Experimental quantum position verification: practical challenges and single-photon correlations

Kanneworff, K.N.

Samenvatting

In dit proefschrift presenteren we ons werk voor een eerste experimentele demonstratie van een quantum positieverificatieprotocol (QPV) met behulp van een temporeel gedemultiplexte quantum dot één-foton bron.

Positieverificatie is een authenticatiemethode die gebaseerd is op het verifiëren van de geografische locatie van de bewijzer. Bij positieverificatie bevinden zich meerdere controleurs, die elkaar vertrouwen, rondom de persoon die zijn positie wil bewijzen: de bewijzer. De controleurs sturen informatie naar de bewijzer, die een vooraf bepaalde taak moet uitvoeren met behulp van alle ontvangen gegevens en vervolgens het resultaat moet terugsturen. Door de tijd tussen het verzenden en ontvangen van signalen te meten, kunnen de controleurs hun afstand tot de bewijzer bevestigen. Ervan uitgaande dat informatie zich met de snelheid van het licht voortbeweegt, de maximaal mogelijke snelheid, komt de voortplantingstijd van de signalen rechtstreeks overeen met tweemaal de afstanden tussen de controleurs en de bewijzer.

In dit proefschrift tonen we een eerste QPV-demonstratie-experiment in één dimensie, dat kan worden uitgebreid naar drie dimensies. In het eendimensionale geval bevinden twee controleurs zich aan weerszijden van de bewijzer langs een rechte lijn. Eerdere theoretische studies hebben aangetoond dat het gebruik van quantum informatie essentieel is voor veilige positiebepaling, aangezien de no-cloning-stelling het perfect kopiëren van quantum toestanden verhindert. Dit staat in contrast met klassieke informatie, die wel perfect kan worden gekopieerd.

In hoofdstuk 2 geven we een gedetailleerd overzicht van verschillende QPV-protocollen. Deze protocollen kunnen worden gecategoriseerd op basis van het aantal qubits, één of twee, wat ze per ronden gebruiken. We vergelijken deze protocollen op het gebied van verliesbestendigheid, de haalbaarheid van het verzenden van quantum informatie met snelheden onder de lichtsnelheid en de hoeveelheid vooraf gedeelde verstrengeling die nodig is om het protocol te compromitteren. Theoretische studies hebben aangetoond dat één-qubitprotocollen die substantiële klassieke informatie van alle controleurs bevatten, robuuster zijn tegen aanvallen waarbij vooraf gedeelde verstrengeling wordt gebruikt. Bovendien maken deze protocollen het mogelijk om quantum informatie te verzenden met snelheden lager dan de lichtsnelheid, op voorwaarde dat klassieke informatie zich wel met de lichtsnelheid voortplant. Twee-qubit-protocollen zijn daarentegen volledig verliesbestendig. Dit betekent dat vijanden geen enkel verliesniveau in hun voordeel kunnen uitbuiten, wat cruciaal is voor de implementatie met echte hardware.

Voor qubits die zich met de snelheid van het licht kunnen verplaatsen, zijn enkele fotonen die worden gegenereerd door een quantum dot één-foton bron zeer geschikte kandidaten. In dit werk wordt quantum informatie gecodeerd in de polarisatietoestand van licht. In hoofdstuk 3 onderzoeken we de werking en stabilitiet van polarisatiemodulatoren, de apparatuur dat voor deze codering wordt gebruikt. Daarnaast onderzoeken we de werking en stabiliteit van lange (200 m) single-mode glasvezel kabels die worden gebruikt om de fotonentransmissie tussen de controleurs en de bewijzer te simuleren. Voor

beide optische componenten stellen we vast dat de transformaties die op de polarisatietoestand van licht worden toegepast, als unitair kunnen worden beschouwd. De fideliteit van de polarisatietoestanden, die de gelijkenis tussen toestanden kwantificeert, wordt gebruikt als maatstaf om verschuivingen in de polarisatietoestand van licht over langere perioden te definiëren. Uit deze analyse leiden we de stabiliteit af van zowel de polarisatiemodulatoren als de lange optische vezels, wat waardevolle inzichten oplevert voor het ontwerp van een QPV-demonstratie-experiment. In het laatste deel van hoofdstuk 3 onderzoeken we de polarisatiemodusdispersie in lange single-mode glasvezel kabels en constateren we dat de impact verwaarloosbaar is.

Een quantum dot één-foton bron zendt een stroom van enkelvoudige fotonen uit in één ruimtelijke modus. Vanwege het epitaxiale groeiproces van quantum dots is het een uitdaging om twee bronnen te fabriceren die fotonen uitzenden die perfect identiek (niet te onderscheiden) zijn. Om het twee-foton QPV-protocol uit te voeren, is interferentie tussen twee enkele fotonen vereist. Hiervoor is een methode nodig om fotonen die in één ruimtelijke modus worden uitgezonden, over ten minste twee ruimtelijke modi te verdelen. Bovendien moet de ononderscheidbaarheid van enkele fotonen van onze quantum dot één-foton bron gekarakteriseerd worden. Deze vragen worden behandeld in hoofdstukken 4 en 5.

In hoofdstuk 4 wordt de stroom van enkele fotonen probabilistisch verdeeld over twee paden met behulp van een Mach-Zehnder-interferometer (MZI) met een optisch padlengteverschil om fotonen die op verschillende tijdstippen zijn gecreëerd te laten interfereren. In dit hoofdstuk onderzoeken we niet alleen de ononderscheidbaarheid van onze bron van enkele fotonen, maar ook de correlaties die worden waargenomen bij een vertraging die overeenkomt met de interne vertraging van de interferometer. We geven zowel een intuïtieve verklaring voor de oorsprong van deze correlaties als een stelsel van vergelijkingen dat de correlaties bij alle mogelijke vertragingen beschrijft. Dit theoretische kader levert een uitdrukking op voor de ononderscheidbaarheid van enkele fotonen die rekening houdt met onevenwicht in de intensiteit van de twee paden in de MZI, en imperfecties in de voorbereiding van de polarisatietoestand van de fotonen. De validiteit van dit analytische model wordt geverifieerd aan de hand van experimentele gegevens die zijn verkregen door MZI's met zowel een korte (9 ns) als een lange (1 us) interne vertraging.

In hoofdstuk 5 onderzoeken we een meer deterministische verdeling van enkele fotonen over twee ruimtelijke modi met behulp van een optische switch. We geven een didactische uitleg van hoe demultiplexing de stroom van fotonen en de gemeten correlaties beïnvloedt. We stellen vast dat de normalisatie van de tweede-orde correlatiefunctie zorgvuldig moet worden uitgevoerd, vooral wanneer de schakeltijd slechts iets langer is dan het interval tussen opeenvolgende fotonen. Ten slotte presenteren we de gemeten correlaties voor onze gedemultiplexte quantum dot bron, waar de optische switch een schakeltijd van 1 us heeft. Hieruit blijkt dat bij langzame schakeling de normalisatiefout als verwaarloosbaar kan worden beschouwd.

In het laatste hoofdstuk van dit proefschrift integreren we de bevindingen uit de voorgaande hoofdstukken om tot een eerste experimentele demonstratie van quantum positieverficatie te komen. Voor deze demonstratie hebben we gekozen voor het twee-foton SWAP-protocol vanwege zijn volledige verliesbestendige eigenschappen. De resultaten tonen aan dat de Hong-Ou-Mandel (HOM) interferentiecontrast van onze één-foton bron de beperkende factor is, waardoor we de drempel niet kunnen bereiken om onderscheid te maken tussen een eerlijke bewijzer en tegenstander die opereren onder lokale operaties

en klassieke communicatie (LOCC). Modellering van de experimentele omstandigheden in combinatie met een state-of-the-art één-foton bron die in de literatuur wordt beschreven, geeft echter aan dat de LOCC-drempel binnen bereik ligt.

Verder onderzoek zou continue verbeteringen van hetzelfde protocol moeten bevatten met behulp van een state-of-the-art één foton bron. Eveneens is voortdurende ontwikkeling van QPV-protocollen van belang. Het doel is een protocol dat minimale quantum middelen vereist, de overdracht van quantum informatie met snelheden onder de lichtsnelheid mogelijk maakt, en volledig bestendig is tegen optische verliezen.