Quantum Rules!

aantekeningen (uit bronnen van) EdX course

idee: Moeder Natuur berekent

Hefboom: gewogen gemiddelde

serie weertanden: optellen

parallelle weerstanden: reciprook optellen lenzenformule twee gewichten op een weegschaal

Maar er zijn meer regels. Voor quantum systemen kun je beter quantumregels gebruiken. Berekenen van chemische substanties

bronnen Quantum Zoo [1] Quanttiki [2]

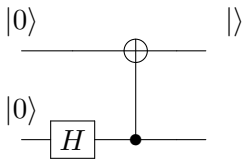
bij de vragen: parser geeft het geinterpreteerde getal weer. Hiervoor is een submit knop nodig Die heb je ook nodig voor een meermerkeuzevraag Understanding chemistry Zuurstof met twee streepjes

De covalente binding Uitleg in Absolutely small

The focus in QM is shifting from

$$\frac{i}{\hbar}\frac{d\Psi}{dt} = H\Psi$$

to



information

Nice: Solving a maze animation

Challenges for society

- spoiling enery
- waisint materials
- climate is changing too fast
- need for medicine
- ..
- electrical cables without loss of energy
- Drug development (Quantum Chemistry)
- Predicting material properties for electronics, energy storage
- machine learning
- optimization in robotics
- handling big data for sequencing genomics
- airplane desing
- ..

[1] https://math.nist.gov/quantum/zoo/

[2] https://www.quantiki.org/wiki/teleportation-protocol

photosynthesis pathway antenna chlorophyll: extreme fast solving of labyrinth

film Lieven van der siepen: Twee mensen lopen in schadusspel en botsen, of lopen langs elkaar . (plato's grot, superpositie)

film how to iunderstand superposition Stel dat electronen twee eigenschappen hebben, kleur en hardheid

kleur: [B,W] hardheid: [H,S] (hmm zacht en zwart zelfde letter) twee apparaten: een om kleur te sorteren, en een om hardheid te sorteren (eigenlijk spin in twee verschillende richtingen,

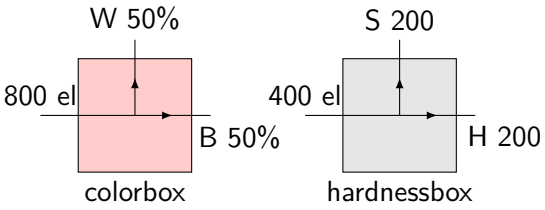


Fig. 1: experiment 1

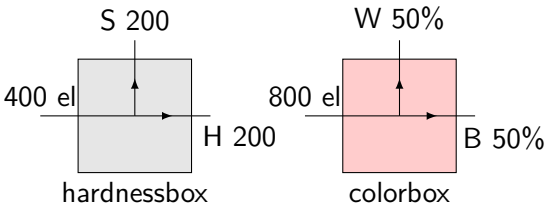


Fig. 2: experiment 2

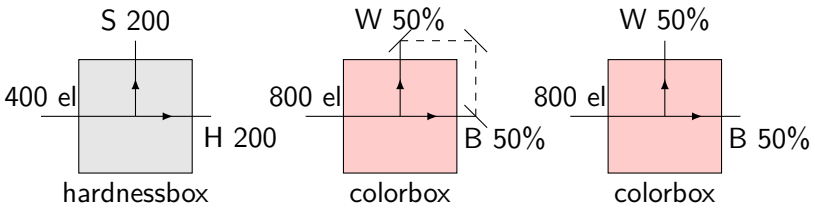


Fig. 3: experiment 2

module 2

trage video: superposition interference entanglement cloning is not possible error correction not simple but can be done

Divicencio

- QC must be scalable

- Qbits must be initiable
- good qbits are needed, long coherence
- have a universal set of quantum gates
- you can measere them

video high-level languare to compiler error correction converted into quantum instructions converted into physical signals (pulsees) to control and operate physical qubits time constraint synchonicity is a challenge

video what is q internet?

technologies not available in classic internet

- secure communication
- secure identification
- position verification
- secure dedicated computing
- ...

end node are qcompters small ones, less than 10 qb, mosly 1 qb is enough power of entanglement incontrast on a qc we always need more qubits than can besimulated on a classical computer in order to do something new and interesting ??

switches repeaters traffic control

why powerful? secure - not qubits cannot copied

entangelment maximum coordination (=maximum correlation??) only two qubits can be maximally entangled

module 3

classic factoring goes with 2^n quantum factroing N^3 -hard to build - need large nr of qubits to factor: a number of 2000 bitswill take 10000 qubits minimum Redundancy needed for erroro correction vcan be factor of 1000-10000 So for now we are safe, but in 10-20 yrs other encryption systems are rerquitred

video encryption

classic: shared key One Time Pad The message and key have the same length Message and key are bitwise multiplied modulo 2 msg 0110 key 1010 enc 1100 if key==message send 0 else send 1 Bob can reverses the operation

msg .... key 1010 enc 1100

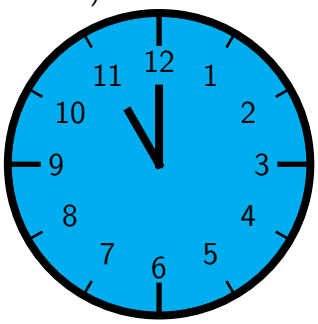
Eve cannot decrypt the message if she has no info on the key

Sannon proved that to be totally secure, you need a key just as long as the message A BW image 64x64=4096 bits info would require a 4096 bit key

in practice keys are much shorter

The number of key is limited. Easy proof (??)

A little variation of an example taken from the PGF documentation (Section 83 Repeating Things: The Foreach Statement, page 912 for version 3.0):



regels klok liegt niet (6 of 12) en (3 of 9).

Korte filmpjes -collapse in superposition (ps duidelijk na spel met klok)

bit flip uitleg bitflip / sign flip is me onduidelijk

iig computational basis (6,12), Hadamard basis (3,9) scenarios's met Alice, Bob, Eve niet moeilijk.

module3, Learn more

learn more encryptie methoden **RSA** http://doctrina.org/How-RSA-Works-With-Exa html lastiger. meer voorbeelden bij multiplicatieve inverse nodig.

eulersś totient

shor's algorithm (wikipedia pagina) veel te lastig

caesar's cipher te simpel

enigma machine interessant maar off topic?

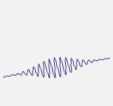
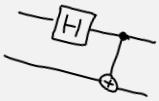
braket wikipaedia artikel overstijgt vwo niveau

BB84 Bennett and Brassard 1984 https://www.youtube.com/watch?v=UVzRbU6y7Ks&feature=youtu.be zie ook teoelichting bij video.

volgt logischerwijs op spel met de klok

uit https://www.youtube.com/watch?v=7SMcf1MdOaQ:




Quantum Rules!

//table op zijn plek houden

Alice's bit value	1	0	0	1	0	1	1	1
Alice's sending mode	+	+	+	X	X	+	+	+
Bob's receiving mode	+	+	X	+	+	+	+	X
Bob's result	1	0	0	0	0	1	1	0
Same mode?	Y	N	Y	N	N	Y	Y	N
Shared secret key	1		0			1	1	

Tabel 1: BB-84