Razvoj kvantnih računara

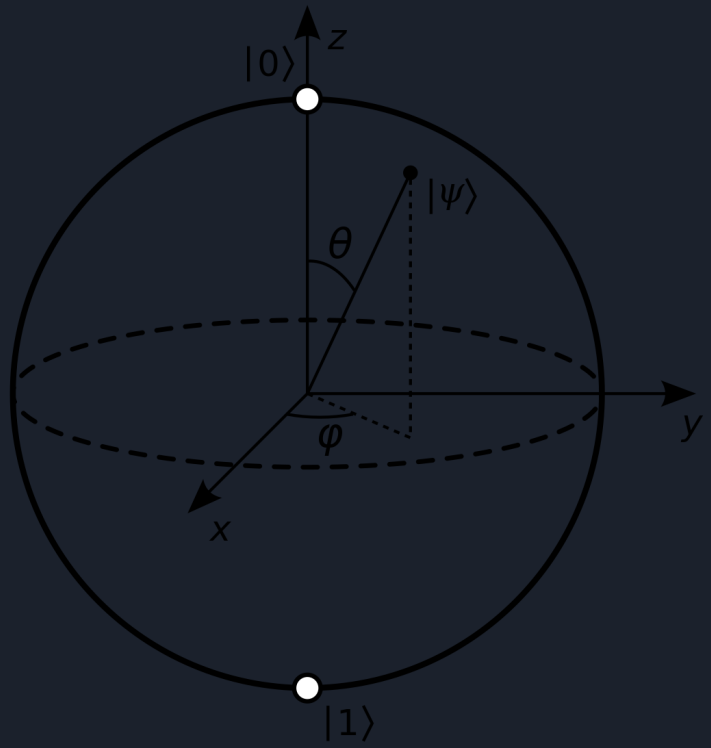
Pavle Veličković 67/2017

Šta su kvantni računari?

- Računari zasnovani na principima kvantne mehanike
- Koriste kvantne bitove tj. qubite
- Primenjuju fenomene kvantne mehanike pri računanju

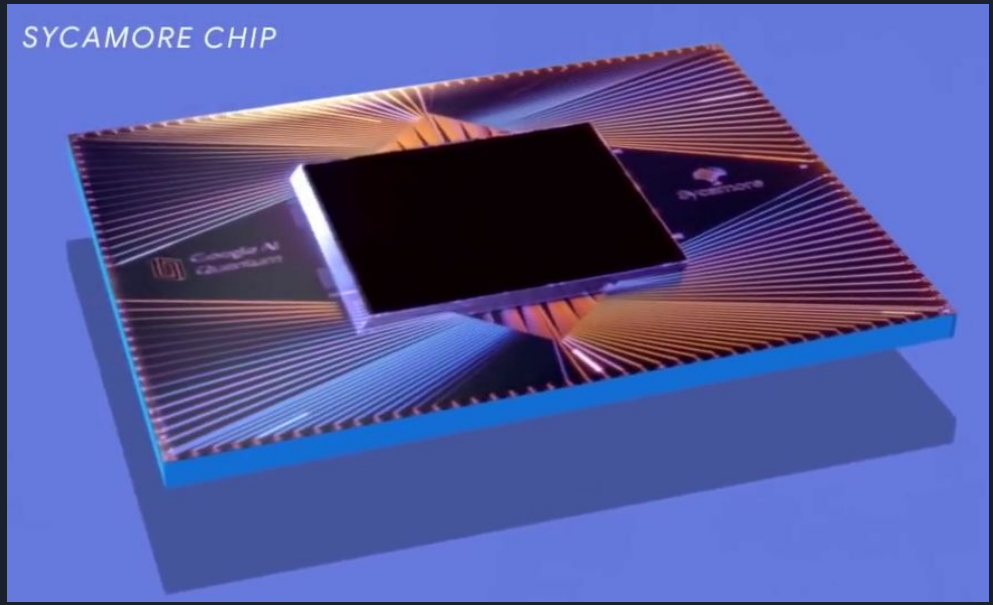
Razlika između bitova i qubita

- Bitovi imaju dva stanja, 0 i 1
- Uvek su u jednom od ta dva stanja
- Qubiti takodje imaju dva stanja, 0 i 1
- Qubiti mogu biti u superpoziciji stanja
- Superpozicija se opisuje talasnom funkcijom
- Qubiti mogu biti upleteni



Qubit tehnologije

- Postoje razni načini za konstruisanje fizičkih qubita
- Zarobljeni jonski qubit
- Superprovodnički qubit
- Ostale tehnologije (fotoni, neutralni atomi, itd.)

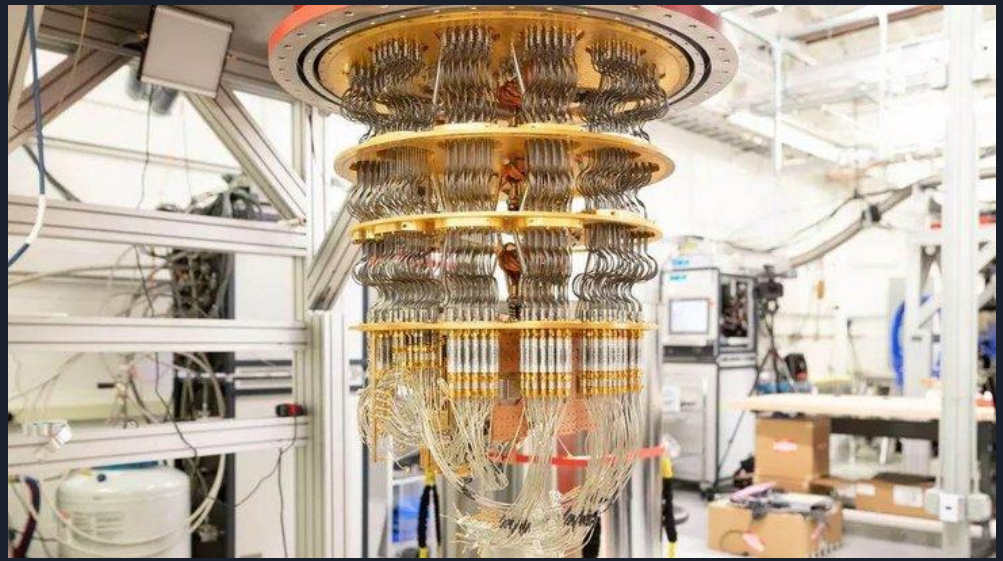


Dobre strane kvantnih računara

- Potencijalno mnogo brži od klasičnih
- Kvantni algoritmi mogu da ubrzaju rešavanje problema efikasnijim izračunavanjima, korišćenjem principa kvantne mehanike
- Kvantni algoritmi su kompozicija kvantnih algoritamskih primitiva
- Kvantne algoritamske primitive su izvor kvantnog ubrzanja
- Groverov algoritam pretrage
- Kvantne simulacije

Kvantna nadmoć

- Trenutak kada kvantni računari postanu brži od klasičnih za neke probleme



Loše strane kvantnih računara

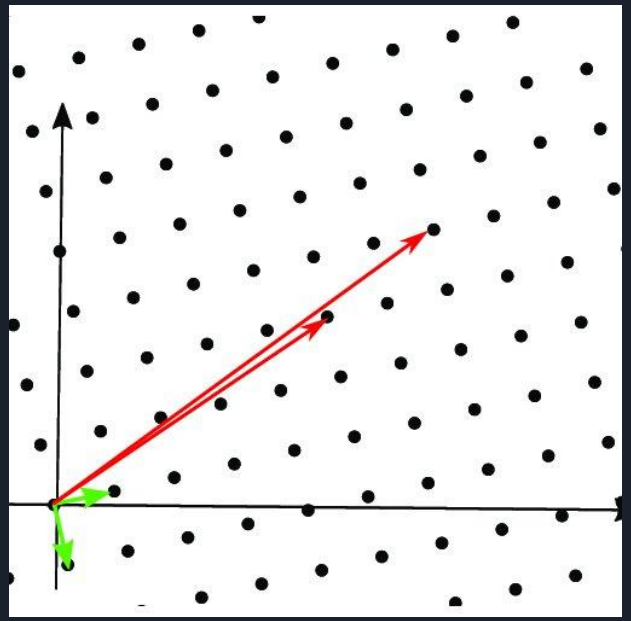
- Razvoj i konstrukcija su skupi
- Ne zna se da li će biti korisni i da li će zaživeti
- Veoma ograničena primena
- Ugrožavanje trenutno široko zastupljenih kriptosistema probijanjem enkripcije

Šorov algoritam

- Kvantni algoritam za faktorizaciju velikih brojeva
- Enkripcija se zasniva na one-way funkcijama
- Često korišćen RSA sistem je zasnovan na težini faktorizacije velikog broja na velike proste brojeve
- Šorov algoritam koristi svojstvo da za 1<x<n važi da postoji r tako da $x^r \equiv 1 \pmod{n}$, tražimo najmanje takvo r
- Kvantni računar može veoma brzo da nađe r koristeći superpoziciju i kvantnu Furijeovu transformaciju
- Ako znamo r, možemo veoma brzo da nadjemo faktore broja n
- Šorov algoritam je znatno brži od bilo kog algoritma za faktorizaciju koji klasični računari mogu da koriste

Post-kvantna kriptografija

- Potrebno je naći bolje enkripcione algoritme i dobiti kriptosistem otporan na napade od strane kvantnih računara
- Za sada postoje četiri algoritama koja se razmatraju
- Kriptografija rešetki se smatra najznačajninim kandidatom za post-kvantnu kriptografiju
- Zasnovana je na SVP i CVP problemima



Harvest Now Decrypt Later

- Vlade, hakeri, kompanije i neki drugi pojedinci i grupe prikupljaju enkriptovane podatke sa interneta
- Ne mogu da ih dekriptuju sada, ali moći će kvantnim računarima
- Računaju na to da će neki od podataka još uvek biti relevantni (npr. nepromenjene lozinke)
- Ova taktika se zove “Harvest Now Decrypt Later”

Literatura

1. Quantum Computing Progress and Prospects (2019), National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Computer Science and Telecommunications Board; Intelligence Community Studies Board; Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing; Emily Grumbling and Mark Horowitz, Editors [https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects]
2. Quantum algorithms: A survey of applications and end-to-end complexities (2023), Alexander M. Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, Chi-Fang Chen, András Gilyén, Connor T. Hann, Michael J. Kastoryano, Emil T. Khabiboulline, Aleksander Kubica, Grant Salton, Samson Wang, Fernando G. S. L. Brandão [https://arxiv.org/abs/2310.03011]
3. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (1978), R.L. Rivest, A. Shamir, L. Adleman [http://people.csail.mit.edu/rivest/Rsapaper.pdf]
4. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (1996), Peter W. Shor [https://arxiv.org/abs/quant-ph/9508027]
5. Post Quantum Cryptography and its Comparison with Classical Cryptography (2024), Tanmay Tripathi, Abhinav Awasthi, Shaurya Pratap Singh, Atul Chaturvedi [https://arxiv.org/abs/2403.19299]
6. The Mathematical Foundation of Post-Quantum Cryptography (2024), Chuanming Zong [https://arxiv.org/abs/2404.19186]

Hvala na pažnji