Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Postkwantum-cryptografie

Bescherm uw data vandaag tegen de dreiging van morgen

Factsheet FS-2017-02 | versie 1.1 | 31 augustus 2017

De komst van kwantumcomputers kan grote gevolgen hebben voor organisaties die werken met versleutelde gegevens. Met een kwantumcomputer wordt het mogelijk gegevens te ontsleutelen die beveiligd zijn met de meestgebruikte vormen van cryptografie. Gegevens die op dit moment nog voldoende beveiligd zijn, zijn dat na de komst van kwantumcomputers niet meer. De gevolgen zijn echter nog groter: er kunnen nu al versleutelde gegevens worden onderschept, zodat ze in de toekomst met een kwantumcomputer ontsleuteld kunnen worden. Het NCSC adviseert organisaties een actieplan op te stellen. Dit moet duidelijk maken binnen welke tijdlijn er maatregelen genomen moeten worden om gegevens tegen kwantumcomputers te beschermen.

Wat is een kwantumcomputer?

Een kwantumcomputer is een nieuw soort computer gebaseerd op kwantummechanische principes. Ze worden momenteel nog ontwikkeld, maar het concept van kwantumcomputers bestaat al sinds de jaren tachtig. Verschillende partijen zijn bezig met het bouwen van geavanceerde kwantumcomputers.[1]

De werking van een kwantumcomputer is fundamenteel anders dan die van een klassieke computer. Zo zal een kwantumcomputer veel sneller zijn in het oplossen van bepaalde problemen dan een klassieke computer. Dit maakt

Doelgroep

Informatiebeveiligers
IT-managers

Aan deze factsheet hebben bijgedragen:

Betaalvereniging Nederland, KPN CISO, Ministerie van Veiligheid en Justitie, NBV, Peter Schwabe (RU), PQCRYPTO (Tanja Lange)

[1] Bron: https://www.aivd.nl/publicaties/publicaties/2014/11/20/informatieblad-over-quantumcomputers

kwantumcomputers waardevol voor het oplossen van ingewikkelde wetenschappelijke vraagstukken.

De eigenschappen van kwantumcomputers maken het ook mogelijk om de meestgebruikte vormen van cryptografie te breken.

Cryptografische algoritmes die gebruikt worden voor sleuteluitwisseling en het genereren van digitale handtekeningen zijn gebaseerd op lastig op te lossen wiskundige problemen. Een klassieke computer lost deze problemen niet zomaar op, maar voor een kwantumcomputer zijn ze een stuk minder ingewikkeld. Een aanvaller met een kwantumcomputer kan daardoor een groot deel van de versleutelde informatie die via het internet verstuurd wordt ontsleutelen.[2] Met een kwantumcomputer is het tevens mogelijk de betrouwbaarheid van digitale handtekeningen aan te tasten.

Kwantumcomputers die geavanceerd genoeg zijn om deze taken te vervullen bestaan op dit moment nog niet; de TU Delft verwacht een geavanceerde kwantumcomputer te realiseren tussen 2030 en 2040. Ook partijen als Google, Microsoft, IBM, en Intel werken aan de ontwikkeling van kwantumcomputers, en er lijkt tevens interesse te zijn vanuit grote inlichtingendiensten.[3]

In eerste instantie zullen voornamelijk overheden en wetenschappers gebruik willen maken van deze nieuwe techniek. De kans dat consumenten straks een fysieke kwantumcomputer in hun woonkamer hebben staan is – mede gezien de kosten – erg klein.

Het is echter waarschijnlijk dat kwantumcomputers na hun komst snel beschikbaar komen als cloudtoepassing. Hierdoor wordt de techniek – evenals de mogelijkheid om veelgebruikte cryptografie te breken – ook beschikbaar voor individuen.

In het vervolg van deze factsheet wordt met de term kwantumcomputer een geavanceerde kwantumcomputer bedoeld, die in staat is om de meestgebruikte vormen van cryptografie te breken.

Wat betekent de komst van kwantumcomputers voor mijn organisatie?

De komst kwantumcomputers heeft grote gevolgen voor organisaties die werken met versleutelde gegevens. Het gaat dan specifiek om gegevens die door derden te onderscheppen zijn. Dit zijn bijvoorbeeld gegevens die via een internetverbinding verzonden worden, of gegevens die na een datalek op internet gepubliceerd zijn.

Met een kwantumcomputer kunnen gegevens die beveiligd zijn met de meestgebruikte vormen van cryptografie worden ontsleuteld. Gegevens die op dit moment nog voldoende beveiligd zijn, zijn dat na de komst van kwantumcomputers dus niet meer.

Ook wordt het met een kwantumcomputer mogelijk de authenticiteit van digitale handtekeningen aan te tasten. Een aanvaller met een kwantumcomputer kan de geheime sleutel die voor een digitale handtekening gebruikt wordt achterhalen. Daarmee kan een aanvaller nieuwe handtekeningen genereren en zich zo voordoen als iemand anders.

Om de vertrouwelijkheid van gegevens en de betrouwbaarheid van digitale handtekeningen ook na de komst van kwantumcomputers te blijven beschermen zijn vormen van cryptografie nodig die bestand zijn tegen kwantumcomputers.

Kwantumalgoritmes

Het breken van cryptografie op een kwantumcomputer gebeurt met speciale algoritmes die enkel op een kwantumcomputer gebruikt kunnen worden: kwantumalgoritmes.

Shors algoritme is een kwantumalgoritme dat veelgebruikte cryptografische algoritmes voor sleuteluitwisseling en digitale handtekeningen breekt (asymmetrische cryptografie). Cryptografische algoritmes als RSA, ECDSA en Diffie-Hellman zijn dan niet meer veilig.

Met *Grovers algoritme*, een ander kwantumalgoritme, kunnen kwaadwillenden versneld zoeken naar vercijfersleutels of wachtwoorden.[4] Grovers algoritme is echter betrekkelijk traag; bij het gebruik van voldoende lange sleutels of wachtwoorden is Grovers algoritme niet effectief. Onderzoeksproject PQCRYPTO-EU adviseert daarom voor AES het gebruik van 256-bit sleutels.[5]

[2] Bron: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
[3] Bron: https://www.aivd.nl/publicaties/publicaties/2014/11/20/informatieblad-over-quantumcomputers

[4] De term 'versleuteling' omvat alle vormen van symmetrische encryptie, zoals AES, Salsa20, 3DES en RC4.
[5] Kijk voor de meest recente aanbevelingen op https://pqcrypto.eu.org/recommend.html.

Waarom moet mijn organisatie zich vandaag al zorgen maken over de komst van kwantumcomputers?

Er worden mogelijk vandaag al versleutelde gegevens onderschept, zodat ze in de toekomst met een kwantumcomputer ontsleuteld kunnen worden. Deze gegevens worden in afwachting van de kwantumcomputer opgeslagen, bijvoorbeeld door partijen die geïnteresseerd zijn in uw organisatie. Na de komst van kwantumcomputers zijn deze gegevens niet meer voldoende beveiligd en kan het gebruikte cryptografische algoritme gebroken worden. Gegevens die vandaag al bestaan en die ook na de komst van kwantumcomputers beschermd moeten blijven, moeten dus nu al aanvullend worden beschermd.

Digitale handtekeningen

Voor digitale handtekeningen is het in sommige gevallen ook belangrijk ze nu al aanvullend te beschermen.

Digitale handtekeningen worden gebruikt in producten die nog steeds in gebruik zullen zijn na de komst van kwantumcomputers. Denk hierbij aan Internet-of-Things-apparatuur, die digitale handtekeningen gebruikt om instructies van buitenaf op echtheid te controleren.

Op het moment dat er kwantumcomputers bestaan kunnen deze producten digitale handtekeningen niet meer betrouwbaar controleren. Een aanvaller met een kwantumcomputer kan een digitale handtekening namaken om deze apparaten vervalste instructies te sturen.

Er zal tijdig overgestapt moeten worden op sterkere vormen van cryptografie voor het aanmaken en controleren van deze handtekeningen, vanwege de lange levensduur van deze producten.

Wat adviseert het NCSC?

Het NCSC adviseert organisaties een actieplan op te stellen. Dit actieplan moet duidelijk maken binnen welke tijdlijn er maatregelen genomen moeten worden om gegevens tegen kwantumcomputers te beschermen.

Blijkt uit het actieplan dat uw organisatie nu al moet starten met het aanvullend beveiligen van gegevens? Bekijk dan de laatste aanbevelingen van het Europese onderzoeksproject PQCRYPTO-EU.[6] Dit project onderzoekt vormen van cryptografie die veilig blijven na de komst van kwantumcomputers.

[6] Kijk voor de meest recente aanbevelingen op https://pqcrypto.eu.org/recommend.html.

Bestaan er in uw organisatie geen gegevens die na de komst van kwantumcomputers nog steeds beschermd moeten blijven? Wacht dan met de overstap op nieuwe vormen van cryptografie. Afwachten heeft als voordeel dat er steeds betere vormen van cryptografie beschikbaar komen die bestand zijn tegen kwantumcomputers.

Het actieplan is afhankelijk van een aantal factoren

- **Het geschatte moment dat kwantumcomputers beschikbaar komen**. Niemand weet precies wanneer men er in slaagt een kwantumcomputer te bouwen. Maak desondanks een inschatting van het moment waarop u verwacht dat er kwantumcomputers zullen bestaan. Het kiezen van dit moment is in feite een vorm van risicoacceptatie. Hoe later u dit moment kiest, hoe groter de kans dat er voor die datum al kwantumcomputers bestaan.

- **De beschermingstijd van gegevens**. Het verschilt per organisatie en per soort gegevens hoe lang gegevens beschermd moeten blijven. Sommige gegevens hebben een levensduur tot na het moment dat de eerste kwantumcomputer beschikbaar komt. Deze gegevens moeten dus beveiligd worden met cryptografie die niet door een kwantumcomputer gebroken kan worden. Andere gegevens hebben een kortere levensduur of zijn tegen de tijd dat er kwantumcomputers bestaan al niet meer gevoelig.

  De manier van gebruik van gegevens. Verschillende soorten gegevens worden op verschillende manieren gebruikt en beveiligd. Elk soort gegevens zal dan ook andere prestatie-eisen aan cryptografie stellen. Denk bijvoorbeeld aan het verschil tussen gegevens die uitgewisseld worden tussen twee computers en de uitwisseling van gegevens met een smartcard.

- **De implementatietijd**. Dit is de tijd die de organisatie nodig heeft om over te stappen op nieuwe vormen van cryptografie. Deze tijd is bijvoorbeeld nodig voor het formuleren van beleid en het vervangen van hard- en software.

- **De beschikbaarheid van nieuwe vormen van cryptografie.** Er wordt momenteel gewerkt aan de ontwikkeling van cryptografie die ook na de komst van kwantumcomputers veilig blijft. Het zal nog enige tijd duren eer cryptografie die bestand is tegen kwantumcomputers gestandaardiseerd is en is geimplementeerd in hardware en software.

Handelingsperspectief

- Verzamel betrokken personen in uw organisatie. Stel gezamenlijk vast aan welke eisen beveiligde gegevens en/of digitale handtekeningen moeten voldoen. Dit verschilt per categorie gegevens. Bepaal welke soorten gegevens er in uw organisatie uitgewisseld worden, hoe lang deze beschermd moeten blijven, en op welke manier deze gegevens uitgewisseld worden. Sluit hierbij aan bij bestaande methoden voor dataclassificatie binnen uw organisatie.
- Stel het tijdstip vast waarop u verwacht dat kwantumcomputers beschikbaar komen.
- Maak – per categorie gegevens – een tijdlijn waarin duidelijk wordt wanneer moet worden gestart met het aanvullend beschermen van gegevens. Houd hierin rekening met de tijd dat gegevens beschermd moeten blijven, het geschatte moment waarop passende cryptografie beschikbaar komt die bestand is tegen kwantumcomputers, de tijd die nodig is om deze oplossing te implementeren, en de periode waarin er ruimte is om nog af te wachten.
- Bepaal het actieplan. Stel hierin de passende vorm van cryptografie vast voor elke categorie gegevens uit uw organisatie.

Hoe kunnen gegevens nu al beschermd worden tegen kwantumcomputers?

De ontwikkeling van cryptografische algoritmes die bestand zijn tegen kwantumcomputers levert - naarmate de tijd vordert - steeds betere oplossingen op.

Postkwantumcryptografie is de verzamelnaam voor alle vormen van cryptografie die veilig blijven na de komst van kwantumcomputers. Dit zijn zowel symmetrische als asymmetrische vormen van cryptografie.

Naast het onderzoek van het eerder genoemde Europees onderzoeksproject PQCRYPTO-EU, heeft ook het Amerikaanse National Institute of Standards and Technology (NIST) een uitvraag[7] geopend om de komende jaren gestandaardiseerde vormen van postkwantumcryptografie te ontwikkelen.

Versleuteling

Voor het versleutelen van gegevens geldt dat de lengte van de gebruikte sleutels vergroot moet worden om het gebruikte cryptografische algoritme bestand te maken tegen een kwamtumcomputer. AES-128 is bijvoorbeeld sterk genoeg om te beschermen tegen een aanvaller met klassieke middelen, maar niet tegen een aanvaller met een kwantumcomputer.

[7] Zie http://csrc.nist.gov/groups/ST/post-quantum-crypto/workshops.html

Onderzoeksproject PQCRYPTO-EU adviseert daarom voor AES het gebruik van 256-bit sleutels.[8]

Sleuteluitwisseling

Alle veelgebruikte vormen van cryptografie die gebruikt worden voor sleuteluitwisseling zijn niet meer betrouwbaar na de komst van kwantumcomputers.

Het handmatig uitwisselen van sleutels kan een goede oplossing zijn als het noodzakelijk is vandaag al te beginnen met het aanvullend beveiligen van gegevens. Deze oplossing ligt echter niet altijd voor de hand. Bij communicatie tussen twee datacenters is handmatige sleuteluitwisseling - bijvoorbeeld met een smartcard - voorstelbaar; voor reguliere internetcommunicatie is deze oplossing minder relevant.

U kunt handmatige sleuteluitwisseling niet alleen gebruiken in plaats van, maar ook in aanvulling op bestaande cryptografische sleuteluitwisseling. De buitenste laag van versleuteling vindt dan plaats op basis van de cryptografisch uitgewisselde sleutel. Daarbinnen vindt een laag van versleuteling plaats op basis van de handmatig uitgewisselde sleutel. De buitenste laag beschermt tegen aanvallers met klassieke middelen, de binnenste laag tegen aanvallers die beschikken over een kwantumcomputer.

Quantum Key Distribution

Op dit moment is Quantum Key Distribution nog geen geschikt alternatief voor postkwantumcryptografie.[9]

In tegenstelling tot traditionele cryptografie, die gebaseerd is op complexe wiskundige problemen, is Quantum Key Distribution een vorm van cryptografie gebaseerd op natuurkundige principes.

Quantum Key Distribution kent echter nog een aantal beperkingen.[9] Zo worden de veiligheidseigenschappen van Quantum Key Distribution nog onvoldoende begrepen. Ook vereist Quantum Key Distribution het gebruik van zeer kostbare hardware, die zowel de verzender als de ontvanger van de gegevens in bezit moet hebben. Het geografisch bereik van deze hardware is daarnaast maar beperkt.

[8] Kijk voor de meest recente aanbevelingen op https://pqcrypto.eu.org/recommend.html.
[9] Zie verder: https://www.ncsc.gov.uk/information/quantum-key-distribution

Digitale handtekeningen

Methoden van postkwantumcryptografie die gebruikt worden voor digitale handtekeningen en sleuteluitwisseling kennen momenteel nog een aantal beperkingen. Deze beperkingen betreffen de prestaties of bruikbaarheid van de methoden.[10] Ook is de veiligheid van veel voorstellen voor deze methoden van postkwantumcryptografie nog niet voldoende onderbouwd met wiskundig onderzoek.[11] Daarnaast moeten deze vormen van postkwantumcryptografie nog geïmplementeerd worden in veelgebruikte hardware en software.

Onderzoeksproject PQCRYPTO-EU adviseert het gebruik van SPHINCS-256 als methode voor *stateless* digitale handtekeningen en XMSS als methode voor *stateful* digitale handtekeningen.[12]

De cryptografische algoritmes die gebruikt worden voor het plaatsen van digitale handtekeningen kunnen *stateful* of *stateless* zijn. Voor het plaatsen van digitale handtekeningen zijn *stateful* algoritmes maar in een beperkt aantal situaties veilig bruikbaar. Deze vereisen namelijk het intern getrouw bijhouden van een toestandswaarde, een zogenaamde state, wat de toepassing aanzienlijk complexer maakt. Voor *stateless* algoritmes geldt deze beperking niet.

Tot slot

De komst van kwantumcomputers lijkt misschien nog ver weg, maar de gevolgen voor organisaties die werken met gevoelige gegevens zijn nu al aanwezig. Hoewel het aanbod van alternatieve vormen van cryptografie op dit moment nog schaars is, is het essentieel om vandaag al na te denken over vormen van cryptografie die uw organisatie moet implementeren, en de tijd die daarvoor nodig is.

[10] Bron: https://www.aivd.nl/publicaties/publicaties/2015/04/15/bereid-u-voor-op-de-komst-van-de-quantum-computer
[11] Bron: https://www.aivd.nl/actueel/nieuws/2014/11/20/quantumcomputer-vereist-nieuwe-cryptografische-oplossingen
[12] Kijk voor de meest recente aanbevelingen en nadere specificaties op https://pqcrypto.eu.org/recommend.html

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-02 | versie 1.1 | 31 augustus 2017