0.1 Praktische opdrachten:BB84

naam:

klas:

datum:

In werkblad BB84 staat het protocol beschreven hoe je met enkele fotonen een quantum communicatie op kunt zetten die theoretisch altijd veilig is. In theorie is het allemaal mooi, maar de techniek is niet perfect. In deze opdracht laten we de belangrijkste voorwaarde voor veiligheid van het protocol los: het werken met enkele fotonen. Enkele fotonen detectors zijn gewoonweg te duur en te kwetsbaar voor ons lab. Het no-cloning principe geldt niet meer.

We proberen het protocol uit met simpele middelen, een zaklamp wat lenzen, polaroid filters.

Alice wil een geheime boodschap naar Bob sturen. versleuteling is daarvoor de oplossing. Een boodschap niet te ontcijferen als de sleutel geheim is en even lang of langer dan de boodschap. Dat is makkelijk in te zien met de werking van de klassieke **XOR**-poort.

Door de boodschap voor verzending met de sleutel (die even lang als de boodschap!) door een **XOR**-poort te halen is de boodschap wiskundig aantoonbaar niet te achterhalen zonder kennis van de sleutel, want elk bit is op een random manier versleuteld.

Bob heeft de sleutel en hoeft alleen nogmaals de **XOR**-poort op de ingekomen boodschap los te laten om Alice' boodschap te achterhalen.

In het BB84 protocol kunnen Alice en Bob een quantum sleutel kunnen opstellen die zij alleen kennen. Zij hebben die niet hoeven delen over een klassiek kanaal. Zij hebben de sleutel gedeeld zonder die daadwerkelijk over te zenden.

Uitvoering Omdat wij het allemaal met de hand doen beperken we de lengte van de boodschap tot twee letters. Je hebt vijf bits nodig om de letters A-Z binair om te zetten. De boodschap is dus tien bits lang.

Hoeveel bits moet Alice met haar klassieke random generator opzetten?

We beginnen met een serie random bits die vier keer zo lang is als de boodschap, 40 bits.

Alice kiest bij elk bit in welke basis het verstuurd wordt (Standaard of Diagonaal) en houdt dat bij.

Bouw de opstelling. Knip twee exemplaren van de polaroidhouders uit stevig karton. Plak de polaroids er in dezelfde stand op.

Monteer een lamp en een collimator lens op een optische rails. Zet de de lamp in het brandpunt en beeldt de lamp af op een plaats ver weg. Laat het licht door twee polaroids vallen. Zet de filters in dezelfde oriëntatie„ onder een hoek van 45° en loodrecht op elkaar. Gebruik het blote oog, of een lichtsensor om de intensiteit bij die drie standen te meten.

Als je veel tijd hebt kun je een automatisch systeem maken, maar de simpelste vorm is om de volgnummers van de te verzenden bits even door het lokaal te roepen (een klassiek kanaal). Tijdens de uitvoering is dit de enige informatie die team Alice mag roepen naar team Bob. Alle andere communicatie wordt onderschept door Eve.

voorbereiding Team Alice moet nauwkeurig de toestand van de verzonden bits en de bijbehorende filterstand bijhouden. Hetzelfde geldt voor team Bob.

team Alice: Een formulier met N kolommen en rijen voor

- **a**. random gegenereerde bits
- **b**. filterstanden
- **c**. ...

TeamBob

Een formulier met N kolommen end rijen voor

- **a**. stand van het filter
- **b**. waarneming: aan uit of half

Na het overzenden kan de lamp uit. het quantum gedeelte van de communicatie is nu klaar.

Welke gegevens mag Alice niet communiceren: de random key

Alice en Bob vergelijken welke bits zij in dezelfde basis hebben gemeten door per bit af te kondigen standaard of diagonaal. Als de antwoorden gelijk zijn behouden ze het bit, als ze tegengesteld zijn strepen ze het weg.

Ze houden ongeveer de helft van het aantal bits over. Het aantal bits dat overblijft zal groter zijn dan de lengte van de boodschap (N). Mocht dat niet zo zijn: uithuilen en opnieuw beginnen.

Het verschil tussen de lengte van de boodschap en de goedgekeurde bits kunnen ze gebruiken om te controleren of ze afgeluisterd zijn. Tel de lengte van de boodschap af en gebruik de rest om te controleren of je afgeluisterd bent. Mocht hier een fout in zitten: uithuilen en opnieuw beginnen.

De resterende bits vormen de sleutel die even lang is als de boodschap.

Alice ontvangt de twee letter code van de spelleider.

Met de gereduceerde ASCII tabel digitaliseert Alice de twee letters in een 10-bits Alice versleutelt de boodschap met de **XOR**-poort en belt het resultaat door.

Bob ontcijfert de boodschap door nogmaals de **XOR**-poort er op los te laten. Kijkt in de ASCII kaart om de twee letter code et ontcijferen. Het is het land waar hij Alice zal ontmoeten voor een volgende missie.....

Alice en Bob hebben die sleutel nooit gecommuniceerd.

het verschil tussen de lengte van de boodschap en

Er is nu een sleutel bekend voor de boodschap.

Eén lid van team Alice krijgt nu de code van de spelleider. Deze mag niet met anderen, ook niet met het eigen team, gedeeld worden.

Ascii tabel voor printbare karakters