RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

SWEDISH ARMED FORCES

Position paper over Quantum Key Distribution

French Cybersecurity Agency (ANSSI)

Federal Office for Information Security (BSI)

Netherlands National Communications Security Agency (NLNCSA)

Swedish National Communications Security Authority, Swedish Armed Forces

Samenvatting

Quantum Key Distribution (QKD) tracht gebruik te maken van quantum-eigenschappen waardoor twee partijen een geheime sleutel kunnen afspreken via een onbeveiligd quantum-kanaal. Deze technologie heeft de nodige aandacht gekregen, waarbij soms wordt beweerd dat deze ongekend hoge bescherming biedt tegen aanvallen van zowel gewone computers als van quantumcomputers.

Wegens huidige en intrinsieke beperkingen kan QKD momenteel echter alleen in een aantal specifieke niche gevallen gebruikt worden. Het is niet mogelijk om QKD in de praktijk te gebruiken bij het overgrote deel van de use-cases waarbij klassieke protocollen voor sleuteluitwisseling momenteel gebruikt worden. Ook vanuit een veiligheidsperspectief is QKD nog niet voldoende ontwikkeld. Gezien de urgente noodzaak om niet afhankelijk te zijn van alleen asymmetrische cryptografie die kwetsbaar is voor quantumaanvallen voor het uitwisselen van sleutels, moeten de prioriteiten liggen bij de migratie naar post-quantumcryptografie en/of de toepassing van symmetrische sleutels.

Deze paper is bedoeld voor een algemeen publiek. Daarom zijn technische details voor zover mogelijk weggelaten. Technische termen die een definitie behoeven zijn schuingedrukt en worden onderaan in de definitielijst uitgelegd.

Inhoud

1 De quantum-dreiging

Als grootschalige fouttolerante quantumcomputers in de toekomst beschikbaar worden, kunnen ze met behulp van het algoritme van Shor [17] het grootste deel van de *asymmetrische cryptografie* kraken. Hier is onze digitale infrastructuur momenteel op gebouwd. Zelfs als cryptografisch relevante *quantumcomputers* nog niet beschikbaar zijn, wordt de vertrouwelijkheid van onze communicatie bedreigd, omdat vijandelijke actoren versleutelde berichten kunnen opslaan om ze in de toekomst te ontcijferen. Deze dreiging staat bekend als het store-now-decrypt-later-scenario.

Een mogelijkheid om de quantum-dreiging tegen te gaan is om de vooraf gedeelde *symmetrische* sleutels te gebruiken in combinatie met *klassiek veilige asymmetrische cryptografie*, in gevallen waarbij het haalbaar is om de *symmetrische* sleutels veilig te verspreiden. Een andere mogelijkheid is om *asymmetrische cryptografie* te ontwikkelen die geacht wordt veilig te zijn tegen aanvallen van klassieke computers en *quantumcomputers*. De zogenaamde *post-quantumcryptografie* heeft de afgelopen jaren een grondig standaardisatieproces ondergaan bij NIST en wordt ook door ISO gestandaardiseerd. Hierdoor wordt de eerste selectie van NIST-standaarden beschikbaar in 2024. Veel nationale instanties voor cyberveiligheid en communicatieveiligheid hebben aanbevelingen gedaan [1, 4, 5, 6, 13, 14, 18] en overheden hebben hun voornemens en plannen aangekondigd voor een tijdige migratie naar *post-quantumcryptografie*.

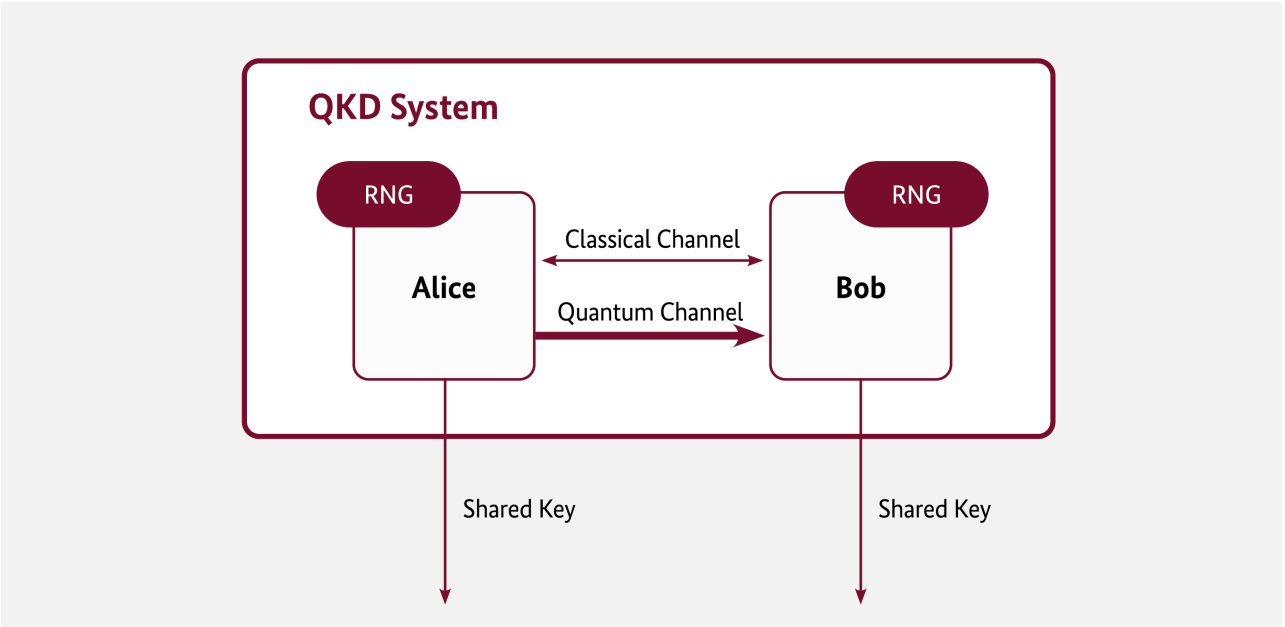
Een andere voorgestelde oplossing voor quantum-veilige *sleuteluitwisseling* is Quantum Key Distribution (QKD). QKD bestaat uit protocollen die quantumfysische fenomenen benutten voor een beveiligde *sleuteluitwisseling*. Dit is behoorlijk anders dan *post-quantum* en *klassiek beveiligde asymmetrische cryptografie*, wat betreft de principes waarop de beveiliging gebaseerd is en de manier waarop het toegepast wordt. Grote nationale en Europese projecten zijn momenteel gewijd aan de ontwikkeling van QKD-systemen en de constructie van grootschalige quantumcommunicatienetwerken; in het bijzonder het EuroQCI project dat opgezet is door de Europese Commissie. Een aantal nationale instanties voor cyberveiligheid en communicatieveiligheid hebben hun standpunt bekend gemaakt voor het gebruik van QKD of aspecten van QKD-beveiliging [2, 4, 5, 12, 15].

2 Waar QKD in kan voorzien

Om twee partijen, bijvoorbeeld Alice en Bob, overeen te laten komen tot een gedeelde geheime sleutel door middel van een QKD-protocol, moeten zij meestal verbonden zijn via een quantumkanaal (zoals een glasvezelkabel) en een klassiek communicatiekanaal. Om man-in-the-middle-aanvallen te voorkomen, moeten de berichten die verzonden worden via het klassieke communicatiekanaal, geauthenticeerd worden. Een gebruikelijke manier om dit te bereiken is dat Alice en Bob van tevoren een geheime sleutel delen en deze vervolgens gebruiken om berichten te authenticeren die via het kanaal verzonden worden. In een QKD-protocol worden quantumtoestanden (bijvoorbeeld als gepolariseerde fotonen) uitgewisseld of verspreid en gemeten; na post-processing wordt vervolgens een geheime sleutel uit de metingen gehaald door klassieke communicatie over het geauthenticeerde kanaal. Alice en Bob kunnen een afluisteraar ontdekken door delen van de resultaten van hun metingen te vergelijken, aangezien een quantumtoestand verandert als er enige interactie plaats heeft gevonden.

De theoretische veiligheid van QKD-protocollen is gebaseerd op quantumfysische principes, terwijl *post-quantumcryptografie* en *klassiek beveiligde asymmetrische cryptografie* gebaseerd zijn op de veronderstelde complexiteit van bepaalde wiskundige problemen. Dit betekent, ten minste in theorie, dat QKD-protocollen zelfs veilig zijn tegen aanvallers die over onbeperkte rekenkracht beschikken of mogelijke toekomstige algoritmische innovaties. Ze beweren in het bijzonder veilig te zijn in het store-now-decrypt-later-scenario.

Om beveiligd te zijn tegen aanvallers met onbeperkte rekenkracht moet de werkelijke data beschermd worden door een absoluut veilig encryptiemechanisme (bijvoorbeeld het *one-time pad-schema*). Dit vereist weer een QKD-kanaal met een bandbreedte die gelijk is aan dat van een klassiek datakanaal. Dergelijke bitrates zijn voor de meeste realistische toepassingen nog ver weg van wat QKD nu kan bereiken. Dit betekent dat de geheimen die gedeeld worden via quantum-kanalen



Figuur 1 Schematische illustratie van een QKD-systeem. Alice en Bob communiceren als onderdeel van het QKD-protocol via het klassieke kanaal en het quantum-kanaal. Aan het einde van het protocol verkrijgen ze gedeelde geheime sleutels die gebruikt kunnen worden voor bijvoorbeeld versleuteling. Random Number Generators (RNGs) zijn normaal gesproken onderdeel de QKD-modules van Alice en/of Bob.

gebruikt moeten worden als sleutels voor gevestigde *symmetrische cryptografische algoritmes* zonder absolute veiligheid zoals AES. Een dergelijk algoritme ondermijnt alle claims over absolute veiligheid tegen aanvallers met onbeperkte rekenkracht.

Het is ook belangrijk om te benadrukken dat de veiligheidsgaranties van QKD-protocollen slechts gelden in een theoretisch model. Elke praktische toepassing van een QKD-protocol, net zoals elke andere cryptografische toepassing, zal imperfecties hebben en afwijken van het theoretische model. Meerdere QKD-systemen zijn onveilig gebleken door aanvallen afhankelijk van de fysieke eigenschappen van de concrete apparaten die gebruikt worden om QKD-protocollen uit te voeren. Hierdoor is grondige evaluatie van QKD-systemen nodig om vertrouwen te krijgen in de veiligheid van concrete toepassingen. Beweringen over “absolute” of “onvoorwaardelijke” veiligheid die QKD zou bieden, kunnen nooit gelden voor werkelijke toepassingen.

3 Hoe QKD-technologisch beperkt is

De huidige QKD-technologie heeft een aantal tekortkomingen. Hierdoor kan QKD voorlopig in de praktijk alleen worden overwogen voor een aantal specifieke niche use-cases. *Post-quantumcryptografie* en *symmetrische* sleutels (met vooraf gedeelde symmetrische sleutels) moeten worden gezien als de primaire oplossingen voor *quantum-veilige cryptografie*. Hieronder leggen we kort een aantal tekortkomingen van QKD uit.

Benodigde gespecialiseerde hardware en hoge kosten

In tegenstelling tot *post-quantum* en *klassieke beveiligde asymmetrische cryptografie* kan QKD niet gebruikt worden op klassieke hardware. Er is gespecialiseerde hardware voor nodig, zoals ‘single-photon’-bronnen en -detectoren. De aankoop van deze apparatuur en het onderhoud van een QKD-systeem of QKD-netwerk voor de gehele levenscyclus gaan gepaard met heel hoge kosten. Dit soort apparatuur kan vanzelfsprekend niet ingezet worden door elke individuele gebruiker die beveiligde communicatie nodig heeft. Bovendien is het ook niet geschikt voor gebruik met mobiele apparaten.
Daar komt bij dat de basisclaim van QKD verandert, namelijk dat elke poging tot afluisteren ontdekt wordt, elke poging in een denial-of-service-aanval. In het algemeen kan elke inmenging in het communicatiekanaal

(zelfs als het niet expliciet gemeten wordt door een aanvaller) in de praktijk leiden tot een denial-of-service. Deze dreiging is nog niet grondig onderzocht en de kosten die gepaard gaan met het beschermen van quantum-kanalen tegen dergelijke aanvallen zijn nog onbekend.

Beperkingen van afstand en *end-to-end security*

Afhankelijk van afstand, groeit het signaalverlies in glasvezelkabels exponentieel. Hierdoor is het momenteel niet mogelijk om quantumtoestanden betrouwbaar te verzenden over langere afstanden via glasvezelkabels. Huidige QKD-demonstraties kunnen momenteel maximaal een paar honderd kilometer overbruggen en commerciële QKD-systemen bereiken over het algemeen ongeveer honderd kilometer [8]. Er moeten vertrouwde knooppunten ("trusted nodes") toegevoegd worden voor een langere afstand, zodat elke keer een sleutel overeengestemd wordt tussen elk paar opeenvolgende knooppunten. *End-to-end security* kan momenteel dus niet bereikt worden over langere afstanden met QKD op glasvezelbasis.

Een mogelijke oplossing om langere afstanden te overbruggen is het gebruik van quantum-repeaters die gebaseerd zijn op quantum-verstrengeling. Er wordt nog fundamenteel onderzoek gedaan naar quantum-repeaters. Ze zijn momenteel nog niet toepasbaar in de praktijk. Een alternatief is om QKD op basis van satellieten te gebruiken. Huidige toepassingen gaan echter vooral uit van 'non-geostationary orbits', zodat de beschikbaarheid van deze satellieten, die ook gevoelig zijn voor weersomstandigheden, beperkt wordt tot een korte tijdsperiode per dag. Dit beperkt de tijd waarin sleutels kunnen worden gegenereerd nog meer. Bovendien vormen de satellieten zelf ook vertrouwde knooppunten in de meeste huidige toepassingen. Een infrastructuur van satellieten voor QKD draagt natuurlijk bij aan zeer significante kosten.

Vertrouwen op klassieke cryptografie voor authenticatie

Zoals eerder uitgelegd is er voor QKD een klassiek geauthenticeerd kanaal nodig tussen de twee communicerende partijen. Er zijn meerdere opties voor het invoeren van een authenticatiemechanisme. Een optie is om vooraf gedeelde sleutels te gebruiken met *symmetrische* berichtauthenticatie. Hiervoor moet een geheime gedeelde sleutel al aanwezig zijn aan de beide kanten die met elkaar willen communiceren, alvorens een QKD-protocol uit te voeren. Derhalve moeten geheime sleutels op een veilige manier gedeeld en dan periodiek vernieuwd worden voordat QKD uitgevoerd kan worden. Een andere optie is het gebruik van post-quantum *handtekeningen* met bijbehorende *public key infrastructure* (PKI). In dit geval hangt de authenticatie echter af van de veiligheid van het post-quantumprotocol.

4 Waarom QKD niet voldoende ontwikkeld is

Door de technologische tekortkomingen is QKD momenteel niet geschikt voor gebruik in de meeste praktische zaken. Door de hoge kosten van de huidige QKD-technologie is het alleen relevant om te gebruiken in situaties waarbij de specifieke veiligheidsbenodigdheden deze kosten rechtvaardigen en waar bovendien minder dure opties niet toereikend zijn. Zelfs in gevallen waarbij QKD een goede optie lijkt, is veel meer werk nodig om vertrouwen te hebben in de veiligheid van concrete QKD-apparaten. Er moet nog veel werk verricht worden voor de volgende belangrijke aspecten. Dit is echter geen volledige lijst en er zijn ook andere problemen die aandacht vereisen.

Standaarden voor QKD-protocollen

Het ontwikkelen van veilige cryptografische algoritmes en protocollen is ingewikkeld; zelfs experts maken fouten bij het ontwerpen. Daarom is er een consensus in de cryptografische gemeenschap over het belang van de standaardisering van cryptografische algoritmes en protocollen. Naast dat het interoperabiliteit mogelijk maakt, is standaardisering cruciaal voor de veiligheid, omdat experts hierdoor de cryptografische mechanismen nauwkeurig kunnen bestuderen. Een dergelijk proces, bijvoorbeeld het NIST-proces voor *post-quantumcryptografie*, wordt gewoonlijk over een aantal jaren uitgevoerd en kan een hoog niveau van vertrouwen opleveren in de protocollen die uiteindelijk gestandaardiseerd worden.

Hetzelfde zou moeten gelden voor QKD-protocollen. Geen enkel QKD-protocol heeft, voor zover wij weten, een dergelijk standaardiseringsproces ondergaan.

QKD veiligheidsbewijs

Zoals hierboven uitgelegd wordt, kunnen QKD-protocollen beveiliging bieden door middel van quantum-fysische principes, zonder dat aannames over de moeilijkheidsgraad van wiskundige problemen nodig zijn. Grondige veiligheidsbewijzen zijn nodig om er zeker van te zijn dat een bepaald QKD-protocol voor een dergelijke beveiliging zorgt en om het beveiligingsniveau te kwantificeren. Een veiligheidsbewijs zou het QKD-protocol moeten beschrijven in een nauwkeurig wiskundig model met goed gedefinieerde aannames, en een nauwkeurige stelling moeten uitdrukken en de beveiliging van de veiligheid van het protocol in dit model afleiden. Een veiligheidsbewijs is puur theoretisch en wordt uitgevoerd in een abstract model. Voordat dit gerelateerd kan worden aan de veiligheid van een werkelijke toepassing op een betekenisvolle manier, moet de veiligheidsstelling bewezen worden in een model dat zo realistisch mogelijke omstandigheden nabootst.[1] Bovendien is het belangrijk dat alle aspecten van het protocol geformaliseerd worden in het model, zodat het bewijs zo grondig mogelijk is en fouten voorkomen kunnen worden. Er zijn commerciële QKD-protocollen die niet voldoende veiligheidsbewijs hadden en die later onveilig bleken te zijn [7].

Er is de afgelopen jaren veel onderzoek gedaan naar QKD-veiligheidsbewijzen en het gebied is aanzienlijk ontwikkeld [16]. Voor zover wij weten is er geen veiligheidsbewijs voor een praktisch relevant protocol geschreven op een samenhangende en overzichtelijke manier, die aan bovenstaande eisen voldoet. Om vertrouwen te hebben in de theoretische veiligheid van QKD-protocollen, moeten gestandaardiseerde QKD-protocollen vereist worden, met overeenkomende nauwkeurige en overzichtelijke veiligheidsbewijzen die rekening houden met een realistisch model. Deze moeten breed beschikbaar en toegankelijk worden en nauwkeurig bestudeerd worden door verschillende experts.

Evaluatiecriteria en methodologie

Gestandaardiseerde QKD-protocollen met overeenkomende veiligheidsbewijzen zijn niet voldoende. Het bestaan van een grote selectie van fysieke aanvallen tegen QKD-apparaten [3] toont aan dat alle fysieke apparaten die gebruikt worden voor de toepassing, een grondig evaluatieproces moeten ondergaan. Erkende evaluatiecriteria en methodologieën zijn nodig om te kunnen verzekeren dat QKD-protocollen juist zijn toegepast in daadwerkelijke apparaten en dat de implementatie niet gevoelig is voor fysieke aanvallen. Er is al wat werk gedaan op dit gebied. Een Common Criteria Protection Profile voor een belangrijke klasse van QKD-protocollen, de zogenaamde prepare-and-measure-QKD, wordt financieel gesteund door de BSI en is in samenwerking met ETSI ontwikkeld. Er zijn bovendien een ISO/IEC-norm

voor veiligheidseisen en test- en evaluatiemethoden voor QKD [9, 10] gepubliceerd. Er is echter nog een lange weg te gaan. Er moeten bijvoorbeeld nog steeds QKD-gerelateerde normen ontwikkeld worden, evenals een evaluatiemethodologie voor fysieke aanvallen tegen QKD-systemen. Op dit gebied is mogelijk ook aanvullend onderzoek nodig.

5 Conclusie

QKD is een interessante technologie en onderzoek naar dit onderwerp moet voortgezet worden om te onderzoeken of er manieren zijn om de beperkingen van de huidige technologie te overwinnen. De onderliggende technologie kan ook nuttig zijn voor andere toepassingen.

Wegens huidige en intrinsieke beperkingen kan QKD momenteel alleen in een aantal specifieke niche gevallen toegepast worden. Het is niet mogelijk om QKD in de praktijk toe te passen voor het overgrote deel van de use-cases waarbij *klassieke protocollen voor sleuteluitwisseling* momenteel gebruikt worden. Ook is QKD nog niet voldoende ontwikkeld vanuit een veiligheidsperspectief. Er is veel meer werk nodig om het vertrouwen te versterken in QKD-protocollen en in QKD-apparaten die dergelijke protocollen uitvoeren, waaronder werk aan protocolnormen, andere QKD-gerelateerde normen, veiligheidsbewijzen, en evaluatiemethodologieën.

Anderzijds kan *post-quantumcryptografie* toegepast worden op klassieke hardware en dus ingezet worden in klassieke communicatie-infrastructuren; standaardisering van algoritmes en hun integratie in protocollen en dataformats is redelijk geavanceerd, en een aantal algoritmes gebaseerd op verschillende wiskundige aannames is beschikbaar, waardoor het risico geminimaliseerd kan worden. Door de urgente noodzaak om niet alleen te vertrouwen op *asymmetrische cryptografie* die kwetsbaar is voor quantum-aanvallen, moet de prioriteit liggen bij de migratie naar *post-quantumcryptografie* in hybride oplossingen met traditionele *symmetrische* sleutels of *quantum-veilige asymmetrische cryptografie*.

---

1 Het aanvalmodel moet bijvoorbeeld zo algemeen mogelijk zijn, er moet rekening gehouden worden met verlies in het quantumkanaal en imperfecties in de detectoren, en de beveiligingsnorm moet stand houden voor eindige sleutelgroottes en niet slechts asymptotisch, bijvoorbeeld niet alleen in de grens van oneindig veel uitgewisselde signalen.

6 Definitielijst

Begrip	Definitie
Asymmetrische cryptografie	Ook bekend als publieke sleutelcryptografie. Een soort cryptografie waarbij een sleutelpaar, bestaande uit een publieke sleutel en een geheime sleutel, voor alle operaties gebruikt wordt. Iedereen kan bijvoorbeeld klare tekstberichten versleutelen met de publieke sleutel, maar alleen de geheime sleutel kan gebruikt worden om de hieruit voortvloeiende cijfertekstberichten te ontcijferen wanneer asymmetrische cryptografie vertrouwelijkheid biedt. De geheime sleutel wordt ook gebruikt om de ondertekening te genereren, terwijl de publieke sleutel door iedereen gebruikt kan worden om de resulterende ondertekeningen te verifiëren als asymmetrische cryptografie wordt gebruikt voor authenticatie of onweerlegbaarheid. Om dit in de praktijk te laten werken, moeten de publieke en geheime sleutels in het sleutelpaar vanzelfsprekend sterk verband houden tot elkaar. De veiligheid van de asymmetrische cryptografie is daarom normaal gesproken gebaseerd op de moeilijkheidsgraad van hele specifieke wiskundige problemen.
End-to-end-beveiliging	Zorgt ervoor dat enkel de partijen die met elkaar communiceren, en geen passieve of actieve tussenpersonen, toegang kunnen krijgen tot de klare tekst van de berichten die uitgewisseld worden in een communicatieprotocol.
Klassiek veilige asymmetrische cryptografie	Asymmetrische cryptografische mechanismen die, in tegenstelling tot post-quantumcryptografie, niet beveiligd zijn tegen aanvallen van grootschalige quantumcomputers. Hieronder vallen ook de RSA en elliptische kromme-cryptografie.
One-time pad	Een symmetrisch versleutelprotocol dat perfecte beveiliging biedt, in de zin dat er geen informatie over de klare tekst uit de cijfertekst gehaald kan worden. Voor dit protocol kan elke encryptiesleutel maximaal één keer gebruikt worden en moet deze dezelfde lengte hebben als, of langer zijn dan de klare tekst. Hierdoor wordt het zelden gebruikt.
Post-quantumcryptografie	Asymmetrische cryptografische mechanismen die beveiligd zijn tegen aanvallen door klassieke computers en quantumcomputers. Post-quantumcryptografie kan worden toegepast op klassieke computers.
Protocol voor handtekeningen	Een soort asymmetrische cryptografie die gebruikt kan worden om een handtekening te genereren en verifiëren, bijvoorbeeld om berichten te authenticeren.
Protocol voor sleuteluitwisseling	Een mechanisme of protocol dat het mogelijk maakt voor twee partijen om een gedeelde geheime sleutel af te spreken via een onbeveiligd communicatiekanaal. Deze geheime sleutels worden dan gebruikt om klare tekstberichten te versleutelen met symmetrische cryptografie.
Public Key Infrastructure (PKI)	Een systeem dat digitale certificaten kan creëren, verspreiden, verifiëren en intrekken en dat gewoonlijk gebruikt wordt voor het beheer van publieke sleutels om het gebruik van asymmetrische cryptografie mogelijk te maken.
Quantumcomputer	Een computer die quantummechanische verschijnselen gebruikt om berekeningen uit te voeren, in tegenstelling tot de huidige klassieke computers die klassieke verschijnselen gebruiken om berekeningen uit te voeren. Quantumcomputers kunnen sommige problemen sneller oplossen dan klassieke computers.
Quantum-veilige cryptografie	Cryptografische mechanismen en protocollen die veilig zijn tegen aanvallen van klassieke computers en quantumcomputers. Deze omvatten post-quantumcryptografie en Quantum Key Distribution.

Symmetrische cryptografie	Een vorm van cryptografie waarbij dezelfde sleutel voor alle operaties wordt gebruikt. Dezelfde sleutel wordt bijvoorbeeld gebruikt om klare tekstberichten te versleutelen en om de daaruit voortvloeiende cijfertekstberichten te ontcijferen als symmetrische cryptografie gebruikt wordt voor vertrouwelijkheid. Op een vergelijkbare manier wordt dezelfde sleutel gebruikt om authenticatietags te genereren en verifiëren wanneer symmetrische cryptografie wordt gebruikt voor berichtauthenticatie.

7 Bibliografie

[1]ANSSI: ANSSI views on the Post-Quantum Cryptography transition (2023 follow up), https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography (29/08/2023)

[2]ANSSI: Should Quantum Key Distribution be Used for Secure Communications? (ANSSI – Technical Position Paper: QKD v2.1), https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be- used-secure-communications

[3]BSI: Implementation Attacks against QKD Systems, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD- Systems.html (21/12/2023)

[4]BSI: Quantum-Safe Cryptography, www.bsi.bund.de/dok/pqmigration-en (18/05/2022)

[5]M. Ekerå, Swedish NCSA, Swedish Armed Forces, "The quantum threat to cryptography, our mitigation strategy, and our stance on quantum key distribution", keynote at the NATO IST-SET-198 Symposium, Amsterdam, the Netherlands, October 3–4, 2023.

[6]M. Ekerå, Swedish NCSA, Swedish Armed Forces, "Advice on mitigating the quantum threat to cryptography", presentation at the ESA workshop, Noordwijk, the Netherlands, June 27, 2022.

[7]Javier González-Payo, Róbert Trényi, Weilong Wang, and Marcos Curty. Upper security bounds for coherent-one-way quantum key distribution. Phys. Rev. Lett., 125:260510, Dec 2020.

[8]Huttner, B., Alléaume, R., Diamanti, E. et al. Long-range QKD without trusted nodes is not possible with current technology. npj Quantum Inf 8, 108 (2022). https://doi.org/10.1038/s41534-022-00613-4

[9]ISO/IEC 23837-1:2023. "Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements", https://www.iso.org/standard/77097.html

[10] ISO/IEC 23837-2:2023. "Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods", https://www.iso.org/standard/77309.html

[11] Lydersen, L., Wiechers, C., Wittmann, C. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon 4, 686–689 (2010). https://doi.org/10.1038/nphoton.2010.214

[12] NCSC: Quantum security technologies, https://www.ncsc.gov.uk/whitepaper/quantum-security- technologies (24/03/2020)

[13] NLNCSA: Prepare for the threat of quantum computers, https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of- quantumcomputers (18/01/2022)

[14] NSA: Announcing the Commercial National Security Algorithm Suite 2.0, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF (07/09/2022)

[15] NSA: Quantum Key Distribution (QKD) and Quantum Cryptography (QC), https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[16] Christopher Portmann and Renato Renner. Security in quantum cryptography. Rev. Mod. Phys., 94:025008, Jun 2022.

[17] Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press. pp. 124–134.

[18] TNO, CWI, AIVD: Het PQC-migratie handboek, https://www.aivd.nl/documenten /publicaties/2023/04/04/pqc-migratie-handboek (03/2023)