf{P}_B)$, $\mathsf{Q}_{(A)B} = \varphi_{G_A}(\mathsf{Q}_B)$ en $\mathcal{E}_A \cong \mathcal{E}/G_A$ met behulp van isogenieën. Merk op dat de isogenie φ_{G_A} lastig te berekenen is als G_A groot is.
5. Alice maakt $\mathsf{P}_{(A)B}$ en $\mathsf{Q}_{(A)B}$ bekend, ten behoeve van Bob.
6. Bob idem m_B, n_B, R_B, G_B, $\mathsf{P}_{(B)A}$, $\mathsf{Q}_{(B)A}$, $\mathcal{E}_B$.
7. Alice ontvangt $\mathsf{P}_{(B)A}$ en $\mathsf{Q}_{(B)A}$ van Bob. Zij vervolgt haar berekening. Ze berekent eerst $R_{(B)A} = m_A \cdot \mathsf{P}_{(B)A} + n_A \cdot \mathsf{Q}_{(B)A}$. Laat $G_{(B)A}$ de groep zijn voortgebracht door $R_{(B)A}$. Deze groep impliceert een isogenie, zeg $\varphi_{G_{(B)A}}$. Vervolgens kan zij $\mathcal{E}_{(B)A} \cong \mathcal{E}_A/G_{(B)A}$ bepalen. Ten slotte bepaalt Alice $j_{(B)A}$.
8. Bob idem $R_{(A)B}$, $G_{(A)B}$, $\varphi_{G_{(A)B}}$, $\mathcal{E}_{(A)B}$, $j_{(A)B}$.
9. Aangezien

   $$\mathcal{E}_{(B)A} \cong \mathcal{E}_A/G_{(B)A} \cong \mathcal{E}_B/G_{(A)B} \cong \mathcal{E}_{(A)B}$$

   volgt $j = j_{(B)A} = j_{(A)B}$.

De in stap 9 gevonden j kan worden gebruikt als een sleutel voor een geheim sleuteluitwisselprogramma.

Afmetingen sleuteluitwisselprogramma

In de cryptografie is het gebruikelijk om aan te geven hoe veilig je programma is. Andere cryptografen kunnen dit vergelijken met andere programma's. Het gaat veel te

ver om deze veiligheid nauwkeurig toe te lichten, maar belangrijk is vooral dat je nagaat hoeveel rekenkracht een aanvaller van het systeem nodig zal hebben. 128 bits houdt in dat de aanvaller hooguit 2^{128} mogelijkheden moet nagaan. Voor de isogenieën over supersinguliere elliptische krommen suggereren de auteurs [5] voor een veiligheid van 128 bits de volgende keuzes van p, a en b:

- $p = 2^a \cdot 3^b - 1 \approx 2^{512}$.
- In het geval dat $\mathcal{E}$ een supersinguliere elliptische kromme is, geldt $\#\mathcal{E} = 2^{2a} \cdot 3^{2b} \approx 2^{1024}$.
- Het totaal aantal isomorfie-klassen van supersinguliere elliptische krommen is $\frac{p+1}{12} = 2^{a-2} \cdot 3^{b-1} \approx 2^{508}$.

Het begrip kwantumveiligheid is gerelateerd aan de veiligheid nadat ook aanvallers in het bezit zijn van kwantumcomputers. Kunnen deze aanvallers efficiënter een programma aanvallen met een kwantumcomputer? Dit is een uitermate interessant onderwerp, maar ongeschikt om hier even te behandelen.

Voor de kwantumveiligheid van 128 bits suggereren de auteurs $p \approx 2^{768}$ (en daarmee groeien ook a en b). Een sleuteluitwisseling zou kunnen worden uitgevoerd in 50 ms op een simpele computer.

Algoritme van Vélu

We gaan hier uit van de elliptische kromme $\mathcal{E}: y^2 = x^3 + ax + b$. Tevens is er een groep $G \subset \mathcal{E}$ gegeven. We bepalen nu de elliptische kromme $\mathcal{E}': y^2 = x^3 + Ax + B$, zodanig dat $\mathcal{E}' = \mathcal{E}/G$. Als deze isogenie wordt weergegeven met ϕ, dan wordt tevens het beeld van een punt $P \in \mathcal{E}$, $\phi(P) \in \mathcal{E}'$ bepaald. U zult zien dat het rekenwerk enorm zal toenemen naarmate $|G|$ groeit.

Zij gegeven $G \subset \mathcal{E}$ een groep en $P \in \mathcal{E}$ een punt.

Stap 1. We splitsen G op in vier deelverzamelingen:

$$G = \{0\} \cup C_2 \cup R^+ \cup R^-.$$

Hierin is 0 de oorsprong (punt op oneindig), C_2 de 2-torsiepunten, ofwel punten T met $2T = 0$. Voor R^+ en R^- geldt dat de punten in deze verzamelingen tegengestelde y-coördinaat hebben. Het maakt niets uit hoe de verdeling wordt gemaakt, want uiteindelijk wordt alleen gebruik gemaakt van y^2. Laat $S = C_2 \cup R^+$.

Stap 2. Zij $Q = (x_Q, y_Q) \in S$.

$$\begin{aligned} g_Q^x &= 3x_Q^2 + a, \\ g_Q^y &= -2y_Q, \\ u_Q &= \left(g_Q^y\right)^2, \\ v_Q &= \begin{cases} g_Q^x Q \in C_2, \\ 2g_Q^x Q \in R^+. \end{cases} \end{aligned}$$

Stap 3. Sommeer voor alle $Q \in S$:

$$\begin{aligned} v &= \sum_{Q \in S} v_Q, \\ w &= \sum_{Q \in S} u_Q + x_Q v_Q. \end{aligned}$$

Stap 4. Bepalen van $\mathcal{E}' = \mathcal{E}/G$:

$$\begin{aligned} A &= a - 5v, \\ B &= b - 7w. \end{aligned}$$

Er geldt: $\mathcal{E}': Y^2 = X^3 + AX + B$.

Stap 5. Ten slotte bepalen we $\varphi_G(P) = (X, Y)$. Er geldt:

$$\begin{aligned} X &= x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2} \right), \\ Y &= y - \sum_{Q \in S} \left(\frac{2yu_Q}{(x - x_Q)^3} + \frac{v_Q(y - y_Q)}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right). \end{aligned}$$

(bron: proefschrift van Shumow [11, p. 32])
Voor de Sage-gebruiker is het niet nodig om deze formules zelf te implementeren. De v en w in stap 3 zijn te bepalen met respectievelijk `EllipticCurveIsogeny__v` en `EllipticCurveIsogeny__w`.

Referenties

1 Daniel Bernstein en Tanja Lange, Post-quantum cryptography – dealing with the fallout of physics success (2017), eprint.iacr.org/2017/314.pdf.

2 Denis Charles, Eyal Goren en Kristin Lauter, cryptographic hash functions from expander graphs (2006), eprint.iacr.org/2006/021.pdf.

3 Christina Delfs en Steven Galbraith, Computing isogenies between supersingular elliptic curves over $\mathcal{F}_p$ (2013), arXiv/1310.7789.

4 Luca de Feo, Cyril Hugounenq, Jérôme Flût, en Éric Schost, Explicit isogenies in quadratic time in any characteristic (2016), arXiv/1603.00711.

5 Luca de Feo, David Jao en Jérôme Flût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, PQCrypto 2011, *Journal of Mathematical Cryptology*, 8(3) (2014) 209–247.

6 Steven Galbraith en Anton Stolbunov, Improved algorithm for the isogeny problem for ordinary elliptic curves (2011), arXiv/1105.6331.

7 David Jao, Isogenies in a quantum world (Slides), ecc2011.loria.fr/slides/jao.pdf.

8 David Kohel, Endomorphism rings of elliptic curves over finite fields (1989), echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf.

9 John Proos en Christof Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves (2003), arXiv.quant-ph/0301141.

10 Alexander Rostovtsev en Anton Stolbunov, Public-key cryptosystem based on isogenies (2006), eprint.iacr.org/2006/145.pdf.

11 Daniel Shumow, *Isogenies of Elliptic Curves, a Computational Approach*, thesis, 2009.

12 Andrew Sutherland, Elliptic Curves, college-dictaten, ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes, 2015.

13 Henk van Tilborg, Elliptic curve cryptosystems; too good to be true?, *Nieuw Archief voor Wiskunde* 5/2(3) (2001), 220–225.