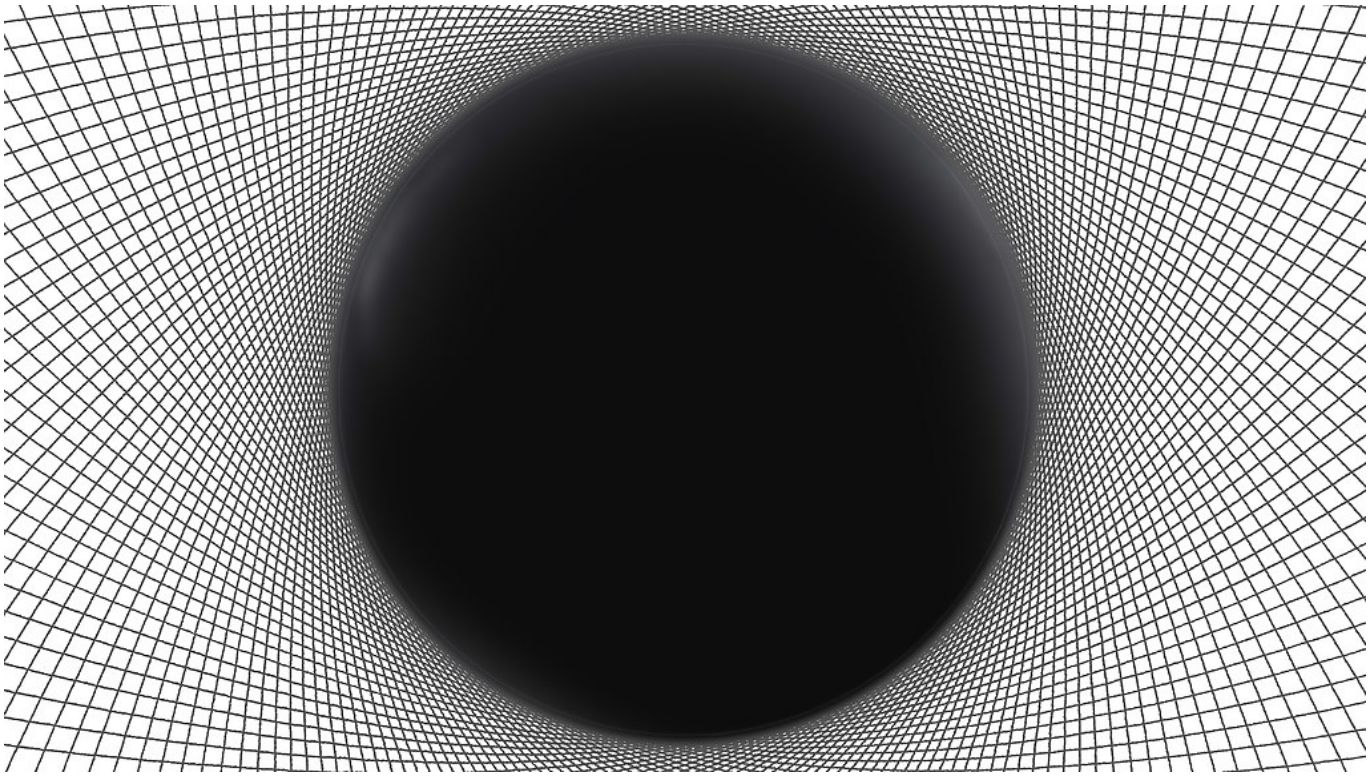
Een zwart gat als quantumversleutelaar

Als genoeg massa in een klein genoeg volume terechtkomt, wordt de zwaartekracht zo groot dat niets kan ontsnappen. Het gevolg: een zwart gat. Verrassend genoeg blijft de informatie in een zwart gat niet voor altijd verborgen: de quantummechanica voorspelt dat zwarte gaten langzaam verdampen, en daarbij hun geheimen prijsgeven. In dit artikel bespreek ik een simpel model voor dit verdampingsproces waarin zwarte gaten zich gedragen als versleutelaars van informatie.



Afbeelding 1. Een zwart gat. De waarnemingshorizon is weergeven als een zwart boloppervlak. Afbeelding: Daniel Innes.

De Hawkingparadox

Zwarte gaten hebben een waarnemingshorizon: de grens die aangeeft van waaruit iets wel of

niet kan ontsnappen. Deze horizon is wat een zwart gat zwart maakt: aangezien zelfs licht niet aan de aantrekkingskracht kan ontsnappen, zien we de horizon als een zwart boloppervlak. Maar schijn bedriegt: in tegenstelling tot bijvoorbeeld het aardoppervlak, is de horizon van een zwart gat niet massief, maar kun je er van buiten naar binnen gewoon doorheen bewegen[1]. Een zwart gat in vallen is daarmee nog geen plezierige onderneming: als je het al voor elkaar krijgt om niet uit elkaar gescheurd te worden door de heftige getijdenkrachten, is de eindbestemming voor iedere waarnemer die de horizon passeert de singulariteit, een punt met oneindige kromming. Omdat ruimte en tijd op een bepaalde manier van plek wisselen zodra je de horizon passeert, is het bereiken van de singulariteit – voor een waarnemer binnen de horizon – even onvermijdelijk als het bereiken van een tijdstip in de toekomst voor iemand die zich buiten het zwarte gat bevindt.

Het kwam als een grote verrassing toen Stephen Hawking in de jaren 70 liet zien dat zwarte gaten straling uitzenden: ze zijn niet volledig zwart! Deze *Hawkingstraling* is een gevolg van bepaalde quantumeffecten bij de horizon. Iets wat straling uitzendt verliest energie, en daarmee massa. Een zwart gat kan om deze reden – net als een kaars die opbrandt – langzaam verdampen. Een cruciaal verschil tussen het zwarte gat en de kaars is de aard van de vrijgekomen straling: uit Hawkings berekening volgt dat de vrijgekomen straling geen informatie over het vormingsproces bevat, in tegenstelling tot de warmtestraling van een kaars. De informatie van alle dingen die in het zwarte gat zijn gevallen lijkt daarmee verdwenen zodra het gat volledig is verdampt. Volgens Hawking zijn zwarte gaten in staat om informatie te vernietigen!

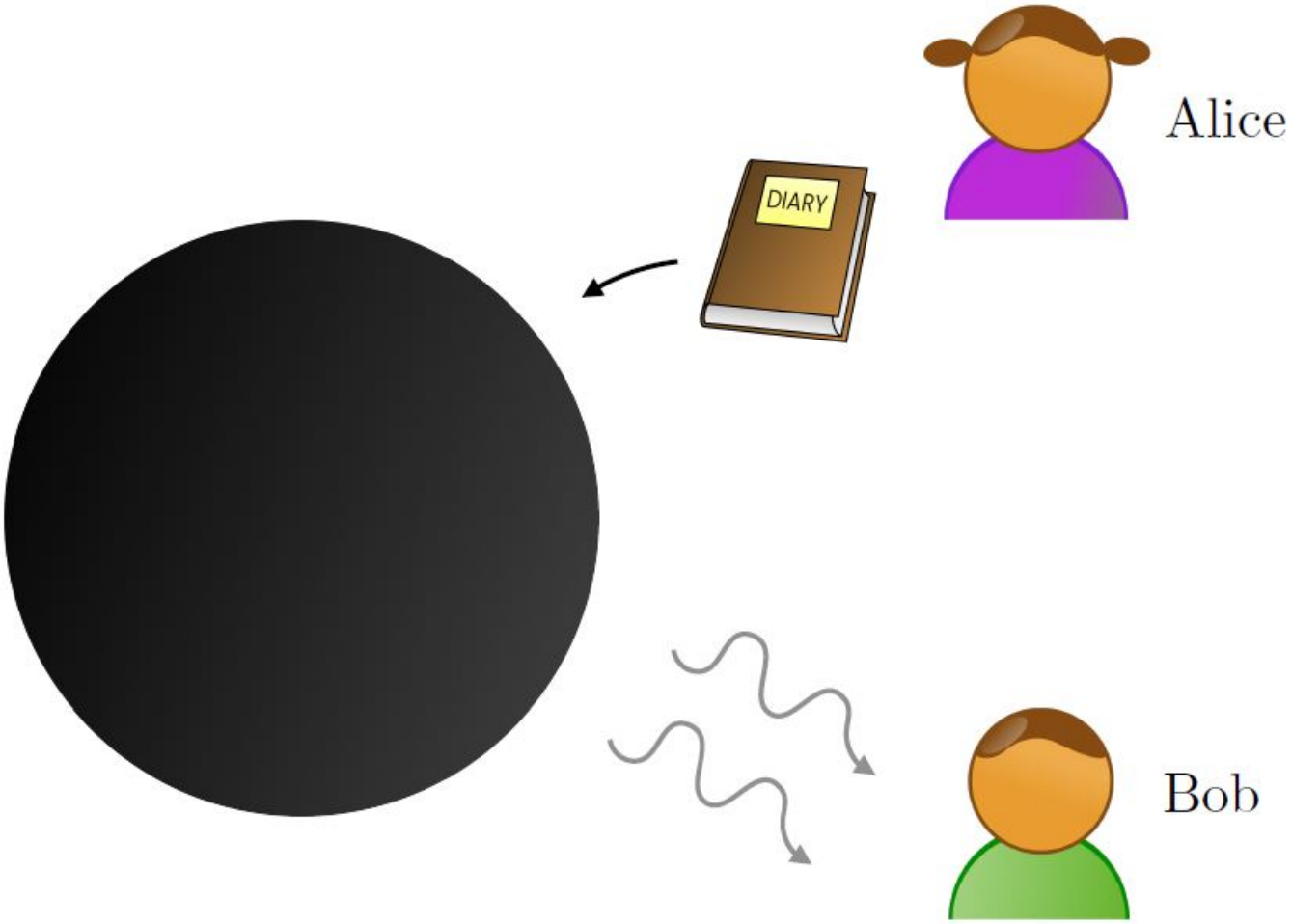
Tegenwoordig zijn de meeste natuurkundigen ervan overtuigd dat zwarte gaten, net als kaarsen en eigenlijk alle andere natuurkundige systemen die we kennen, wel degelijk informatie behouden bij het verdampingsproces. Er is een aantal goede reden (een die we al vaker bespraken is de ontdekking van de *AdS/CFT correspondentie*[2]) om te verwachten dat informatiebehoud een fundamentele eigenschap is van de natuur. De paradox – het feit dat Hawkings berekening informatieverlies voorspelt, maar dat we dat niet verwachten – komt voort uit ons onbegrip over hoe quantummechanica en zwaartekracht tegelijk moeten worden gebruikt. Tot op heden is het nog niet gelukt om precies te begrijpen hoe je beide kunt combineren, en daarmee de paradox op te lossen. Voor meer over de recente vooruitgang kun je bijvoorbeeld dit artikel eens bekijken. Voor nu doe ik de aanname dat het

verdampen van een zwart gat informatie behoudt, en dat deze inderdaad beschikbaar is in de vrijgekomen Hawkingstraling. Dan blijven er nog steeds een hoop open vragen – waarvan ik er één hier zal bespreken.

Alice en Bob

Om wat meer inzicht te krijgen in hoe zwarte gaten werken, is het nuttig om een simpel model voor het verdampingsproces te bestuderen. (Zie over dat model ook dit artikel van Evita verheijden en het vervolg erop.) We bekijken een systeem dat bestaat uit een zwart gat, een dagboek en twee bewoners van een zeer geavanceerde samenleving in de toekomst, Alice en Bob. Om het geheel wat interessanter te maken stellen we ons voor dat het dagboek bepaalde geheime informatie van Alice bevat, waarvan ze niet wil dat Bob die in handen krijgt. In een normale situatie zou Alice het dagboek waarschijnlijk weggooien of verbranden, maar Bob is uitermate handig: zo kan hij uit de overblijfselen – de straling, rook en as die vrijkomt bij een verbrandingsproces, of een hoop verscheurde bladzijdes – precies reconstrueren wat er in het dagboek stond. Daarom gaat Alice voor een nog dramatischere oplossing: ze gooit haar dagboek in een zwart gat. Dit moet toch voldoende zijn om Bob ervan te weerhouden haar dagboek te lezen?

Bob is echter ook bekend met de natuurkunde van zwarte gaten – in het bijzonder met het Hawkingproces – en besluit om rustig af te wachten tot de informatie uit het dagboek zichtbaar wordt in de uitgezonden Hawkingstraling. Zelfs een zwart gat kan Alice niet helpen! Toch heeft Bob een groot nadeel: de verdamping van een zwart gat is een extreem traag proces. Een volledige verdamping kan zo maar vele miljarden jaren in beslag nemen. De geheimen van Alice zullen dus niet voor eeuwig verborgen, maar misschien wel lang genoeg. Of toch niet?

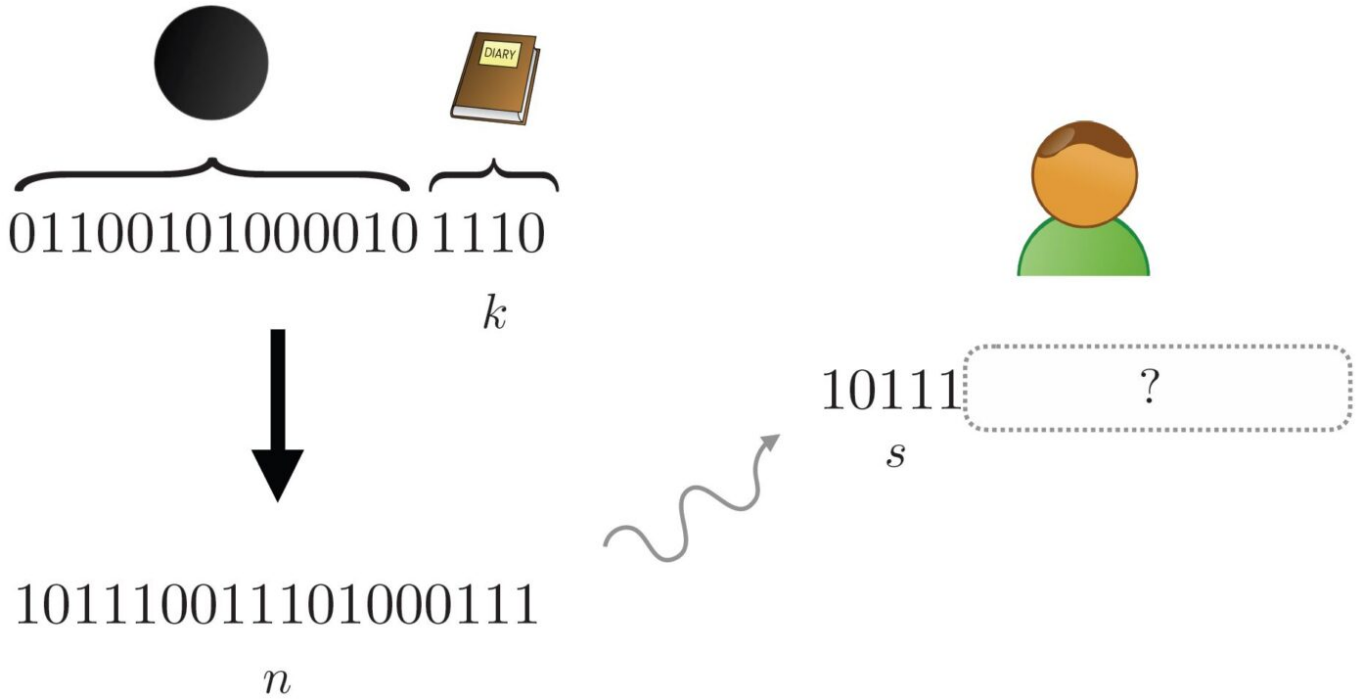


Afbeelding 2. Hoe vernietig je een dagboek? Alice gooit haar dagboek in een zwart gat, waarna Bob de Hawkingstraling opvangt en de geheime informatie probeert te reconstrueren.

Om dit te onderzoeken bekijken we eerst een klassiek model voor de verdamping: de toestand van het zwarte gat en van het dagboek worden gegeven door een reeks klassieke bits. Een *bit*, de eenheid van computertaal, staat voor een 0 of een 1. Ieder stukje klassieke informatie – denk hierbij bijvoorbeeld aan een nieuwsbericht of een afbeelding – kan worden opgeslagen als een lange reeks van zulke nullen en enen, ook wel een `*bitstring*' genoemd. De lengte van de reeks geeft grofweg aan hoeveel informatie erin kan worden opgeslagen. Voor het zwarte gat is dit natuurlijk een erg onrealistisch model – we weten dat Hawkingstraling een quantumproces is – maar voor nu nemen we daar even genoegen mee. We stellen ons het zwarte gat voor als een string van $n - k$ bits en het dagboek als een string van k bits. Het gecombineerde systeem, waarbij het dagboek in het zwarte gat is gevallen, bestaat nu dus uit n bits.

De dynamica van het zwarte gat komt in dit model als volgt tot uiting: de dagboekbits worden niet simpelweg aan die van het zwarte gat geplakt, maar ook nog eens door elkaar gehusseld (in het Engels wordt dit proces ook wel '*scrambling*' genoemd.) De *k* bits die de informatie van het dagboek bevatten zitten daarmee 'verborgen' tussen die van het oorspronkelijke zwarte gat. We kunnen ons dit scramblingproces wiskundig voorstellen als een toepassing van een willekeurige permutatie (dat wil zeggen: een verwisseling) op alle mogelijke reeksen van nullen en enen. Ik benadruk dat het hier gaat om een verwisseling van de volledige bitstring door een andere bitstring (en dus niet van de nullen en enen in de bitstring onderling.) Als je weet welke permutatie is toegepast en je de toestand van het volledige systeem kent, kun je deze verwisseling ongedaan maken, en daaruit de informatie van het dagboek herleiden.

Na deze procedure laat het zwarte gat de bits één voor één vrij in de vorm van Hawkingstraling, terwijl Bob vol verwachting toekijkt. We nemen aan dat Bob het zwarte gat lang heeft bestudeerd en de complexe dynamica ervan goed heeft begrepen: hij weet dus precies welke permutatie is toegepast, en wat de interne toestand van het oorspronkelijke zwarte gat was. Zie afbeelding 3 voor een overzicht.



Afbeelding 3. Een klassiek model voor de verdamping van een zwart gat. De gecombineerde informatie van het zwarte gat en het dagboek is opgeslagen in een reeks van n bits. De interne dynamica van zwarte gat (zwarte pijl) verwisselt deze reeks met een

andere reeks van n bits lang. Vervolgens komen de bits één voor één uit het zwarte gat in de vorm van Hawkingstraling (grijze pijl). Hoeveel bits heeft Bob nodig om de originele k bits van het dagboek te achterhalen?

Sneller dan verwacht

Hoe snel kan Bob het dagboek lezen? Als hij wacht tot het zwarte gat volledig is verdampt – zodat hij toegang krijgt tot de volledige *n*-bitstring – zou hij simpelweg de permutatie ongedaan kunnen maken, en de bits van het dagboek kunnen aflezen. Het blijkt echter dat Bob al veel sneller toegang heeft tot de informatie: hij hoeft maar iets meer dan *k* bits aan Hawkingstraling te ontvangen om het volledige dagboek (met kleine foutmarge) te reconstrueren. De geheimen van Alice worden dus helemaal niet zo goed beschermd! In feite geeft het zwarte gat bijna zo snel als mogelijk alle informatie weer vrij.

Het bovenstaande resultaat volgt uit een korte berekening. Bob heeft geen toegang tot de *k* dagboekbits van de originele bitstring. Dat geeft een totaal van 2^k mogelijke boodschappen – na toepassing van de permutatie – die kunnen overeenkomen met de oorspronkelijke bitstring. Welk van deze boodschappen is de correcte? We nemen aan dat Bob een totaal van *s* bits van deze boodschap in de vorm van Hawkingstraling heeft ontvangen. We willen nu de kans *P* berekenen dat Bob fout zit: dat een van de `verkeerde' boodschappen toevalligerwijs begint met dezelfde *s* bits. De kans dat dit voor een willekeurige bitstring gebeurd is 2^{-s}, en met een totaal van $2^k - 1$ verkeerde boodschappen kan de volgende bovenschatting voor de foutkans worden afgeleid[3]:

$$P \leq 2^{-s} \cdot 2^{k} = 2^{-c}, \quad s = k + c .$$

Hieruit volgt dat Bob een totaal van $k + c$ bits nodig heeft om de kans op een fout kleiner te maken dan . De *c* extra bits zijn over het algemeen verwaarloosbaar in vergelijking met het aantal bits *k* dat nodig is om bijvoorbeeld een volgeschreven dagboek op te slaan.

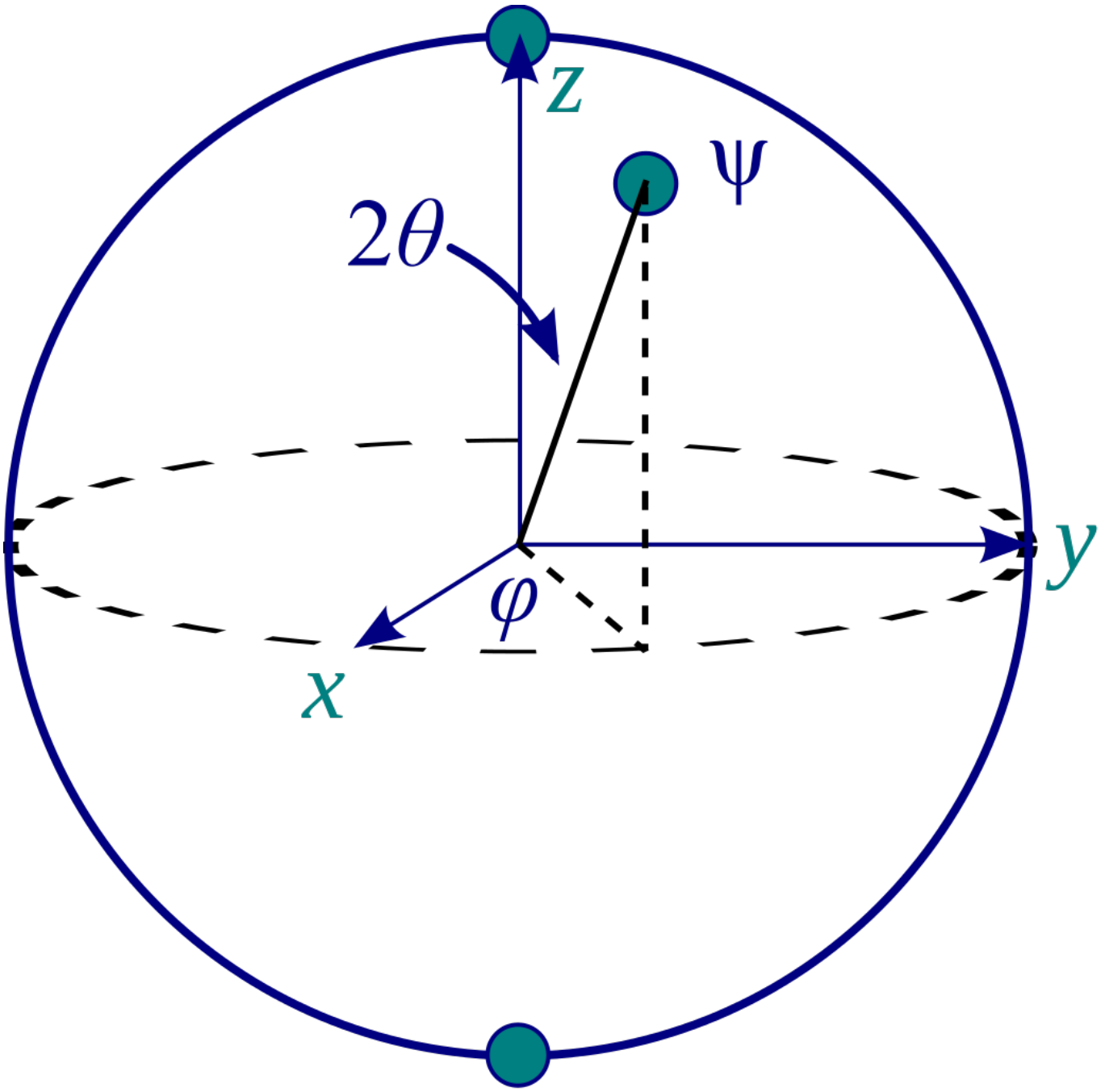
Conclusie: Bob hoeft maar heel even te wachten. Zodra er iets meer dan het aantal bits van het dagboek zelf uit het zwarte gat komen kan Bob met goede zekerheid zeggen wat het dagboek zegt. Ik benadruk nogmaals dat de bits die Bob opvangt uit de straling niet direct gelinkt zijn aan de originele bits van het dagboek; het kunnen ook willekeurige bits van het

originele zwarte gat zijn. In dit simpele model lijken zwarte gaten meer op `informatiespiegels': ze kaatsen de informatie die je erin gooit zo snel als kan weer terug.

Quantumfoutcorrectie

Het bovenstaande proces kunnen we ook als volgt interpreteren: zwarte gaten zijn in staat om de informatie van het dagboek te versleutelen in een boodschap die robuust is tegen het wegvallen van een groot deel van de informatie. De *k* dagboekbits – dit is de relevante informatie – worden opgeslagen in een boodschap van *n* bits, en die worden met behulp van een permutatie vervangen door andere bits – dit geeft de versleutelde boodschap. Het blijkt nu dat we maar een klein deel van de versleutelde boodschap, namelijk iets meer dan *k* bits, nodig hebben om de originele informatie terug te vinden. Dit is een typisch kenmerk van bepaalde versleutelingscodes uit de informatietheorie die gebruikt worden om fouten te corrigeren (zie bijvoorbeeld dit artikel.) Zo'n versleutelingsmethode is erg handig als je een belangrijke boodschap wilt versturen, maar last hebt van ruis die een deel van de boodschap laat wegvallen.

Tot nu toe ben ik natuurlijk veel te snel gegaan: ik trek conclusies over het quantumgedrag van zwarten gaten door een extreem simpel klassiek model te bekijken. Het blijkt echter dat je een soortgelijke analyse kunt maken in het geval van *qubits*, de quantumversie van een klassieke bit. De relevante berekeningen zijn technisch wat ingewikkelder, maar conceptueel blijft de conclusie hetzelfde: ook in het geval van quantuminformatie heb je maar een klein deel van de Hawkingstraling nodig om de originele boodschap te reconstrueren. Het feit dat we met quantuminformatie te maken hebben maakt bepaalde aspecten wel wat ingewikkelder: zo is het in de quantumwereld niet mogelijk om een exacte kopie van een toestand te bezitten. (Dit resultaat staat bekend als 'no-cloning'.) Bobs kennis over de interne toestand van het zwarte gat wordt in dit geval vertaald naar het bezit van een quantumtoestand die maximaal *verstrengeld* is met het zwarte gat. Om zo'n toestand te bereiken moet Bob eerst wachten tot de helft van het zwarte gat is verdampt[4]: de vrijgekomen Hawkingstraling is nu maximaal verstrengeld met het overgebleven zwarte gat.



Afbeelding 4. Een qubit. De toestand van een qubit wordt wiskundig vaak voorgesteld als een punt op het oppervlak van een bol: de situatie is dus iets ingewikkelder dan met een klassieke bit die alleen 0 of 1 kan zijn. De quantumversie van het verdampingsmodel – het zogenaamde Hayden-Preskillprotocol – wordt daarmee ook iets moeilijker. Afbeelding via Wikimedia Commons.

De exact procedure om de informatie van het dagboek te reconstrueren wordt het *Hayden-Preskillprotocol* genoemd, en heeft veel weg van een een protocol voor *quantumteleportatie* – een manier om quantuminformatie te teleporteren. Aan de details van deze methode kan

een heel nieuw artikel worden gewijd. Voor nu is het leuk om op te merken dat het verband met foutcorrectiecodes – dat we in het klassieke model vonden – ook in de quantumversie aanwezig is. *Quantumfoutcorrectie* is een zeer interessant vakgebied waarin technieken worden ontwikkeld om quantuminformatie robuust te maken tegen verstoringen. Erg relevant gezien de huidige ontwikkeling van quantumcomputers: die worden namelijk geplaagd door zulke verstoringen; quantuminformatie is veel gevoeliger dan klassieke informatie en kan bij de minste of geringste verstoring al onbruikbaar worden. Wie had dat gedacht: dat zwarte gaten ons iets kunnen leren over de technologie achter quantumcomputers (en vice versa)!

Samenvattend: zwarte gaten gedragen zich anders dan je misschien zou verwachten; het zijn een soort `informatiespiegels'. Wanneer je geheime informatie – bijvoorbeeld in de vorm van een dagboek – wilt vernietigen is een zwart gat wellicht niet de beste optie: uit de Hawkingstraling die vrijkomt bij het verdampingsproces kan de geheime informatie al snel worden gereconstrueerd. Je hoeft maar een paar bits meer te ontvangen dan de originele boodschap. Anders gezegd: zwarte gaten zijn goed in het versleutelen van quantuminformatie zodat deze robuust is tegen verstoringen: een belangrijk kenmerk van quantumfoutcorrectiecodes. Over de relatie tussen de twee valt nog veel te leren – laten we hopen dat de geheimen van ons universum, net als die van Alices dagboek, niet al te lang versleuteld blijven.

---

[1] Dit is wat de meeste natuurkundigen verwachten. Er zijn in de loop der jaren ook andere voorstellen geweest: één daarvan – die onder de naam `firewall' bekend staat – stelt dat de gebruikelijke noties van ruimte en tijd al ophouden te bestaan bij de horizon. De waarnemer kan in dat geval de horizon niet zonder meer passeren, en komt een ondoordringbare `muur van vuur' tegen.

[2] Zie bijvoorbeeld dit artikel waarin ik kort de AdS/CFT correspondentie bespreek.

[3] Zie bijvoorbeeld het originele artikel van Patrick Hayden en John Preskill, waarin ze dit resultaat interpreteren als een resultaat over klassieke errorcorrectiecodes in de informatietheorie waarbij een deel van de code wordt gewist.

[4] Dit tijdstip wordt ook wel de ‘Pagetijd’ genoemd.