Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Samenvatting

Cryptografie gaat over het beveiligen van informatie op een manier waarop alleen de beoogde personen toegang hebben tot die informatie. Stel, bijvoorbeeld, dat een hypothetische persoon, genaamd Alice, een privébericht zou willen sturen naar een andere hypothetische persoon, genaamd Bob. Als Alice en Bob een manier hadden om te communiceren zodat niemand hen zou kunnen afluisteren, dan zou dat makkelijk zijn; ze zouden hun berichten onversleuteld kunnen overbrengen. In de echte wereld is een perfect veilige communicatieverbinding echter vrijwel onmogelijk te garanderen, zeker wanneer communicatie over het internet gebeurt. Alice en Bob zouden dus op een bepaalde manier een soort codetaal moeten afspreken. Maar hoe kunnen ze dat doen, als we aannemen dat kwaadwillende personen al hun communicatie kunnen afluisteren? Eén manier, is met een zogeheten *Diffie–Hellman sleuteluitwisseling*; een methode voor twee partijen om een gezamenlijk geheim af te spreken over een publiek kanaal. Een gangbare manier, toegepast door veel applicaties die gebruik maken van *begin-tot-eind*-versleuteling, is gebaseerd op wiskundige objecten genaamd *elliptische krommen*. Een voorbeeld van een elliptische kromme is de verzameling van punten (x, y) in het vlak die voldoen aan de vergelijking $y^2 = x^3 + 3x^2 - x - 3$; zie Figuur 9.1.

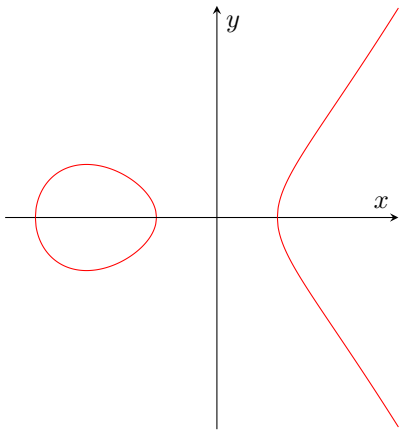

Figure 9.1: Een elliptische kromme gegeven door $y^2 = x^3 + 3x^2 - x - 3$.

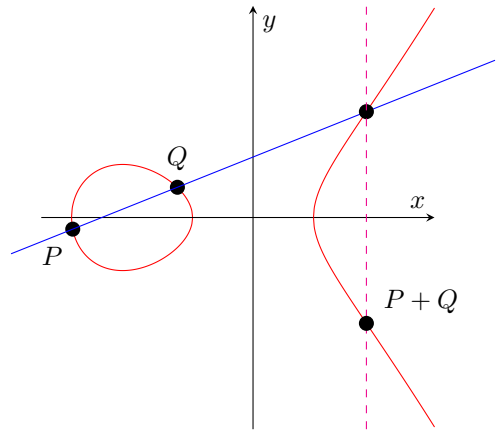

Figure 9.2: Het optellen van twee punten op een elliptische kromme.

Wat elliptische krommen zo speciaal maakt, is dat er een meetkundig recept bestaat om punten op de kromme op te tellen: Stel bijvoorbeeld, dat we twee punten op de kromme, zeg P en Q, zouden willen optellen. We tekenen dan eerst de lijn door P en Q.

Het blijkt dat deze de kromme in precies één ander punt zal snijden.[2] De verticale lijn door dit laatste punt snijdt de kromme weer precies in één ander punt, wat we $P+Q$ noemen; de som van P en Q. In het geval dat $P = Q$, dan definiëren we "de lijn door P en Q" als de raaklijn aan de kromme in P. Op deze manier hebben we een methode om $n \cdot P = \underbrace{P + P + \ldots + P}_{n \text{ keer } P}$ voor elk geheel getal $n > 0$ uit te rekenen. Grote zulke veelvouden kunnen overigens met minder dan $n-1$ optellingen uitgerekend worden, door een methode genaamd *double-and-add* (Engels voor "verdubbelen en optellen"). Zo kunnen we bijvoorbeeld $20 \cdot P$ uitrekenen als $20 \cdot P = 2 \cdot (2 \cdot ((2 \cdot (2 \cdot P)) + P))$, wat slechts vijf optellingen kost (waarvan vier een verdubbeling zijn; i.e. een punt optellen bij zichzelf). Nu, als Alice en Bob een elliptische kromme willen gebruiken om een gezamenlijk geheim vast te stellen, dan kan dit als volgt.

(i) Alice en Bob spreken, in het openbaar, een punt P op een elliptische kromme af.

(ii) Alice en Bob genereren (grote) geheime gehele getallen a en b.

(iii) Alice rekent het punt $P_A = a \cdot P$ uit, en stuurt het resultaat naar Bob.

(iv) Bob rekent het punt $P_B = b \cdot P$ uit, en stuurt het resultaat naar Alice.

(v) Met behulp van haar geheim en het punt van Bob, berekent Alice $a \cdot P_B = (a \cdot b) \cdot P$.

(vi) Met behulp van zijn geheim en het punt van Alice, berekent Bob $b \cdot P_A = (a \cdot b) \cdot P$.

Aangezien Alice en Bob op hetzelfde punt op de elliptische kromme uitkomen, hebben ze successvol een gezamenlijk geheim vastgesteld; dat wil zeggen, de *sleuteluitwisseling* is voltooid. Deze gezamenlijke sleutel kan vervolgens gebruikt worden om beveiligde berichten naar elkaar te sturen.

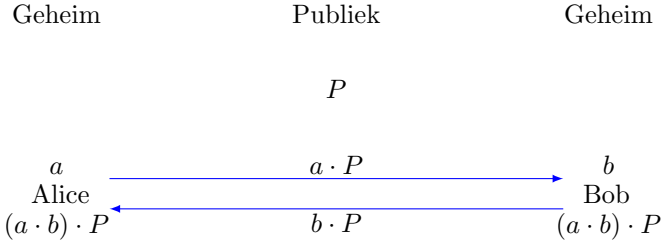

Figure 9.3: Een "Elliptic Curve Diffie–Hellman" sleuteluitwisseling.

De veiligheid van dit protocol steunt op de aanname dat het onmogelijk is om Alice' geheim a vast te stellen uit alleen de publieke informatie van P en $a \cdot P$. Dit heet het *discretelogaritmeprobleem*. Theoretisch gesproken zou het weliswaar mogelijk zijn om

[2] Tenzij de lijn door P en Q verticaal is; dan zeggen we dat $P + Q = O$, waar O het *punt op oneindig* heet. Als de lijn de kromme in één van de punten raakt, dan tellen we dat snijpunt dubbel. Op die manier is "de lijn door P en P" gelijk aan de raaklijn aan de kromme in P.

a uiteindelijk te vinden door $2 \cdot P = P + P$, $3 \cdot P = P + P + P$, $4 \cdot P = P + P + P + P$, enzovoorts, uit te rekenen totdat we $a \cdot P$ tegenkomen, maar dit is praktisch niet haalbaar zodra a heel groot is. Al deze punten nagaan duurt namelijk veel langer dan $a \cdot P$ te berekenen, gegeven a en P, met behulp van de *double-and-add*-methode. Tot op heden zijn er geen snelle algoritmes bekend om het discretelogaritmeprobleem in het algemeen op te lossen. Alhoewel, tenzij we *kwantumcomputers* in beschouwing nemen. Een kwantumcomputer is een speciaal soort computer die zijn rekenkracht baseert op de merkwaardige eigenschappen van subatomaire deeltjes. Op zulke computers bestaan er wél snelle algoritmes die het discretelogaritmeprobleem kunnen kraken. Zo ver we weten, is nog niemand in staat geweest een kwantumcomputer te bouwen die krachtig genoeg is om hedendaagse cryptografie te breken, maar het is onduidelijk of dit in de toekomst wel mogelijk zal zijn. Dit heeft een nieuw vakgebied in het leven geroepen genaamd *post-kwantum cryptografie*. Deze onderzoeksrichting gaat over het zoeken en analyseren van manieren om informatie te versleutelen die veilig zijn tegen aanvallen van kwantumcomputers. *Isogenie-gebaseerde cryptografie* is een deelgebied van deze onderzoeksdiscipline. Isogenieën zijn afbeeldingen tussen elliptische krommen; een soort vervorming die je van de ene elliptische kromme naar de andere brengt. Wanneer je deze vervormingen op een slimme manier kiest, kan je een sleuteluitwisselingsprocedure maken dat erg op het voorgaande protocol lijkt. Voor zo'n procedure beginnen Alice en Bob met het afspreken van een publiek bekende elliptische kromme, maar in plaats van een punt op die kromme te nemen, passen ze nu (geheime) vervormingen toe op de elliptische kromme zelf. Als ze dit doen op een zodanige manier dat de volgorde van hun vervormingen niet uitmaakt, eindigen ze samen met dezelfde elliptische kromme, wat vervolgens hun gedeelde geheim uitmaakt. Een abstracte weergave van dit protocol vindt je in Figuur 9.4

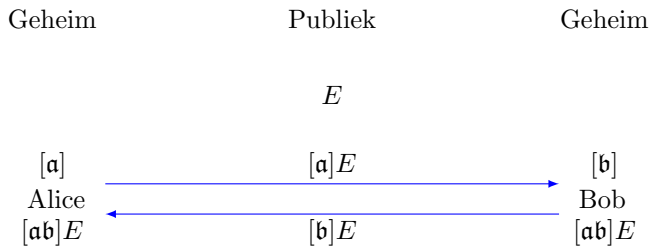

Figure 9.4: Een isogenie-gebaseerde sleuteluitwisseling.

De onderliggende aanname van isogenie-gebaseerde cryptografie is dat het lastig is om, gegeven twee elliptische krommen E_1 en E_2, een vervorming te vinden van die je van E_1 naar E_2 brengt. Dit heet ook wel het *isogenie-pad-probleem*. Men gaat ervan uit dat dit probleem zelfs voor kwantumcomputers lastig is.

In dit proefschrift beschouwen we verschillende computationele problemen die aan isogenieën tussen elliptische krommen kunnen worden toegekend.

Hoofstukken 1, 2, en 3 zijn inleidend en eindigen met een vereenvoudigd overzicht van de hoofdresultaten uit de latere hoofdstukken.

In Hoofdstuk 4 en 5 tonen we aan dat, in zekere instanties, afbeeldingen op elliptische krommen genaamd *pairings* gebruikt kunnen worden om bepaalde computationele moeilijkheidsaannames te weerleggen. Zo vinden we in speciale gevallen efficiënte oplossingen voor het isogenie-pad-probleem, evenals voor een zwakker probleem genaamd het *Diffie–Hellman Beslissingsprobleem*.

In Hoofdstuk 6 ontwikkelen we een meervariabele veralgemening van *Hilbert klassenpolynomen*; veeltermen die elliptische krommen met een bepaalde structuur (gegeven door hun *endomorfismering*) beschrijven. We gaan in het bijzonder in op de computationele voordelen van deze nieuwe veeltermen ten opzichte van eerder bekende klassenpolynomen.

In Hoofdstuk 7 bestuderen we een methode om ketens van isogenieën efficiënt uit te rekenen met behulp van vergelijkingen genaamd *radicale-isogenie-formules*. We ontwikkelen een nieuwe methode om zulke formules uit te rekenen, en verbeteren de efficiëntie van hun evaluatie. Dit zorgt voor een versnelling in het uitvoeren van bepaalde isogenie-gebaseerde protocollen.