

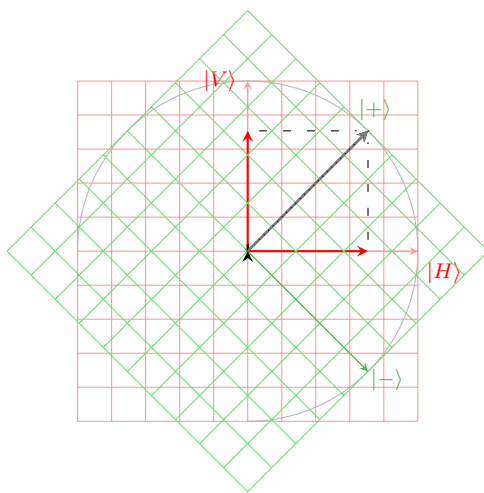
## 8.1 werkblad BB84

In hoofdstuk ?? hebben we met experimenten ?? en ?? de eigenschappen van gepolariseerd licht gebruikt om superpositie te introduceren. In hoofdstuk ?? en werkblad ?? 'Wat zie je' hebben we gezien hoe een waarnemer in een andere basis, andere coördinaten aan dezelfde vector geeft. In dit werkblad werken we met die kennis een quantumcryptie-protocol uit. Dit protocol is in 1984 door Charles Bennet en Giles Brassard [BENNETT20147] gepresenteerd en geldt als eerste voorbeeld van onkraakbare code.

naam:

klas:

datum:



$$\begin{aligned}|+\rangle &= \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle \\|-\rangle &= \frac{1}{\sqrt{2}}|H\rangle - \frac{1}{\sqrt{2}}|V\rangle \\|H\rangle &= \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle \\|V\rangle &= \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\end{aligned}$$

**Figuur 8.1:** In de standaardbasis (rood) wordt de zwarte vector met gelijke kans als  $|H\rangle$  of  $|V\rangle$  waargenomen. In de diagonale basis (groen) wordt de vector met zekerheid als  $|+\rangle$  waargenomen.

We gebruiken twee twee bases: de standaard basis en de diagonale basis. We weten hoe de Hadamard poort de standaardbasis op de diagonale basis afbeeldt én andersom (zie fig. 8.1. Voor toestandsdiagram voor de **H**-poort (zie fig. ?? en de vergelijkingen daarbij).

Fotonen zijn quantumdeeltjes die bij uitstek geschikt zijn voor het quantuminternet. Polarisaie blijft goed behouden over zeer lange lange afstanden, en fotonen reizen lekker snel, met de lichtsnelheid. Je kunt gepolariseerde fotonen versturen onder elke gewenste polarisatierichting.

In deze communicatie zijn er twee partijen, Alice en Bob die op grote afstand van elkaar mogen staan. Ze gebruiken een quantumkanaal voor het verzenden van fotonen (glasvezelkabel), en een klassiek kanaal, een af luisterbare telefoon. Het quantumkanaal is

$$|0\rangle \equiv |H\rangle$$

$$|1\rangle \equiv |V\rangle$$

$$|+\rangle \equiv |D\rangle$$

$$|-\rangle \equiv |A\rangle$$

Vraag: kan daar een versterkertje tussen zitten, het signaal is wat zwak, kan het ook met lichtpulsen

éénrichting. Alice zendt een stroom fotonen naar Bob (één richting) ieder foton in een door haar geprepareerde polarisatie. Ze noteert precies wat ze doet. Bij ontvangst meet Bob de fotonen via een polarisatiefilter dat hij willekeurig standaard of diagonaal zet. Ook hij houdt nauwkeurig bij wat hij doet. Ze verbreken de quantumverbinding en bellen elkaar. Via dit klassieke kanaal spreken ze met elkaar af (bidirectioneel) het vervolg af. We werken deze stappen verder uit.

We weten uit ?? dat als we een foton bijvoorbeeld verticaal polariseren en het vervolgens door een verticaal filter laten gaan, het foton met *zekerheid* doorgelaten wordt, en dat het met *zekerheid* geblokkeerd wordt als er een horizontaal filter volgt. Het gedrag is volledig voorspelbaar, *deterministisch*. Als een verticaal gepolariseerd foton een door een filter gaat dat onder  $45^\circ$  (of  $-45^\circ$ ) staat, is er 50% kans dat het er doorheen gaat.

Alice wil uiteindelijk een boodschap als een reeks klassieke bits naar Bob sturen. Klassieke bits hebben de waarde  $0_b$  of  $1_b$ . Ze houdt de volgende conventie aan:

bit	basis	pol
logisch $0_b$	$\oplus$	H $\leftrightarrow$
logisch $0_b$	$\otimes$	- $\nearrow \searrow$
logisch $1_b$	$\oplus$	V $\updownarrow$
logisch $1_b$	$\otimes$	+ $\nwarrow \nearrow$

Alice heeft dus twee mogelijkheden om een  $0_b$  te sturen en twee mogelijkheden voor een  $1_b$ . Als ze in de juiste basis worden waargenomen is het antwoord deterministisch. De informatie over haar eigen basiskeuze houdt Alice echter geheim. Alice heeft een string random bits gekozen en verzendt die ieder met een random basis.

Bob kan niet beter doen dan de binnenkomende fotonen meten volgens twee bases standaard (recht) en diagonaal. Bob kiest voor ieder foton een basis, en houdt nauwkeurig zowel de basiskeuze als het resultaat bij. Bob heeft geen idee of de basis waarmee hij meet

dezelfde is als waarmee ze verzonden zijn. Ze verbreken daarna hun quantumverbinding. Hier onder een uitgewerkt voorbeeld;

Alice' random bits	0	1	1	0	0	1	1	1	0	0
Alice' basis	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Alice verzendt	$\nwarrow$	$\uparrow$	$\nearrow$	$\leftrightarrow$	$\leftrightarrow$	$\uparrow$	$\nearrow$	$\nwarrow$	$\leftrightarrow$	$\leftrightarrow$
Bob's basis	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$
Bob's meting	0	1	1	0	0	0	1	1	1	0

De rest van het protocol handelen ze af ze met de telefoon: Alice en Bob melden eerst welke bij Bob zijn overgekomen. Voor het gemak hier allemaal! Bob meldt Alice in welke basis hij heeft gemeten. Alleen als hun bases overeenkomen levert het zinnig informatie. De rest gooien ze weg. Ze weten nu over welke bits zij overeenstemming hebben zonder dat de data zelf is gecommuniceerd. Zij weten beiden bijvoorbeeld of een foton in de standaard basis horizontaal of verticaal was. Elk van de overgebleven fotonen bevat één bit informatie uit Alice' random bit string.

Bob's basis	$\oplus$	$\otimes$	$\oplus$			$\otimes$			$\oplus$
Bob's meting	1	1	0			1			0

**Afgeluisterd?** Alice en Bob kunnen zijn afgeluisterd door Eve. Zij zou een foton door een filter kunnen leiden. Daarbij verliest het foton zijn eerdere informatie. Fotonen hebben geen geheugen. Ze kan het nooit meer terugzetten. Zij zou kunnen proberen een foton te versterken en dan een kopie uitlezen en het origineel doorsturen. Ook deze operatie is in tegenstrijd met de fundamente van quantumtheorie [**wootters1982single**]. Alice en Bob testen of zij zijn afgeluisterd met een aantal goedgekeurde qubits (bijvoorbeeld een kwart van het totaal). Deze qubits kunnen ze verder niet gebruiken want ze zijn openbaar gemaakt.

Bob's publiceert		1			1			
Alice bevestigt:		OK			OK			

Ze kunnen concluderen dat hun transmissie niet ernstig is afgeluisterd, anders konden ze opnieuw beginnen. Dat de overgebleven bits kunnen gebruikt worden voor een **one-time pad**. Dit is een sleutel voor de enig bewezen methode die onbrekbare vercijfering mogelijk

we gaan niet in op het volgende Bob's ver en hor basis kan wel eens gedraaid kan staan t.o.v. Alice's. Dat maakt niet uit behalve voor de sterkte van het signaal

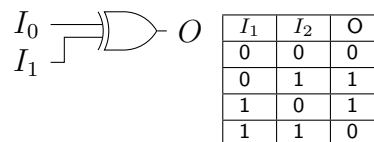
Vraag: Bij groot aantal bits, hoeveel percent komt overeen (=75 %)



one-time pad

maakt. Daarvoor moet de code nog wel aan extra eisen voldoen. Kijk op de bron welke vier eisen daar genoemd worden.

Met het verkrijgen van de sleutel houdt het BB84 gedeelte van de encryptie op. De boodschap is een binaire reeks. De sleutel is precies even lang al de boodschap. De **XOR**-poort is een logische poort (zie par. ??) met de volgende waarheidstabel (zie fig. 8.2).




**Figuur 8.2:** XOR-poort met waarheidstabel.

Alice **XOR**-t haar boodschap met de sleutel en zendt deze data over.

Bob **XOR**-t de boodschap met de sleutel. Wat is het resultaat?

Voordbeeld:

Alice' boodschap	1	0	0	1	0	1	0	0
Alice' sleutel	1	1	0	0	0	1	1	0
Alice verzendt	0	1	0	1	0	0	1	0
	⋮							
Bob ontvangt	0	1	0	1	0	0	1	0
Bob's sleutel	1	1	0	0	0	1	1	0
Bob leest	1	0	0	1	0	1	0	0

Hoeveel fotonen moet Alice versturen als zij de boodschap "Heb je vanavond wat te doen?" wil verzenden zonder dat het afgeluisterd kan worden? Om een letter over te zenden zijn acht bits nodig. De zwakke quantumverbinding verliest 20% van de qubits.

## 8.2 qauntummuntje

Alice en Bob hebben ruzie. Ze willen elkaar even niet zien. Wie mag met de auto weg? Ze bellen elkaar op. Bob ziet het al voor zich: Alice daagt uit tot een kop of munt spelletje over de telefoon. Zij vraagt kop of munt? Wat ik ook kies, zeg zegt gewoon wat haar

uit komt. Ze liegt. Dat deed ze vorige keer ook. Ze vertrouwen elkaar even niet.

(De telefoon gaat). Bob: Ja?

(Alice): Alice hier. Kan ik de auto vanmiddag ...

(Bob): Nee

(Alice): Het is ook mijn auto! Laten we er om loten?

(Bob): Ok?

(Alice): Ik gooi een muntje op. Kop of munt?

(Bob): Ja zeg, net als vorige keer zeker.

(Alice): Vertrouw je me niet?

(Bob): Nee!

(Alice): Tsss

(Bob zucht): Ok, we doen het zo. We gebruiken een quantumbasis 'R' of 'D' in plaats van kop of munt.

Alice: Hmmm, ok dan.

volgende filmpje is helaas te ingewikkeld. [filmpje TuD](#)

Alice kiest een reeks random bits (bv 1 kbit) en één willekeurige, basis, bijvoorbeeld "R". Ze kiest een codering ( $H = 1_b$ ,  $V = 0_b$ ).



Alice verstuurt haar reeks van gepolariseerde fotonen.

Bob kiest voor ieder foton dat hij ontvangt een basis, onafhankelijk en willekeurig voor elk foton.


Niet alle fotonen komen over, er zijn gaten in de ontvangstabel.

Na ontvangst Belt hij Alice en zegt welke basis zij heeft gekozen.

Als hij goed geraden heeft wint hij, anders verliest hij.

Alice meldt of Bob gewonnen of verloren heeft en zendt ter controle de reeks random bits waar zij mee begon.

Bob controleert de reeks tegen zijn tabellen. Er moet een perfecte match zijn met de tabel van Alice' basis, en een random relatie met de andere tabel.

Alice' random bits	0	1	1	0	0	1	1	1	0	0
Alice' basis	R									
Alice verzendt	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$
Bob's basis	R	R	D	R	D	D	D	R	D	R
Bob's "R"tabel	0	1		0				1		0
Bob's "D"tabel			1		1	0	0		0	
										
Bob's gok	R?									
Alice' antwoord	Haha, fout!									
Bob's gok	SStuur toch effe jouw reeks									
Alice stuurt origineel	0	1	1	0	0	1	1	1	0	0
Bob's "R"tabel	0	1		0				1		0
Bob's "D"tabel			1		1	0	0		0	

Bob: Alice! Hier met die auto!