Publicatie : Bits&Chips
Datum : 22 jun 2018
cm2 : 1.125
Pagina : 41
Advertentiewaarde : € 6.120,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 6.500

ACHTERGROND
BEVEILIGING

Op zoek naar quantumbestendige cryptografie

De quantumcomputer zal – als die ooit wordt gebouwd – een belangrijk fundament wegslaan onder de beveiligde communicatie die we elke dag gebruiken. Cryptografen haasten zich daarom nieuwe methodes te ontwikkelen. Maar er is nog een lange weg te gaan.

Pieter Edelman

Niemand verwacht dat er binnen een decennium een bruikbare quantumcomputer zal zijn. Toch hebben cryptografen haast met het ontwikkelen van nieuwe methodes die weerstand kunnen bieden aan quantumrekenaars. Zo is de Internet Engineering Task Force (IETF) druk bezig om het quantumbestendige XMSS-protocol te standaardiseren en heeft Google bij wijze van experiment al het Newhope-cryptosysteem in zijn Chrome-browser opgenomen. En ondertussen zijn alle ogen in de cryptogemeenschap gericht op de zoektocht die het Amerikaanse Nist-agentschap heeft afgetrapt.

'Ik denk dat we eigenlijk eerder hadden moeten beginnen', zegt Léo Ducas van het Centrum voor Wiskunde en Informatica (CWI). Hij is een van de auteurs van Newhope, samen met Peter Schwabe van de Radboud Universiteit, Thomas Pöppelman van Infineon en Erdim Alkim van de Turkse Ege Universiteit. 'We beginnen nu net met het standaardisatieproces, en je kijkt tegen iets van vijf jaar van *scrutiny* aan voordat je de eerste standaarden hebt. Dan zit je nog met de tijd om het te implementeren en alle servers te upgraden ... dat kost gigantisch veel tijd.'

Vooral dat laatste is een heikel punt, zo bleek eerder bij de md5-hashfunctie. Onderzoekers raadden al in 1996 af om het algoritme nog langer te gebruiken, en uiteindelijk werd de methode in 2009 definitief verpulverd. Maar de functie bleef nog jaren in gebruik. 'In 2012 kon de befaamde Flame-malware nog profiteren van een kwetsbaarheid in md5', vertelt Schwabe, een van de andere Newhope-auteurs. 'Terwijl er een opvolger was die zich vrijwel hetzelfde gedroeg en als directe vervanger gebruikt kon worden. Het blijkt bijzonder lastig om van een gevestigde methode af te komen.'

Er is bovendien een andere, fundamentelere reden om haast te maken: dingen die vandaag versleuteld worden, moeten ook morgen nog onleesbaar zijn. 'Er wordt best veel getwijfeld aan de haalbaarheid van een quantumcomputer, maar je kunt er simpelweg niet op gokken dat het de komende dertig jaar niet gaat lukken om er een te bouwen', zegt Schwabe. 'Sommige gebruikers moeten ervan op aankunnen dat hun crypto tijdens hun leven niet gekraakt wordt. Denk aan Chinese dissidenten die met mensen buiten het land communiceren. Hun communicatie moet over twintig jaar nog veilig zijn, ook voor een tegenstander die nu alles onderschept.'

Rfid-tags

Het probleem van de quantumcomputer is niet zozeer de 'normale' symmetrische cryptografie, maar de asymmetrische of publieke-sleutelcryptografie (*public key cryptography* of pkc, zie kader 'Asymmetrische cryptografie'). De methode is een van de hoekstenen waarop onze communicatiemaatschappij is gebouwd. Zonder pkc zouden twee partijen nooit veilig kunnen

Léo Ducas

Publicatie : Bits&Chips
Datum : 22 jun 2018
cm2 : 1.125
Pagina : 41
Advertentiewaarde : € 6.120,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 6.500

communiceren als ze elkaar niet eerder hebben ontmoet – en probeer dan maar eens als nieuwe bezoeker op een beveiligde website te komen. Pkc is ten eerste nodig om te verifiëren dat de andere partij wel echt is wie hij zegt te zijn (zie kader 'Keten van vertrouwen'), en vervolgens ook nog om de daadwerkelijke versleuteling te verzorgen.

Maar het concept van de quantumcomputer lijkt wel gemaakt te zijn om juist pkc te kraken. Op dit moment worden er twee (gerelateerde) wiskundige problemen ingezet voor pkc: ontbinden van grote getallen en discrete logaritmes. In 1994 toonde Peter Shor van het MIT aan dat juist die twee problemen efficiënt opgelost kunnen worden met een quantumcomputer. 'Het is zelfs een van de weinige dingen waarin een quantumcomputer beter is dan een klassieke', zegt Ducas. 'Dat komt ook wel doordat we nog aan het leren zijn hoe we quantumalgoritmes moeten ontwerpen, maar je ziet zelden zo'n groot verschil.'

Toch kwam de zoektocht naar een vervanger niet direct op stoom. En dat terwijl cryptografen al sinds de jaren zeventig met ideeën spelen voor quantumcomputerbestendige pkc. De belangrijkste reden is dat de nieuwe methodes allemaal inboeten op snelheid en vooral sleutelgrootte. 'Bij de huidige asymmetrische methodes kun je sleutels zo klein maken als 32 bytes, maar met quantumbestendige cryptografie kan dat zo een megabyte worden. Dat is bij de meeste methodes het voornaamste probleem', stelt Schwabe. 'Hoewel er natuurlijk ook methodes zijn die groot én traag zijn.'

Of dat ook in de praktijk een probleem is, hangt natuurlijk af van de situatie. Een megabyte extra downloaden klonk in de jaren negentig een stuk schrikbarender dan nu. Maar ook embedded devices moeten ermee overweg kunnen. 'De wat krachtigere devices hebben wel een geheugen waar dat soort sleutels in passen, maar als je het over rfid-tags hebt, dan heb je wel een probleem', zegt Schwabe.

Interne toestand

Bovendien ligt, anders dan bij het md5-voorbeeld, een directe vervanger van de huidige methodes niet echt voor de hand. 'We zouden kunnen kijken wat er uit de Nist-competitie komt en proberen dat te verwerken in de huidige protocollen, maar het is waarschijnlijk logischer om het hele protocol te heroverwegen. Dan hou je waarschijnlijk iets beters over', denkt Schwabe.

Hash-gebaseerde handtekeningen, een van de denkrichtingen voor postquantumcrypto, zijn een mooi voorbeeld (zie 'Hash-gebaseerd ondertekenen'). Die aanpak is redelijk efficiënt te implementeren met een beperkte overhead. Maar daarvoor gebruikt het algoritme wel een interne toestand. 'Elke keer dat je ondertekent, moet je je geheime sleutel updaten', legt Schwabe uit. 'Dat op zich is niet moeilijk, maar je krijgt allerlei problemen met het herstellen van oude sleutels uit een backup, of als twee servers met dezelfde sleutel moeten ondertekenen.'

Daar staat tegenover dat de veiligheid van eenmaal ondertekende stukken niet in het geding komt als de geheime sleutel ooit wordt buitgemaakt. Vandaar dat cryptografen toch wel met enthousiasme naar de aanpak kijken. 'Je krijgt er interessante aanvullende security-eigenschappen voor terug', verklaart Schwabe, 'maar als directe vervanger van de huidige methodes kun je het niet inzetten.'

Puur fantasie

Zonder echte noodzaak bleef al het werk rond postquantumcrypto tot nog toe dus vooral academisch. Schwabe: 'Stel je voor dat je zegt tegen iemand die een daadwerkelijk systeem moet onderhouden: wat zou je ervan vinden om iets in te zetten dat ordegroottes groter is én potentieel ook nog veel trager. En als hij zou vragen waarom, zou je zeggen: nou, quantumcomputers. Voor de meeste mensen was dat tot voor kort puur fantasie.'

Hier en daar wordt er wel in de praktijk geëxperimenteerd met quantumbestendige crypto – als aanvulling overigens op reguliere cryptografie. Google's Chrome dus, en verschillende beveiligingsproducten. 'Het zou me ook niks verbazen als Whatsapp of Signal early adopters zijn, want ze hebben een protocol dat ze volledig beheren. Maar als je moet communiceren met devices die

Asymmetrische cryptografie

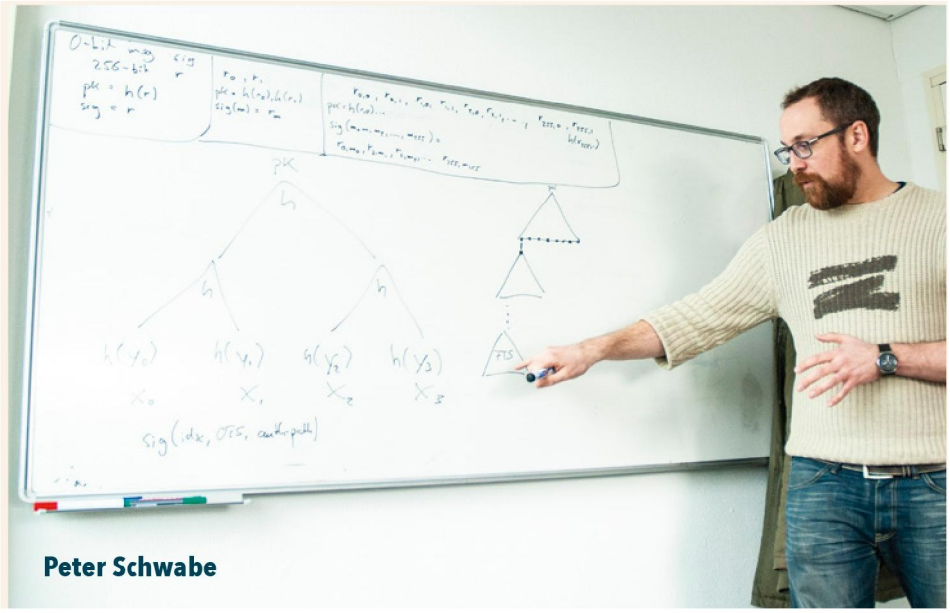
Er zijn twee 'smaken' binnen de cryptologie: symmetrisch en asymmetrisch. De symmetrische variant is de intuïtieve vorm van cryptografie: net als dat je in de fysieke wereld een sleutel hebt waarmee je iets op slot kunt doen en ook weer open kunt maken, kun je met een cryptografische sleutel een stukje data onleesbaar maken en ook weer leesbaar. Het goede nieuws: quantumcomputers hebben weinig vat op deze variant – hooguit moeten de sleutels wat groter worden.

Maar wie versleutelde gegevens met iemand anders wil uitwisselen, heeft een catch 22-probleem: hoe verstuur je de geheime sleutel veilig naar de andere partij voordat je beide een geheime sleutel hebt om veilig mee te communiceren? Daarvoor is het complexere asymmetrische, of publieke-sleutelcryptografie nodig.

Het 'asymmetrische' zit hem erin dat er niet één, maar twee sleutels zijn: de ene kan alleen data versleutelen, de andere alleen ontsleutelen. De 'publieke sleutel'-benaming slaat op het idee om een van die sleutels *niet* geheim te maken: als iemand zijn versleutelcode gewoon openbaar maakt, kan iedereen hem daarmee gecodeerde berichten sturen, terwijl alleen de daadwerkelijke ontvanger de ontsleutelcode heeft om ze ook echt te lezen.

Voor de asymmetrische variant is wel veel meer rekenkracht nodig dan voor de symmetrische versie, tot wel drie ordegroottes meer. Bovendien dijt de hoeveelheid data behoorlijk uit wanneer die asymmetrisch wordt versleuteld. Daarom wordt de methode doorgaans niet gebruikt voor directe versleuteling, maar om de catch 22 op te lossen: twee partijen gebruiken pkc aan het begin van een sessie alleen om een geheime sleutel af te spreken, en gebruiken die vervolgens om hun echte communicatie symmetrisch te versleutelen.

Publicatie : Bits&Chips
Datum : 22 jun 2018
cm2 : 1.125
Pagina : 41
Advertentiewaarde : € 6.120,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 6.500



Peter Schwabe

je niet in je beheer hebt, heb je standaardisatie nodig', stelt Schwabe.

Het doel van de Nist-competitie is om dergelijke praktisch inzetbare methodes te destilleren uit al die academische ideeën. Het project brengt de wereldwijde cryptografiegemeenschap samen in een open competitie waarin iedereen voorstellen kan insturen en ook iedereen kan proberen daar gaten in te schieten of verbeteringen in aan te brengen. Wat het project vooral interessant maakt, is dat het allemaal in het openbaar gebeurt. 'Bij het Iso of het Etsi is het allemaal wat gesloten', is Schwabes ervaring.

Deze vorm was eerder erg succesvol voor de totstandkoming van AES, de de facto standaard voor symmetrische crypto, en later ook voor hashing-algoritme Sha-3. Voor postquantumcrypto is de insteek wel iets anders. Het is niet per se de bedoeling een enkele winnaar aan te wijzen, maar om de bruikbare methodes te vinden. Bovendien kunnen voorstellen die op elkaar lijken worden samengevoegd, en zo zijn er nog wat verschillen.

De eerste fase werd begin dit jaar afgerond: het verzamelen van inzendingen. Dat leverde in totaal negenenzestig voorstellen op. België en Nederland zijn daarin niet onverdienstelijk: op een stuk of vijftien papers staan onderzoekers uit de Lage Landen in de auteurslijst. 'Het is mooie pr voor ons, niet?', meent Schwabe, die zelf bij zeven voorstellen betrokken is. 'Maar je zou kunnen zeggen dat heel West-Europa goed is in toegepaste cryptografie. Dit is wel de regio waar veel groepen echt bezig zijn met al die verschillende vormen van toegepaste crypto.'

'Vooral in Engeland, Frankrijk, België, Nederland en Duitsland', vult Ducas aan, wiens naam op vier voorstellen prijkt. 'In de VS heb je een beetje een rare situatie. Natuurlijk is er veel praktische expertise binnen de nationale veiligheidsdiensten, maar het open cryptoonderzoek is daar erg theoretisch.'

Tien regeltjes Python

Er zijn vijf families van aanpakken waar cryptografen op inzetten. Naast de eerder genoemde hashes gaat het om McEliece (of codes), dat reeds in de jaren zeventig werd ontwikkeld, *lattices* uit de jaren negentig (zie 'Cryptografie met lattices'), *isogeny*'s en MQ. 'Er zijn nog wel een paar andere, maar die worden niet zo serieus genomen', vertelt Schwabe. 'Er was bijvoorbeeld een voorstel gebaseerd op *random walks* in *graphs*. Drie uur na publicatie van de inzendingen was die compleet en onherstelbaar gekraakt, met tien regeltjes Python.'

Een echte kanshebber springt er wat Ducas en Schwabe nog niet uit. Al was het maar omdat de twee hoofdfuncties van pkc, versleutelen en ondertekenen, waarschijnlijk niet op dezelfde manier ingevuld kunnen worden. 'Hashes zijn alleen geschikt voor handtekeningen, McEliece is vooral goed voor versleuteling', verduidelijkt Schwabe. 'Met lattices kun je wel beide doen, en redelijk efficiënt ook. Isogeny is weer vooral geschikt voor versleuteling, en MQ weer voor handtekeningen – hoewel er verbazingwekkend veel MQ-gebaseerde versleutelingsaanpakken zijn ingediend.'

Dan nog kan het best zijn dat verschillende situaties verschillende oplossingen vereisen. Voor een smartcard of een systeem met securityprocessor kan het bijvoorbeeld aantrekkelijk zijn om een efficiënte methode te gebruiken die een interne toestand moet onthouden, terwijl gewone computers hun veel grotere rekenkracht kunnen inzetten.

Keten van vertrouwen

Naast de catch 22 van het afspreken van een sleutel is er nog een tweede probleem als je met een onbekende wilt communiceren: hoe weet je zeker dat iemand is wie hij claimt te zijn? Daarvoor kan ook asymmetrische cryptografie worden gebruikt. In het simpelste voorbeeld zou een zender zijn ontsleutelcode publiek beschikbaar kunnen maken. Met de andere, geheime sleutel kan dan een digitale handtekening onder elk van zijn boodschappen worden gezet – bijvoorbeeld een versleutelde versie van het bericht. Iedereen kan nu controleren dat de boodschap echt van die zender afkomstig is door de handtekening te ontcijferen en te kijken of daar het origineel uitkomt.

Dit proces staat bekend als ondertekenen (*signing*). In de praktijk zijn de protocollen wat complexer om een daadwerkelijk waterdicht systeem te maken. Bovendien is er nog iets aanvullends nodig. Want hoe weet je nou zeker dat de gepubliceerde sleutel die je krijgt ook echt van je bank of de webwinkel is, en niet van een vervalser?

Dat wordt opgelost doordat zo'n publieke sleutel wordt gepubliceerd via een zogeheten certificaat, een bestand dat ondertekend is door een derde partij die je al kent – bijvoorbeeld je webbrowser. Maar het kan natuurlijk gebeuren dat je die derde partij ook niet kent. Geen nood, want ook zijn publieke sleutel is weer gepubliceerd via een certificaat, dat dan weer door een andere partij ondertekend is. Zo ontstaat een keten van certificaten die je net zo lang kunt volgen totdat je een bekende partij tegenkomt.

Hoewel er al decennia naar quantumbestendige crypto wordt gekeken, is een universele oplossing nog jaren weg. Het is te hopen dat de quantumcomputer daar nog even op wil wachten.