Kwantumcomputers: razendsnel rekenen op de kleinste deeltjes

Door Aad Offerman, dinsdag 21 januari 2014 08:00, reacties: 103, views: 167.608 • Feedback

Kwantumbeveiliging met een Nederlands tintje

Kwantumcomputers maken ook nieuwe beveiligde communicatiemethoden mogelijk. Kwantummechanische verstrengeling kan bijvoorbeeld gebruikt worden om absoluut veilige communicatiekanalen op te zetten. Informatie kan onderweg niet worden afgeluisterd door een man-in-the-middle zonder dat dit aan de uiteinden van de verbinding te zien is.

> Het Majoranadeeltje zou een geschikte bouwsteen voor de qubits kunnen zijn

Hiertoe wordt eerst een serie paarsgewijs verstrengelde qubits over de twee partijen verdeeld, quantum key distribution, om die vervolgens te laten ineenstorten tot hun definitieve waarde. Beide partijen hebben nu dezelfde, of nauwkeuriger gezegd, tegenovergestelde sleutel. Ze kunnen dat controleren door een deel van de zo verkregen bits met elkaar te vergelijken. Komen die bits inderdaad met elkaar overeen, dan weten de partijen zeker dat niemand anders die sleutel heeft. Een man-in-the-middle kan de waarde van een verstrengelde qubit onderweg immers niet achterhalen zonder deze te laten ineenstorten. Op deze manier wordt het distributieprobleem voor symmetrische sleutels opgelost. Dat is waarvoor asymmetrische cryptografie vaak wordt ingezet: het veilig uitwisselen van een symmetrische sessiesleutel.

Belangrijke kanttekening hierbij is dat dergelijke kwantumsystemen wel kunnen worden gebruikt om sleutels uit te wisselen, maar niet om sneller dan het licht te communiceren. De ineenstorting aan twee zijden gebeurt inderdaad sneller dan het licht, maar doordat de concrete uitkomst door het toeval wordt bepaald, kan daarbij geen informatie worden overgedragen.

Wetenschappelijk onderzoek

In de afgelopen jaren zijn her en der bij universiteiten en andere onderzoeksinstellingen de eerste kwantumnetwerken gebouwd waarmee verstrengelde communicatiekanalen en teleportatie van kwantumtoestanden mogelijk worden. Zo lieten onderzoekers uit het Britse Cambridge vorig jaar zien dat het mogelijk is om verstrengelde fotonen via een regulier glasvezelnetwerk te verspreiden.

In Nederland wordt theoretisch onderzoek naar kwantumalgoritmen en complexiteit uitgevoerd door het CWI. Daar draait een groep onder leiding van Harry Buhrman mee met de wereldtop op dit gebied. Andere belangrijke onderzoeksgroepen bevinden zich in Zürich (ETH), Oxford en Cambridge in de UK, Cambridge in de VS (MIT), Berkeley, Waterloo (Canada), Singapore en Beijing.

Majoranadeeltjes

Ook wat de onderliggende hardware betreft is Nederland een belangrijke speler. Een jaar geleden verwierf de Delftse onderzoeksgroep van Leo Kouwenhoven wereldfaam met de ontdekking van het Majoranadeeltje. Behalve voor het Standaard Model heeft dit deeltje in het bijzonder waarde voor ontwikkelaars van kwantumsystemen. Het zou namelijk wel eens een geschikte bouwsteen voor de qubits kunnen zijn.

Ook elders in de wereld gebeurt van alles. Tweakers brengt regelmatig nieuws over technische en wetenschappelijke doorbraken op dit gebied. In die berichten kunnen we lezen hoe wetenschappers steeds meer en steeds stabielere qubits kunnen creëren, opslaan en transporteren. Bovendien lijkt het

Door Aad Offerman - Freelancer

Aad Offerman is al meer dan tien jaar actief als vakjournalist, technologie-auteur, bladenmaker en New Media-specialist in de Nederlandse ict-markt. Hij is afgestudeerd in de Technische Informatica aan de TU Delft, waar hij zich heeft gespecialiseerd in Computer Architectuur en Digitale Techniek. Daarnaast hoopt hij volgend jaar als psycholoog af te studeren aan de Universiteit Leiden, waar hij zich specialiseert in theoretische en klinische psychologie.

Inhoudsopgave

1. Inleiding
2. Bits, qubits en superposities
3. Genormaliseerde golffuncties en amplitudes
4. Rekenkracht, kansverdeling en kwantumberekening
5. Modellering en berekenbaarheid
6. **Kwantumbeveiliging met een Nederlands tintje**
7. De 1bit-kwantumcomputer

Reacties (103)

Lees meer over

Wetenschap

Canadese bedrijf D-Wave inmiddels inderdaad de eerste commerciële kwantumcomputer te kunnen aanbieden.

Volgende pagina
7. De 1bit-kwantumcomputer

Inhoudsopgave

1. Inleiding
2. Bits, qubits en superposities
3. Genormaliseerde golffuncties en amplitudes
4. Rekenkracht, kansverdeling en kwantumberekening
5. Modellering en berekenbaarheid
6. Kwantumbeveiliging met een Nederlands tintje
7. De 1bit-kwantumcomputer
Reacties (103)