Quantencomputing und die Bedrohung für die Sicherheitstechnik

Deni Almasov-Misaev Tobias Brandner

Universität Salzburg

April 1, 2024

Inhaltsverzeichnis

Klassische Computer

- Bits als kleinste Dateneinheit. (0 oder 1)
- Breites Spektrum an Anwendungsgebieten. (Alles was ein Quantencomputer berechnen kann, kann ein klassischer Computer genauso berechnen. Oft ist der Klassische Computer sogar schneller.)
- Relativ geringe Produktionskosten im Vergleich zu Quantencomputern.
- Basierend auf klassischer Physik und Elektronik.

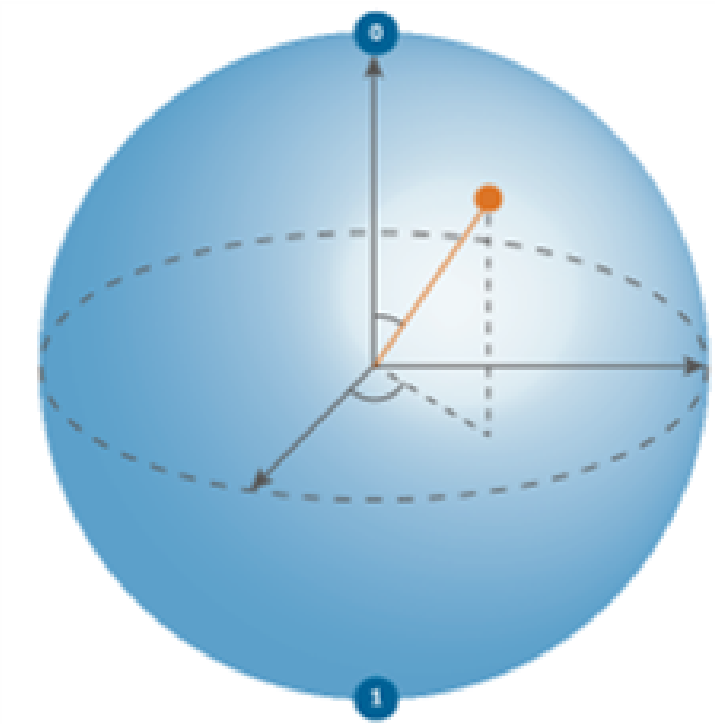
Quantencomputer

- Quantenbit (=Qubit) als Dateneinheit. Nehmen erst bei Messung einen binären Zustand an.
- Spezialisierte Anwendungsgebiete wie Kryptographie, Logistik, Materialwissenschaften und Simulationen.
- Hohe Produktions und Unterhaltskosten.
- Basierend auf Quantenmechanische Phänomene wie Superposition, Verschränkung und Interferenz. Diese ermöglichen einen Zustand namens Quantenparallelismus, der die enorme Rechenleistung von Quantencomputern ausmacht.

Qubit

- Kleinste Einheit in einem Quantencomputer. Vergleich: Normaler Bit in einem klassischen Computer.
- Kann aus verschiedenen "Materialien" hergestellt werden. Quantensysteme von Photonen, Ionen oder Moleküle (und vieles mehr) werden hier ausgenutzt.
- Erhalten ihre Eigenschaften durch die Quantenmechanischen Phänomene der oben erwähnten "Materialien".
- Werden durch Wellenfunktionen beschrieben, welche durch Modelle wie die Bloch-Kugel veranschaulicht werden.

Bloch-Kugel

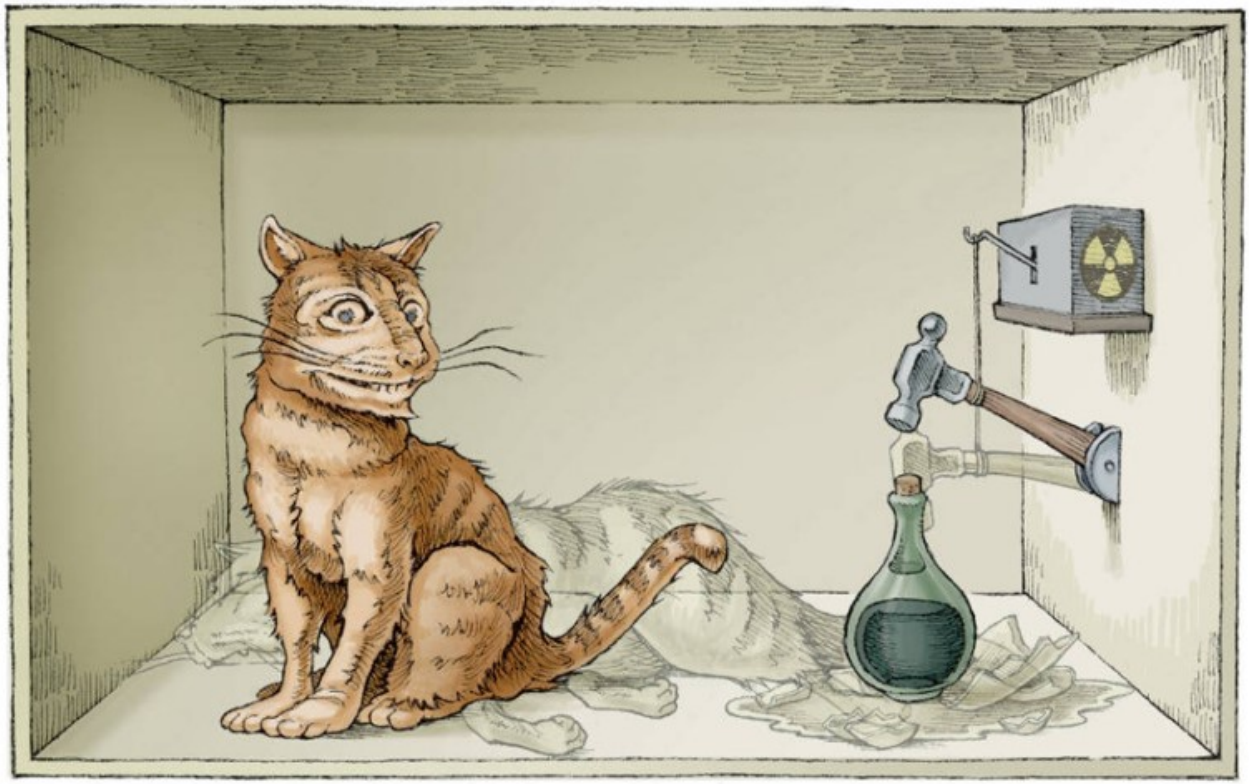


Quelle: `https://www.sciencenews.org/article/quarter-century-ago-qubit-was-born`

Superposition

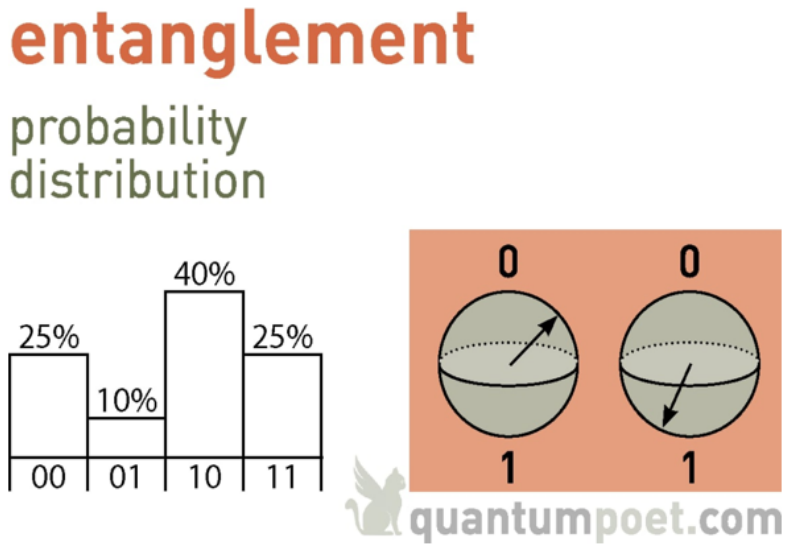
Superposition ist ein Quantenmechanisches Phänomen, welches Teilchen ermöglicht, sich in mehreren Zuständen gleichzeitig zu befinden. Dies ermöglicht Quantencomputern mehrere Rechnungen gleichzeitig durchzuführen (Quantenparallelismus), dabei nehmen Qubits erst zum Zeitpunkt der Messung einen binären Zustand ein.

Schrödingers Katze



Quelle: https://www.faz.net/aktuell/wissen/physik-mehr/die-seltsame-welt-der-atome-schroedingers-katze-erhellt-das-quantenreich-12529251.html

Verschränkung



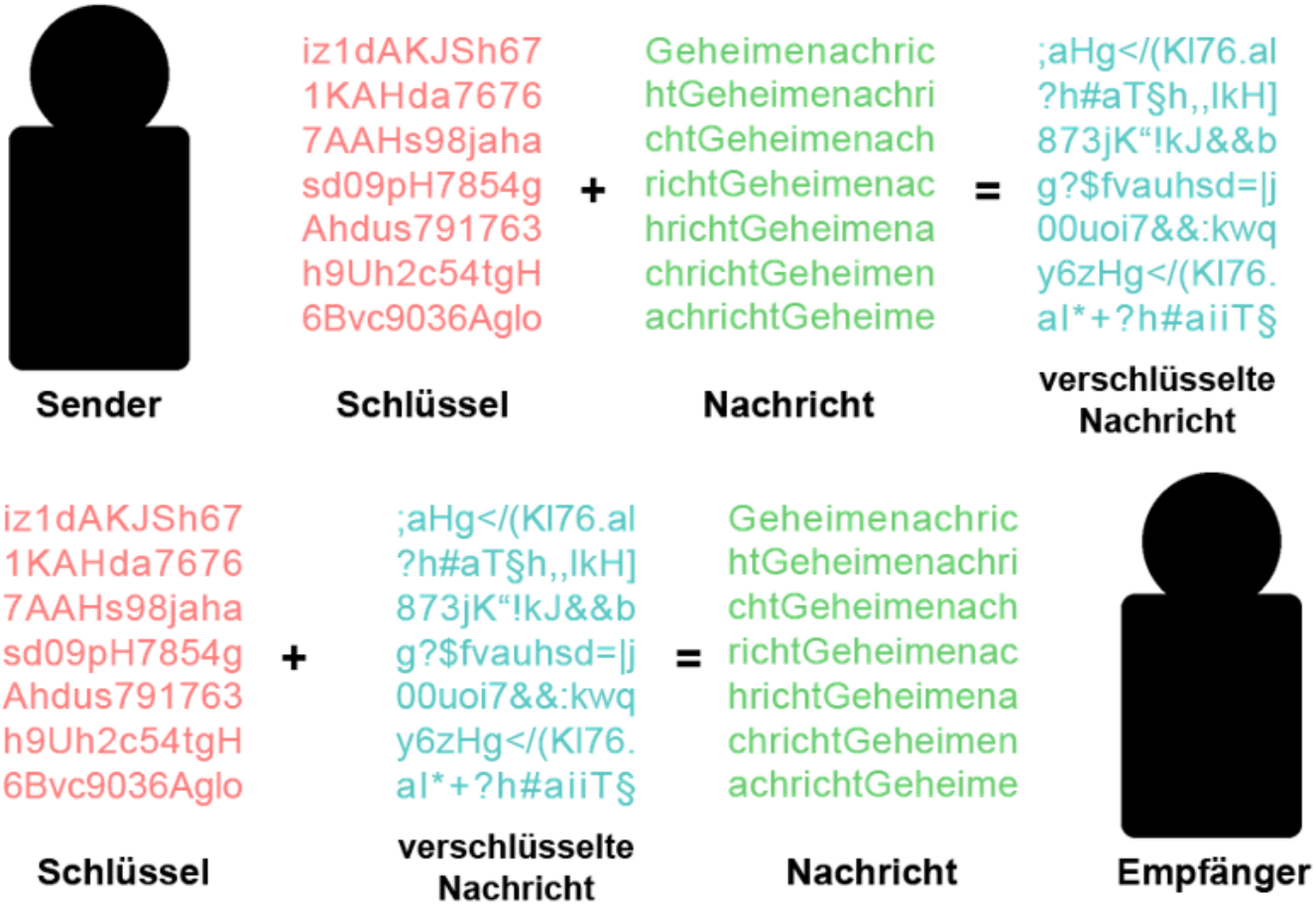
Number of Qubits	Number of States
1	2
2	4
3	8
4	16
…	…
N	2^N

Quelle: `https://quantumpoet.com/quantum-computing-introduction/`

Interferenz

Qubits werden durch Quantenwellenfunktionen repräsentiert, diese beschreiben die Überlagerung verschiedener Zustände. Es können konstruktive und destruktive Interferenzmuster erzeugt werden, um das gewünschte Ergebnis zu erzielen.

Symmetrische Kryptographie



Asymmetrische Kryptographie

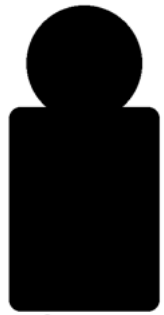
z.B. RSA (Rivest, Shamir, Adleman):

Private Keys		Private Keys		Public Key
64135289477071		33372027594978		2140324650240744961264423
58027879019017		15655622601060		0728393335630086147151447
05773890848250		53551142279407		5501779775492088141802344
14742943447208		60344767554666		7140136643345519095804679
11685963202453	x	78452098702384	=	6109928518724709145876873
23446302386235		17292100370802		9626192155736304745477052
98752668347708		57448673296881		0805119056493106687691590
73766192558569		87756571898625		0197594056934574522305893
4639798853367		8036932062711		2597669747168173806936489

Linke Zahl (RSA-250) faktorisiert in 2700 CPU-Jahren

(RSA Factoring Challenge)

Empfänger



Sender

Kryptographie - Vergleich

Symmetrische Kryptographie

1. Gleicher, geheimer Schlüssel für Ver- und Entschlüsselung.
2. Standards:
   - Advanced Encryption Standard (AES)
   - Data Encryption Standard (3DES)
3. Geringe Bedrohung durch Quantencomputing.

Asymmetrische Kryptographie

1. Unterschiedliche Schlüssel für Ver- und Entschlüsselung.
2. Nutzt schwierige Mathematische Probleme zur Berechnung von Schlüsseln:
   - Faktorisierung (RSA)
   - Diskreter Logarithmus
   - ...
3. Bedroht durch Quantencomputing.

Sicherheit von Verschlüsselungsmethoden

Tabelle: Vergleich der Effektivität verschiedener Verschlüsselungs-Standards nach Quantencomputing

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

"The impact of quantum computing on present cryptography", S.4

Shor's Algorithmus (vereinfacht)

- N... Nummer die faktorisiert werden soll
- Wähle x sodass $0 < x < N$
- Rechne x hoch $0, 1, ..., N$
- Dividiere jedes Ergebnis $(x^0, x^1 x^2, ...)$ durch N und speichere den Rest

- In den Resten ergibt sich eine sich wiederholende Sequenz
- Extrahiere (Quanten Fourer Transformation) die Periodendauer p

- Möglicher Faktor $F = x^{p/2} - 1$

Folgen für Kryptographie

- Meistgenutzte Verschlüsselungsverfahren werden unsicher.
- Quantenresistente Algorithmen nötig.
- Harvest now, decrypt later.
- Daten schon jetzt nicht mehr "sicher".

Kryptographie nach dem Quantencomputer

- Nutzung von Quantenmechanik in der Kryptographie:
  - Prepare-and-measure (Heisenbergsche Unschärferelation)
  - Verschränkungsbasierte Protokolle (Verschränkung)
- Andere mathematische Ansätze:
  - Matrixmultiplikation
  - Multivariate Polynome
  - Hashing
  - ...
- Symmetrische Kryptographie mit größeren Schlüsseln
  - z.B. Advanced Encryption Standard (AES)

Quellenverzeichnis

- https://www.sciencenews.org/article/quarter-century-ago-qubit-was-born (Zugriff 01.04.2024)
- https://www.faz.net/aktuell/wissen/physik-mehr/die-seltsame-welt-der-atome-schroedingers-katze-erhellt-d html (Zugriff 01.04.2024)
- https://quantumpoet.com/quantum-computing-introduction/ Zugriff(01.04.2024)
- Shor, Peter W. "Quantum computing." Documenta Mathematica 1.1000 (1998): 1.
- Mavroeidis, Vasileios, et al. "The impact of quantum computing on present cryptography." arXiv preprint arXiv:1804.00200 (2018).
- https://www.schneier.com/blog/archives/2020/04/rsa-250_factore.html (Zugriff: 01.04.2024)