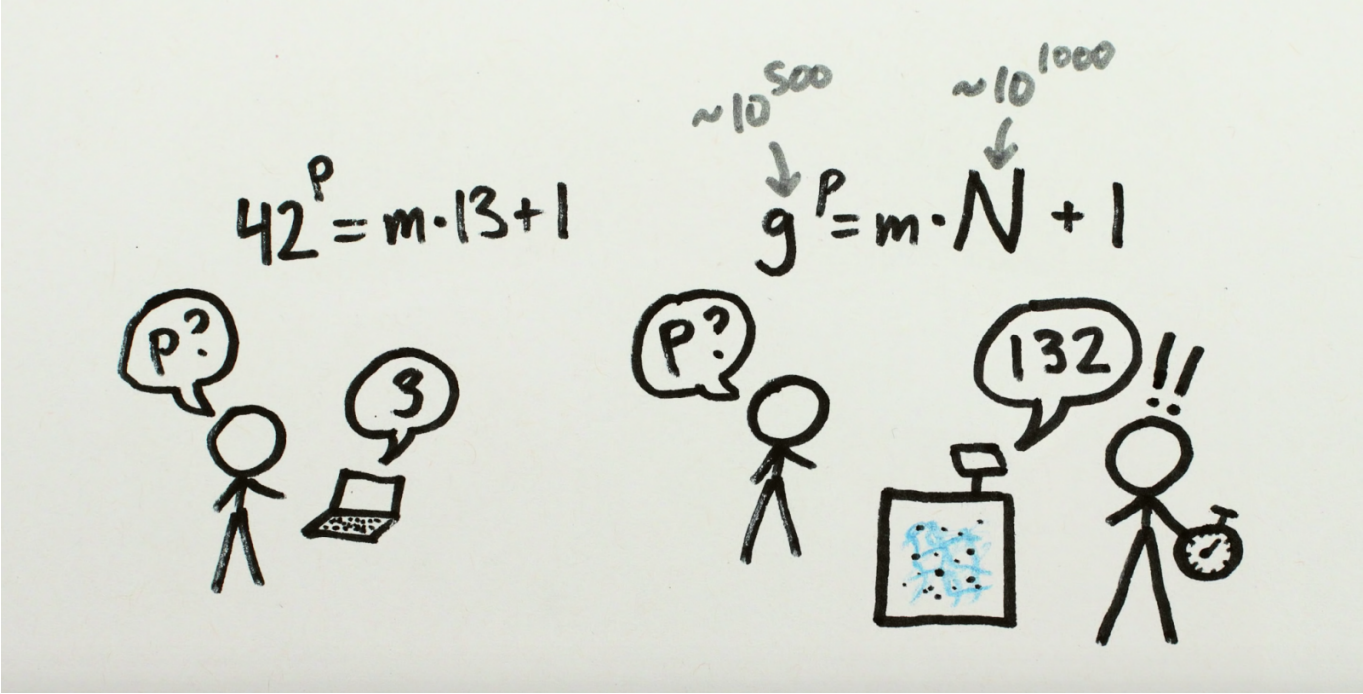
Quantumencryptie: Shors algoritme

Quantumcomputers zijn erg goed in het factoriseren van grote getallen – een eigenschap die bijvoorbeeld gebruikt kan worden om geheime versleutelingen van berichten te kraken. De slogan is: “een quantumcomputer kan alle factoren tegelijk proberen en zo de juiste vinden”. Maar hoe werkt dit nu precies, en vooral: hoe kiest de quantumcomputer de juiste factor? Hier blijkt een ingenieuze wiskundige truc voor nodig te zijn: Shors algoritme. YouTubekanaal MinutePhysics maakte twee mooie videos waarin dit algoritme wordt uitgelegd.



Het RSA-protocol is een voorbeeld van een versleutelingsprincipe dat veel banken en websites gebruiken om op een veilige manier informatie van en naar klanten te sturen. Over hoe dat protocol precies werkt, zullen we het hier niet hebben (zie bijvoorbeeld deze pagina voor een uitleg), maar het principe dat aan de basis ervan ligt is eenvoudig: het is veel gemakkelijker om grote getallen te vermenigvuldigen dan om delers van grote getallen te vinden. Zo kost het weinig moeite om uit te rekenen dat 137 x 541 gelijk is aan 74117, maar

probeer als je het antwoord nog niet weet maar eens uit te vinden wat de delers van 74117 zijn! Dit verschil in complexiteit wordt gebruikt om berichten te versleutelen: grofweg wordt voor encryptie het grote getal gebruikt, maar voor decryptie de losse factoren – en dus is de boodschap veilig voor wie die factoren niet kent.

De details zijn nog iets subtieler – zie de bovenstaande link voor meer informatie – maar feit is: wie snel grote getallen in delers kan ontbinden, kan berichten gemakkelijk ontsleutelen. Nu hoor je vaak zeggen dat juist factoriseren – delers vinden, dus – iets is waar quantumcomputers erg goed in zijn. (Zie bijvoorbeeld de serie artikelen van Joris Kattemölle over quantumcomputers voor meer over dit onderwerp.) Waar een gewone computer namelijk met één getal tegelijk kan rekeken, kan een quantumcomputer dat met heel veel getallen tegelijk. In de quantumwereld kun je immers superposities van verschillende toestanden maken, en kun je dus een input gebruiken die “een beetje 1, een beetje 2, een beetje 3, …” enzovoort is. Daarmee kun je een getal dus gelijktijdig door alle mogelijke getallen delen!

De bovenstaande beschrijving klopt in grote lijnen, maar de grote vraag is: wat doe je nadat de quantumcomputer door alle verschillende getallen gedeeld heeft? Je kunt ook een superpositie namelijk maar één keer aflezen, en je krijgt dan het antwoord van een van de vele mogelijke deeltoestanden. Als je dus 74117 door alle getallen van 1 t/m 74117 zou delen, en vervolgens aan de quantumcomputer een uitkomst vraagt, is de kans groot dat die computer zegt “74117 is niet deelbaar door 367”, of iets dergelijks, en niet “74117 is wél deelbaar door 137”.

Om dit te voorkomen, wil je dus het liefste dat de quantumcomputer alle zinloze antwoorden “vergeet” en je alleen de zinvolle antwoorden kan geven. Maar dat blijkt nog niet zo eenvoudig! Er is een slimme wiskundige truc voor nodig die bekend staat als Shors algoritme (naar de ontdekker, Peter Shor), en die bij uitstek geschikt is om op een quantumcomputer te implementeren.

Omdat Shors algoritme de nodige ingewikkelde details bevat, wordt de beschrijving ervan vaak weggelaten uit populairwetenschappelijke verhandelingen over quantumcomputers. Maar gelukkig is er in dergelijke gevallen het prachtige YouTubekanaal MinutePhysics, waarop Henry Reich aan de hand van mooie animaties juist dit soort dieper gaande details

uitlegt. Recent maakte Reich twee video’s waarin hij Shors algoritme uitlegt – wil je dus écht weten hoe een quantumcomputer codes kan kraken, kijk dan vooral de onderstaande twee filmpjes!