

Zefektivní šifrování i vývoj léků. V Ostravě spustili první tuzemský kvantový počítač



Darek Štalmach
23. září 2025 13:42

Nejsložitější matematické operace nyní v Ostravě počítá "vlk", přesněji řečeno kvantový počítač VLQ. Do provozu ho v úterý slavnostně uvedli v národním superpočítačovém centru IT4Innovations při Vysoké škole báňské – Technické univerzitě Ostrava (VŠB-TUO). Pomůže například s vývojem léků.

„Umožní řešit úlohy, které jsou pro klasické stroje prakticky neřešitelné – třeba v kryptografii, materiálovém výzkumu nebo při vývoji léčiv. Je to úplně nový způsob práce s informacemi a musíme se ho naučit využívat,“ uvedl ředitel IT4Innovations Vít Vondrák.

Zajímavá je i energetická efektivita kvantového počítače. Ten nyní stojí v bezprostředním sousedství svého předchůdce, superpočítače Karolina, který v IT4Innovations nadále funguje.

„Náš kvantový počítač má příkon asi 25 kilowattů, zatímco superpočítač Karolina potřebuje přibližně 800 kilowattů,“ porovnal obě zařízení Marek Lampart.

Nepotřebuje roky, vše spočítá za minuty. Česko má první kvantový počítač



Pavel Karban, Richard Novák

[vybrat autory ke sledování](#) ▼



[Chcete-li článek poslouchat, přihlaste se](#)

[Sdílet](#) [129](#)

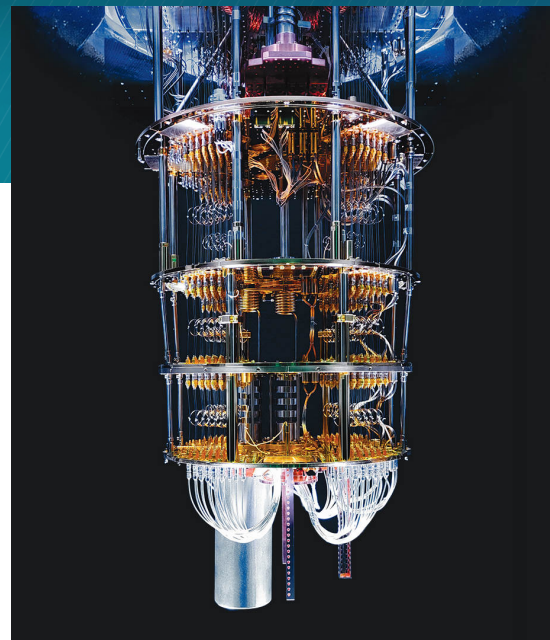
23. 9. 2025, 15:57 • Ostrava

Česko spustilo v úterý svůj první kvantový počítač, disponuje jím Národní superpočítačové centrum IT4Innovations při VŠB-Technické univerzitě Ostrava. Dle očekávání kvantové počítače zcela změní způsob, jakým řešíme extrémně složité výpočetní problémy. V porovnání s klasickými PC sestavami jsou totiž extrémně rychlé. První tuzemský kvantový počítač dostal jméno VLQ, je mimochodem i jedním z prvních v Evropě.

„Například rozklad prvočísel, což je základ kryptografie, zabere klasickým počítačům klidně i roky. Kvantové počítače se dostanou na minuty. V tom je ta obrovská změna, že dovede zrealizovat časově velmi náročné úlohy v poměrně krátkém čase,“ přiblížil běžným uživatelům schopnosti kvantového stroje Vít Vondrák, ředitel IT4Innovations.

→ INFRASTRUKTURA → VLQ KVANTOVÝ POČÍTAČ

VLQ KVANTOVÝ POČÍTAČ



ARCHITEKTURA

- 24 fyzických qubitů,
- topologie ve tvaru hvězdy,
- celkové náklady na systém činí 5 milionů EUR,
- integrován do superpočítače EuroHPC KAROLINA,
- IQM Quantum Computers dodavatelem systému,
- instalace a zprovoznění v roce 2025.

Qubit

- **qubit** = kvantový objekt s dvoudimenzionálním stavovým prostorem (nejmenší netriviální stavový prostor)

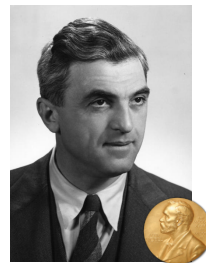
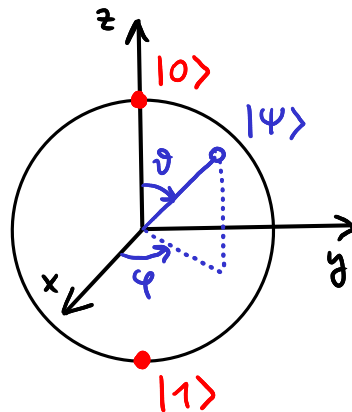
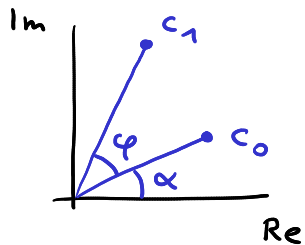
$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle \quad c_0, c_1 \in \mathbb{C} \quad |c_0|^2 + |c_1|^2 = 1$$

Pr. spin $c_0 |\uparrow\rangle + c_1 |\downarrow\rangle$

- Blochova parametrizace a Blochova sféra

$$|\psi\rangle = e^{i\alpha} \left(\cos \frac{\vartheta}{2} |0\rangle + e^{i\varphi} \sin \frac{\vartheta}{2} |1\rangle \right)$$

→ dvě reálná čísla ϑ, φ
určující poměr velikostí
a relativní fázi c_0 a c_1



Felix Bloch
(1905-1983)
NC 1952

Stavový prostor více qubitů

- obecný stav dvou qubitů

$$|\Psi\rangle = c_{00}|0\rangle \otimes |0\rangle + c_{01}|0\rangle \otimes |1\rangle + c_{10}|1\rangle \otimes |0\rangle + c_{11}|1\rangle \otimes |1\rangle$$

zkráceně: $|\Psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$
 $= c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle$ dekadicky


$$\begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

- obecný stav N qubitů

$$|\Psi\rangle = c_{000\dots 0}|000\dots 0\rangle + c_{000\dots 1}|000\dots 1\rangle + \dots = \sum_{n=0}^{2^N-1} c_n |n\rangle$$

kvantový počítač s N qubity je v superpozici 2^N konfigurací

klasicky: 8 bitů - 1B informace

64 bitů - 8B informace

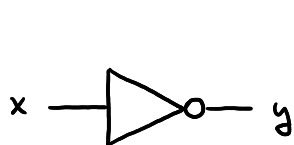
QPU: 8 qubitů $\equiv$ 510 reálných čísel

64 qubitů $\equiv$ 37 trilionů r.č.

- úhlavní nepřítel kvantového počítání - **dekoherence** (prostředí + měření)

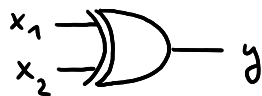
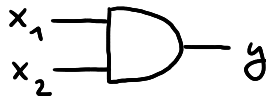
Logická hradla a logické obvody

- elementární logické operace - **hradla**



NOT

x	y
0	1
1	0



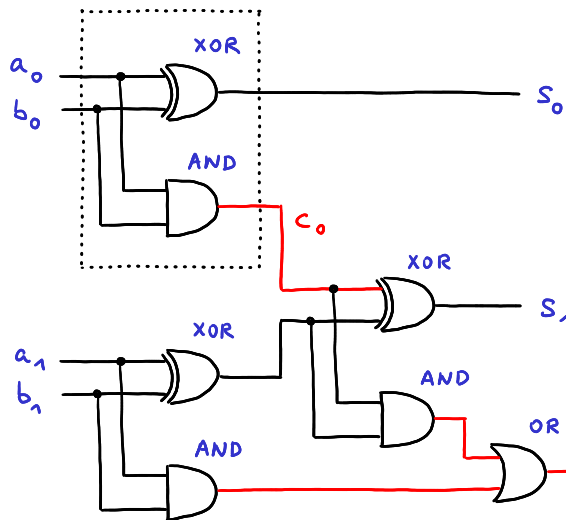
AND

x_1	x_2	y
0	0	0
0	1	0
1	0	0
1	1	1

XOR

x_1	x_2	y
0	0	0
0	1	1
1	0	1
1	1	0

- příklad logického obvodu - dvoubitová sčítacíka



vstup

$$A = a_1 \cdot 2^1 + a_0 \cdot 2^0$$

$$B = b_1 \cdot 2^1 + b_0 \cdot 2^0$$

výstup

$$S = A + B = s_1 \cdot 2^1 + s_0 \cdot 2^0$$

Carry bit (příznak přenosu)

Kvantová hradla

- **hradlo** - unitární operátor operující s qubity $\rightarrow$ unitární matice (2×2 , 4×4)
- 1-qubitové hradlo

$$|\psi\rangle \longrightarrow \boxed{\hat{U}} \longrightarrow |\psi'\rangle = \hat{U} |\psi\rangle$$

$$\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \quad \begin{pmatrix} c'_0 \\ c'_1 \end{pmatrix} = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

unitarita $\hat{U}^\dagger = \hat{U}^{-1}$

$$|c'_0|^2 + |c'_1|^2 = |c_0|^2 + |c_1|^2$$

- standardní sada 1-qubitových hradel (výběr)

$$\boxed{R_x(\theta)} \quad \hat{U} = e^{-i \frac{\theta}{2} \sigma_x}$$

$$\boxed{H} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{Hadamard}$$

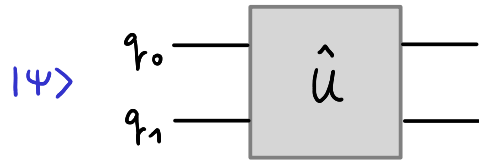
$$\boxed{X} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{bit-flip}$$

$$\boxed{S} \quad R_z\left(\frac{\pi}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$\boxed{Z} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{phase-flip}$$

$$\boxed{T} \quad R_z\left(\frac{\pi}{4}\right) = \begin{pmatrix} 1 & 0 \\ 0 & (1+i)/\sqrt{2} \end{pmatrix}$$

- 2-qubitové hradlo - operuje se stavem dvou qubitů najednou

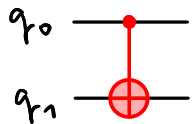


$$|\Psi'\rangle = \hat{U} |\Psi\rangle$$

$\hat{U}$ reprezentováno
unitární maticí 4×4

$$|\Psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle = c_{00}|0\rangle + c_{01}|1\rangle + c_{10}|2\rangle + c_{11}|3\rangle$$

- příklad - CNOT hradlo (controlled NOT)



$CNOT_{01}$

q_0 - kontrolní qubit

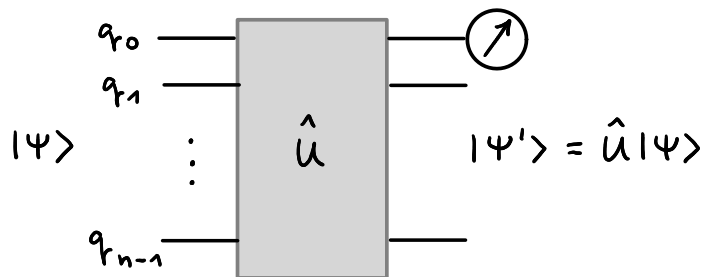
q_1 - probíhá podmíněná operace:

$$\hat{U}_1 = \hat{I} \text{ pro } q_0 = |0\rangle \text{ nebo } \hat{U}_1 = \hat{X} \text{ pro } q_0 = |1\rangle$$

$$\begin{pmatrix} c'_{00} \\ c'_{01} \\ c'_{10} \\ c'_{11} \end{pmatrix} = \begin{pmatrix} \boxed{\hat{I}} & \\ & \boxed{\hat{X}} \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

$|\Psi'\rangle \qquad \qquad \qquad \hat{U} \qquad \qquad \qquad |\Psi\rangle$

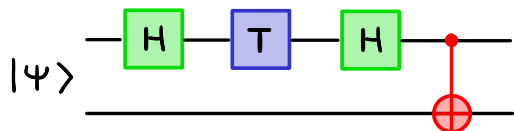
Kvantový obvod / program



- $\hat{U}$ reprezentováno maticí $2^n \times 2^n$
- libovolné $\hat{U}$ lze aproximovat sadou 1-q a 2-q hradel (H, S, T, CNOT)
- stav $|\Psi'\rangle$ nelze určit, můžeme na něm jen (destruktivně) měřit

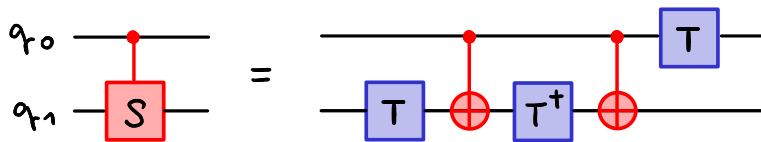
$$P(001\dots 01) = |c_{001\dots 01}|^2$$

Př. operace $|00\rangle \rightarrow \cos \frac{\pi}{8} |00\rangle - i \sin \frac{\pi}{8} |11\rangle$



$$|\Psi'\rangle = \hat{U}_{\text{CNOT}} (\hat{H} \otimes \hat{I}) (\hat{T} \otimes \hat{I}) (\hat{H} \otimes \hat{I}) |\Psi\rangle$$

- opera'torové identity



$$CS = T_0 \text{CNOT}_{01} T_1^\dagger \text{CNOT}_{01} T_1$$

Generátor koček

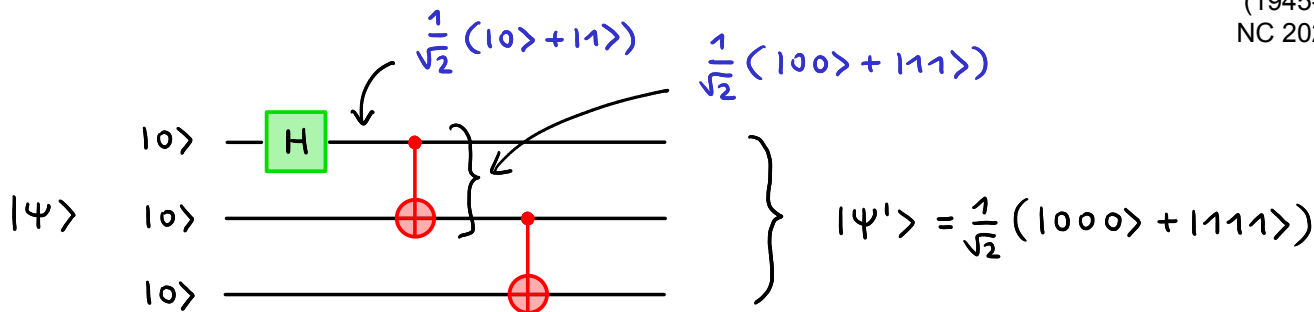
- Greenberger - Horne - Zeilinger / cat state
= superpozice těch nejvzdálenějších stavů:

$$|GHZ\rangle = \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle)$$

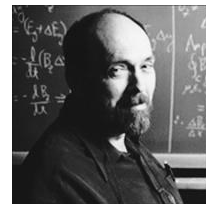
inspirace: Schrödingerova kočka

$$\frac{1}{\sqrt{2}} |\text{cat}\rangle + \frac{1}{\sqrt{2}} |\text{dead}\rangle$$

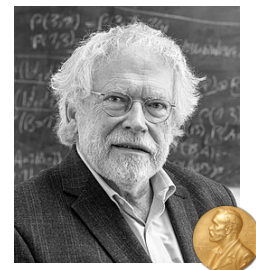
- realizace pomocí kvantových hradel



Daniel Greenberger
(1933-)

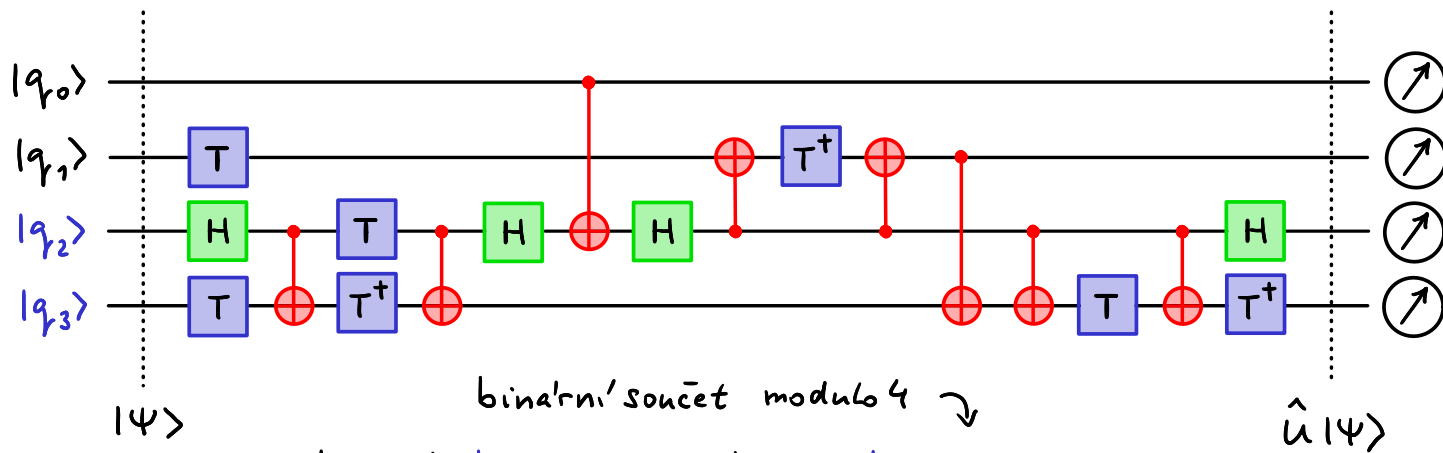


Michael Horne
(1943-2019)



Anton Zeilinger
(1945-)
NC 2022

Kvantová sčítacia



binárny súčet modulo 4

$$\underbrace{|q_0 q_1\rangle}_m \underbrace{|q_2 q_3\rangle}_n \rightarrow |q_0 q_1\rangle \underbrace{|q_0 q_1 + q_2 q_3\rangle}_{m+n}$$

příklady:

$$\underbrace{|2\rangle}_m \underbrace{|1\rangle}_n = \underbrace{|10\rangle}_{q_0 q_1} \underbrace{|01\rangle}_{q_2 q_3}$$

$$\xrightarrow{\hat{U}} |10\rangle |11\rangle = |2\rangle |3\rangle$$

$$|2\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |10\rangle \frac{|00\rangle + |01\rangle}{\sqrt{2}}$$

$$\xrightarrow{\hat{U}} |10\rangle \frac{|10\rangle + |11\rangle}{\sqrt{2}} = |2\rangle \frac{|2\rangle + |3\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + |13\rangle}{\sqrt{2}} \frac{|1\rangle + |2\rangle + |3\rangle}{\sqrt{3}}$$

$$\xrightarrow{\hat{U}} ?$$

Article

Quantum supremacy using a programmable superconducting processor

<https://doi.org/10.1038/s41586-019-1666-5>

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute¹, Kunal Arya¹, Ryan Babbush¹, Dave Bacon¹, Joseph C. Bardin^{1,2}, Rami Barends¹, Rupak Biswas³, Sergio Boixo¹, Fernando G. S. L. Brandao^{1,4}, David A. Buell¹, Brian Burkett¹, Yu Chen¹, Zijun Chen¹, Ben Chiaro⁵, Roberto Collins¹, William Courtney¹, Andrew Dunsworth¹, Edward Farhi¹, Brooks Foxen^{1,5}, Austin Fowler¹, Craig Gidney¹, Marissa Giustina¹, Rob Graff¹, Keith Guerin¹, Steve Habegger¹, Matthew P. Harrigan¹, Michael J. Hartmann^{1,6}, Alan Ho¹, Markus Hoffmann¹, Trent Huang¹, Travis S. Humble⁷, Sergei V. Isakov¹, Evan Jeffrey¹, Zhang Jiang¹, Dvir Kafri¹, Kostyantyn Kechedzhii¹, Julian Kelly¹, Paul V. Klimov¹, Sergey Knysch¹, Alexander Korotkov^{1,8}, Fedor Kostritsa¹, David Landhuis¹, Mike Lindmark¹, Erik Lucero¹, Dmitry Lyakh⁹, Salvatore Mandrà^{3,10}, Jarrod R. McClean¹, Matthew McEwen⁵, Anthony Megrant¹, Xiao Mi¹, Kristel Michielsen^{11,12}, Masoud Mohseni¹, Josh Mutus¹, Ofer Naaman¹, Matthew Neeley¹, Charles Neill¹, Murphy Yuezhen Niu¹, Eric Ostby¹, Andre Petukhov¹, John C. Platt¹, Chris Quintana¹, Eleanor G. Rieffel³, Pedram Roushan¹, Nicholas C. Rubin¹, Daniel Sank¹, Kevin J. Satzinger¹, Vadim Smelyanskiy¹, Kevin J. Sung^{1,13}, Matthew D. Trevithick¹, Amit Vainsencher¹, Benjamin Villalonga^{1,14}, Theodore White¹, Z. Jamie Yao¹, Ping Yeh¹, Adam Zalcman¹, Hartmut Neven¹ & John M. Martinis^{1,5*}

¹Google AI Quantum, Mountain View, CA, USA. ²Department of Electrical and Computer Engineering, University of Massachusetts Amherst, Amherst, MA, USA. ³Quantum Artificial Intelligence Laboratory (QuAIL), NASA Ames Research Center, Moffett Field, CA, USA. ⁴Institute for Quantum Information and Matter, Caltech, Pasadena, CA, USA. ⁵Department of Physics, University of California, Santa Barbara, CA, USA. ⁶Friedrich-Alexander University Erlangen-Nürnberg (FAU), Department of Physics, Erlangen, Germany. ⁷Quantum Computing Institute, Oak Ridge National Laboratory, Oak Ridge, TN, USA. ⁸Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA. ⁹Scientific Computing, Oak Ridge Leadership Computing, Oak Ridge National Laboratory, Oak Ridge, TN, USA. ¹⁰Stinger Ghaffarian Technologies Inc., Greenbelt, MD, USA. ¹¹Institute for Advanced Simulation, Jülich Supercomputing Centre, Forschungszentrum Jülich, Jülich, Germany. ¹²RWTH Aachen University, Aachen, Germany. ¹³Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA. ¹⁴Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL, USA. *e-mail: jmartinis@google.com

Realizace kvantových počítačů

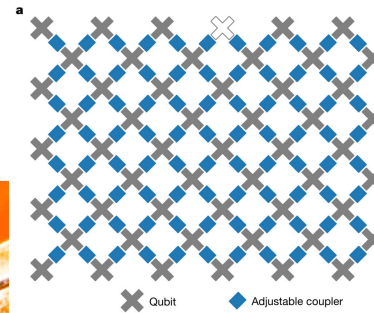
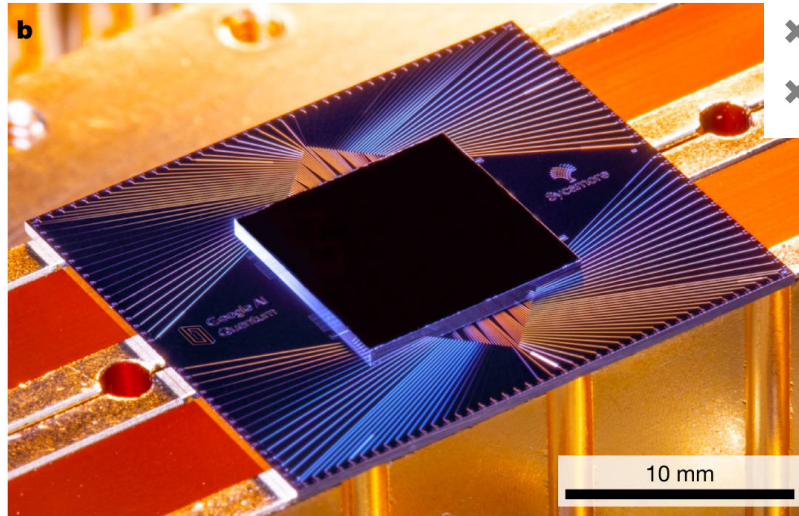
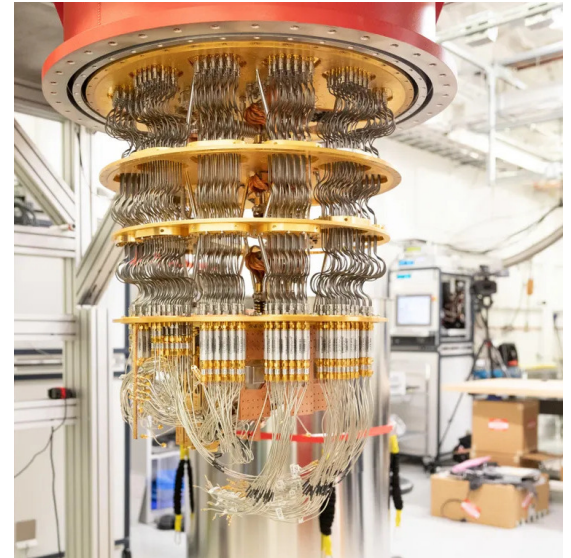


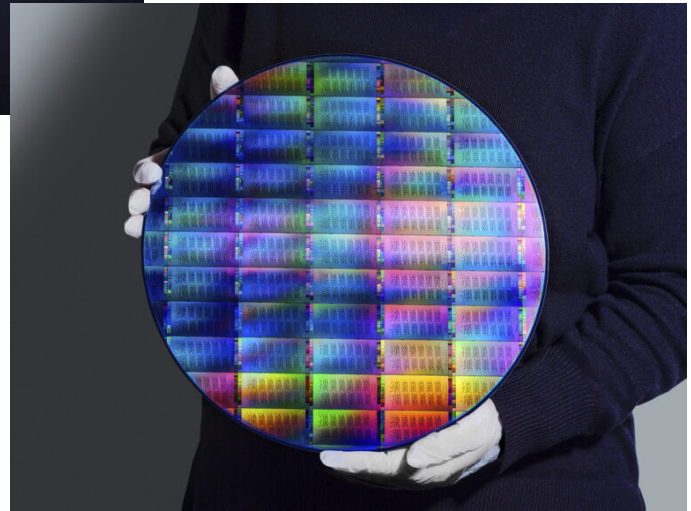
Fig. 1 | The Sycamore processor. **a**, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.



IBM



IBM Quantum System Two

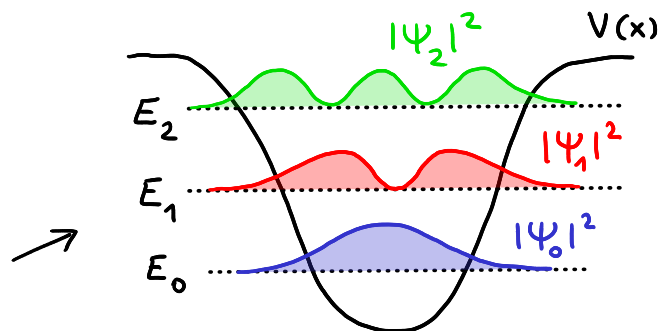


Statistická fyzika nerozlišitelných (a nezávislých) kvantových částic

- jednočásticové energetické hladiny

$$\hat{H} = \sum_{\text{částice}} \hat{H}_{\text{jednočásticový}}$$

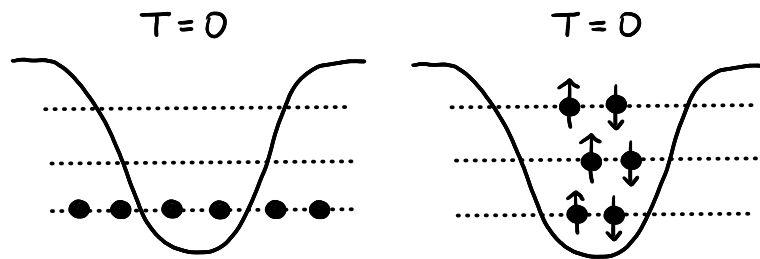
řešením Sch.r.: $\hat{H}_{\text{jednočásticový}} \Psi = E \Psi$



- nerozlišitelné (identické) částice

bosony - celočíselný spin

fermiony - poločíselný spin

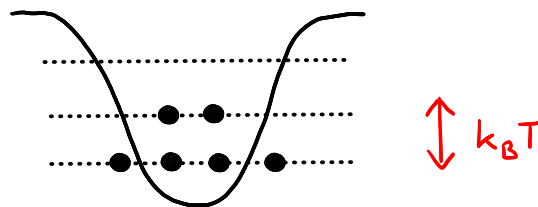


- Boltzmannova exponenciála

$$P(\text{stav s energií } E) \sim e^{-\frac{E}{k_B T}}$$

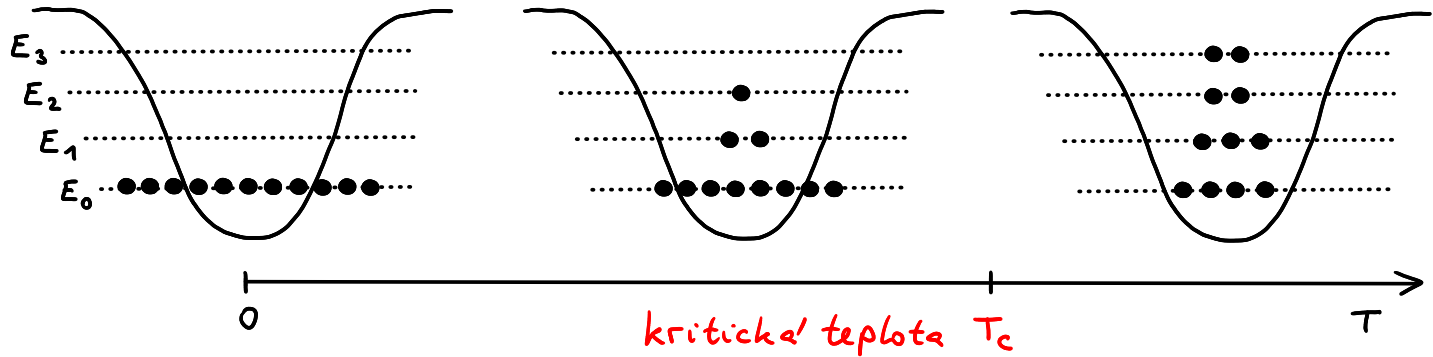
→ změny populace pro $T > 0$

↓ zahrát' na $T > 0$



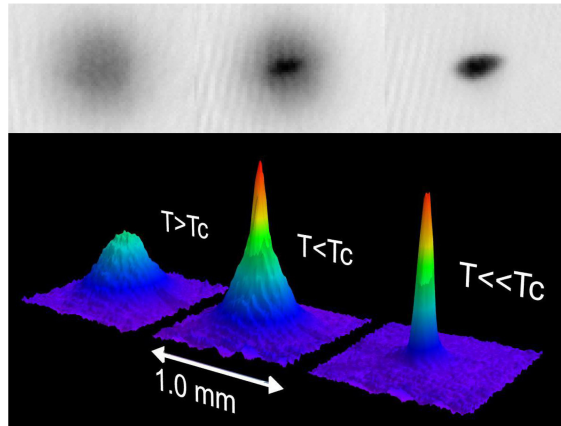
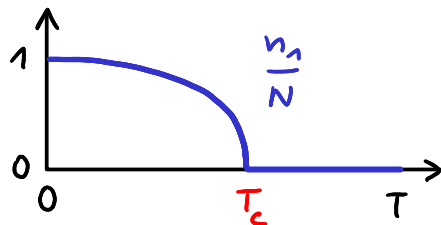
Bose-Einsteinova kondenzace

- při snižování teploty mohou bosony makroskopicky obsadit nejnižší stav



$$\Psi_0(\vec{r}_1) \Psi_0(\vec{r}_2) \dots \Psi_0(\vec{r}_N)$$

díl bosonů na
nejnižší hladině



obláčky par alkal. kovů

^{87}Rb , ^{23}Na , ^7Li

rozměry $\sim$ stovky μm

řádově $10^5 - 10^7$ atomů

$T_c \sim 10\text{ nK} - 1\text{ }\mu\text{K}$

Makroskopická vlnová funkce

- všechny bosony ve stejném stavu ($T = 0$)

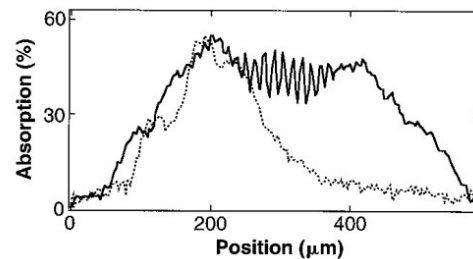
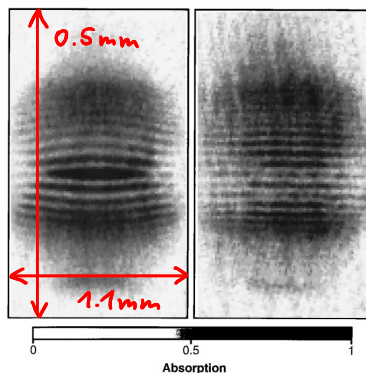
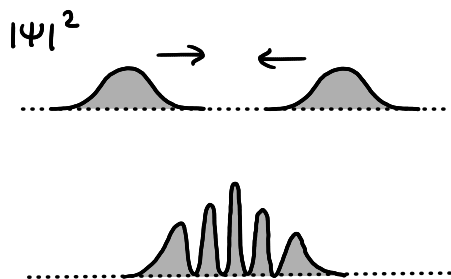
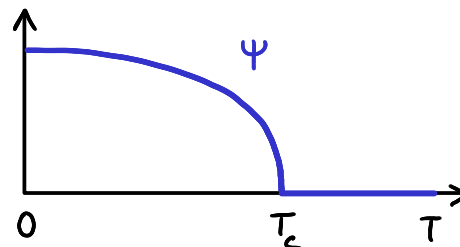
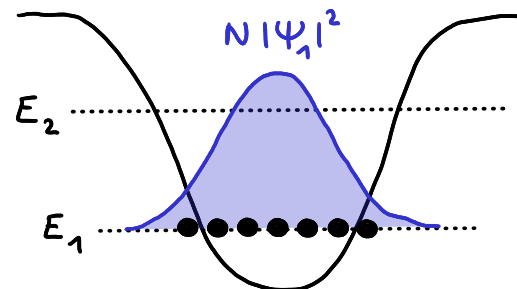
- řídí se stejnou vlnovou funkcí Ψ_0

$$\Psi_0(x, y, z, t) \rightarrow \sqrt{N} \Psi_0(x, y, z, t)$$

- možnost makroskopického pozorování kvantových jevů

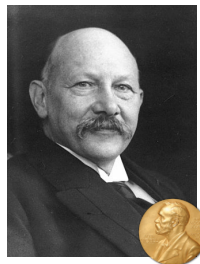
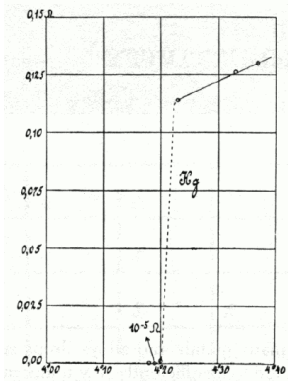
- mocnost Ψ závisí na teplotě

- interference dvou kondenzátů



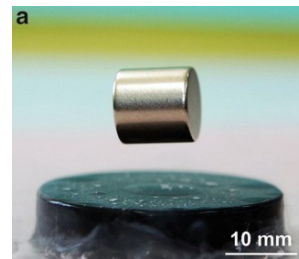
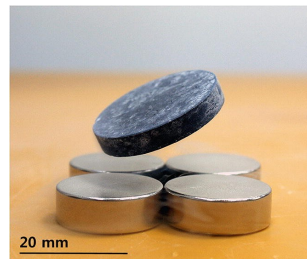
Supravodivost

- vymizení elektrického odporu pod T_c



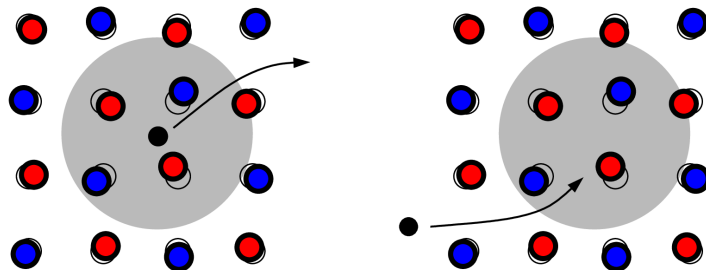
Heike Kamerlingh Onnes
(1853-1926)
NC 1913

- vypuzování magnetického pole (Meissnerův - Ochsenfeldův jev)

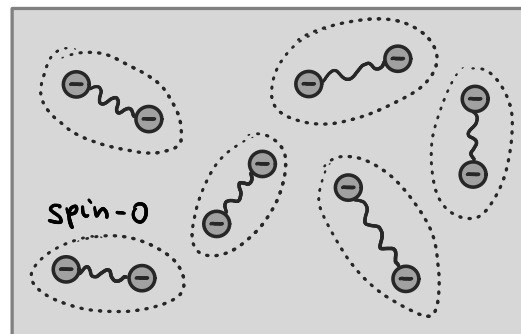


Kim, C.J. (2019). Levitation Experiments Using the Meissner Effect.
In: Superconductor Levitation. Springer, Singapore

- přitažlivá interakce mezi elektrony

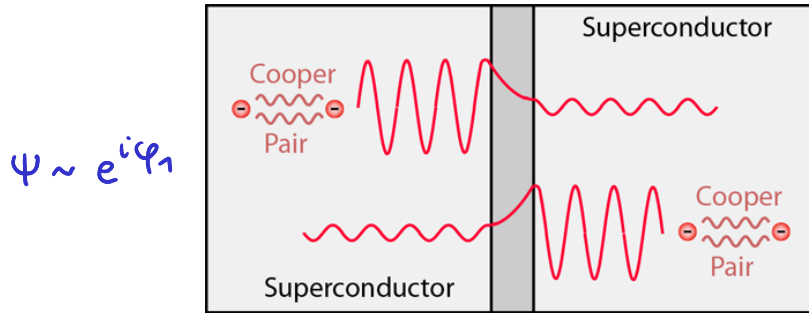


- kondenzace Cooperových párů



Tunelování párů a Josephsonovy jevy

- tunelování Cooperových párů díky „průsaku“ Ψ



Brian D. Josephson
(1940-)
NC 1973

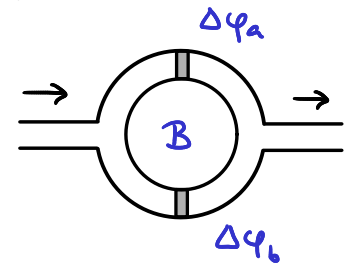
- DC Josephsonův jev: přechod bez $U \rightarrow$ proud

$$I_J = I_0 \sin \Delta\varphi \quad \Delta\varphi = \varphi_2 - \varphi_1$$

- AC Josephsonův jev: přiložene' $U \rightarrow$ oscilace

$$\omega = \frac{d\Delta\varphi}{dt} = \frac{2e}{\hbar} U$$

SQUID



magnetické pole $\rightarrow$ fáze

$$\Delta\varphi_b = \Delta\varphi_a + \frac{2e}{\hbar} BS$$

7 October 2025

The Nobel Prize in Physics 2025

The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Physics 2025 to

John Clarke

University of California, Berkeley, USA

Michel H. Devoret

Yale University, New Haven, CT,
University of California, Santa Barbara and
Google Quantum AI, Santa Barbara, CA, USA

John M. Martinis

University of California, Santa Barbara
and Qolab, Los Angeles, CA, USA



“for the discovery of macroscopic quantum mechanical tunnelling and energy quantisation in an electric circuit”

John Clarke, born 1942 in Cambridge, UK. PhD 1968 from University of Cambridge, UK. Professor at University of California, Berkeley, USA.

Michel H. Devoret, born 1953 in Paris, France. PhD 1982 from Université Paris-Saclay, France. Professor at Yale University, New Haven, CT, and University of California, Santa Barbara, and Chief Scientist for Quantum Hardware at Google Quantum AI, Santa Barbara, CA, USA.

John M. Martinis, born 1958 in Los Angeles, CA, USA. PhD 1987 from University of California, Berkeley, USA. Professor at University of California, Santa Barbara and Chief Technology Officer at Qolab, Los Angeles, CA, USA.



Fáze je kvantová veličina

- operátory fáze a počtu Cooperových párů

rozdíl fází $\Delta\varphi = \varphi_2 - \varphi_1 \rightarrow$ proud

rozdíl počtu Cooperových párů $\Delta n = n_2 - n_1 \rightarrow$ náboj

komutátor $[\Delta\hat{\varphi}, \Delta\hat{n}] = i$ (analogie $[\hat{x}, \hat{p}] = i\hbar$)

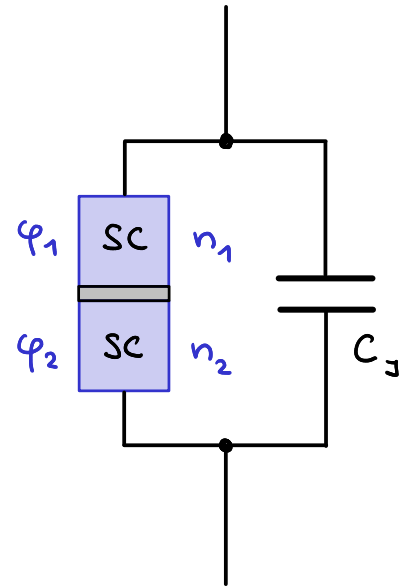
- energetická rovnice $\rightarrow$ Hamiltonián

energie kondenzátoru

$$\int U \cdot I \, dt = \int U \cdot C_J \frac{dU}{dt} \, dt = C_J \int U \, dU = \frac{1}{2} C_J U^2 = \frac{1}{2} \frac{Q^2}{C_J} = \frac{1}{2} \frac{(2e)^2}{C_J} (\Delta\hat{n})^2$$

energie Josephsonova přechodu ("cívký")

$$\int U \cdot I \, dt = \int \frac{\hbar}{2e} \frac{d\Delta\varphi}{dt} \cdot (I_0 \sin \Delta\varphi - I_{\text{bias}}) \, dt = \frac{\hbar}{2e} (-I_0 \cos \Delta\varphi - I_{\text{bias}} \Delta\varphi)$$

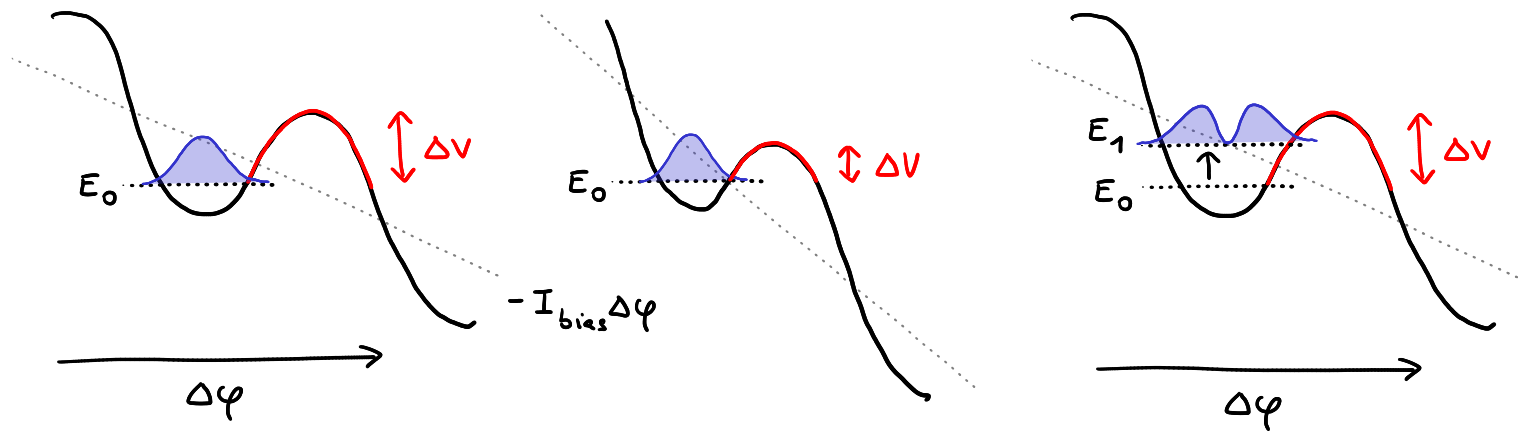


Makroskopické tunelování

- výsledný Hamiltonián

$$\hat{H} = E_c (\Delta \hat{n})^2 - E_J (\cos \Delta \hat{\varphi} + \frac{I_{\text{bias}}}{I_0} \Delta \hat{\varphi}) \quad E_c = \frac{(2e)^2}{C_J} \quad E_J = I_0 \frac{\hbar}{2e}$$

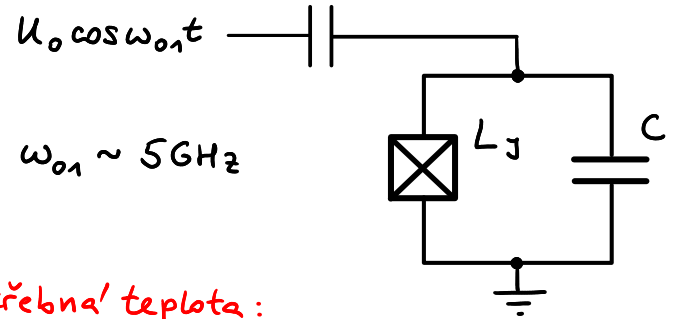
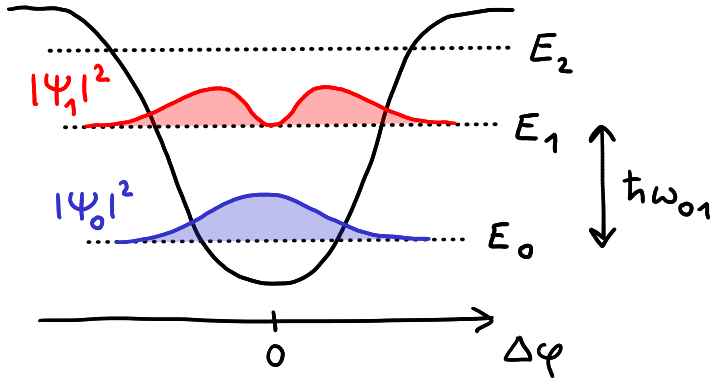
→ pohyb fiktivní částice v potenciálu $V(\Delta\varphi) \sim -\cos\Delta\varphi - \frac{I_{\text{bias}}}{I_0} \Delta\varphi$



- tunelování $\sim e^{-\kappa a}$ reaguje na I_{bias}
- přechod na E_1 pomocí MW pulzu s $\hbar\Omega = E_1 - E_0$ usnadní tunelování

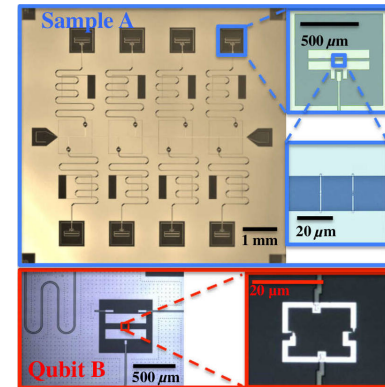
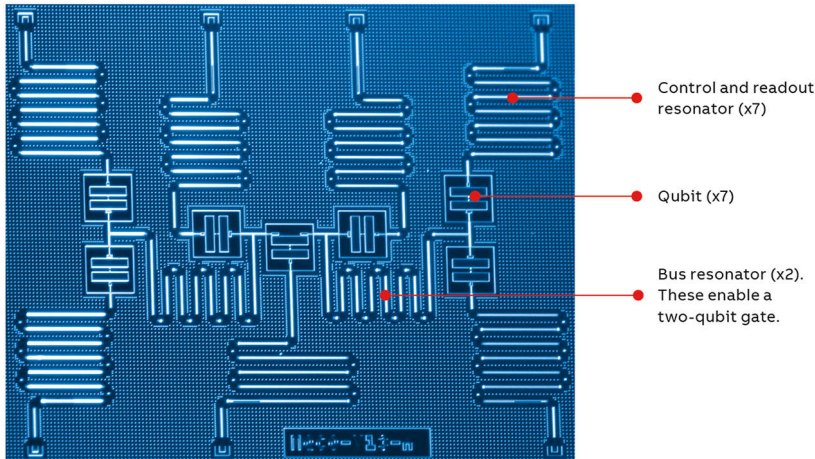
Supravodivé qubity

- anharmonický kvantový oscilátor s Josephsonovým přechodem



potřebná teplota:

$$\hbar\omega_{01} \gg k_B T \rightarrow T \ll 240 \text{ mK}$$



Prvočíselný rozklad

- RSA kryptosystém (1977 Ron Rivest, Adi Shamir, Leonard Adleman)

$$n = p \cdot q$$

n veřejné - slouží k zakódování

p, q tajné - potřebné k dekodování

- RSA Factoring challenge (1991 - 2007)

```
RSA-2048 = 2519590847565789349402718324004839857142928212620403202777713783604366202070
7595556264018525880784406918290641249515082189298559149176184502808489120072
8449926873928072877767359714183472702618963750149718246911650776133798590957
0009733045974880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739934236584823
8242811981638150106748104516603773060562016196762561338441436038339044149526
3443219011465754445417842402092461651572335077870774981712577246796292638635
6373289912154831438167899885040445364023527381951378636564391212010397122822
120720357
```

\$ 200 000

- kvantové úspěchy
- | | | |
|-------|---------------------------|---------------------------------|
| 2001: | $15 = 3 \cdot 5$ | (Shorův algoritmus z roku 1994) |
| 2012: | $21 = 3 \cdot 7$ | (2021 opraven) |
| 2019: | 35 se nezdařilo | |
| 2018: | 249919 (18 bitů) | |
| 2022: | 261980999226229 (48-bitů) | } kvantová optimalizace |
| 2024: | 8219999 (23 bitů) | |
| 2025: | 2048 bitů | |



ARTICLE OPEN



Analyzing the performance of variational quantum factoring on a superconducting quantum processor

Amir H. Karamlou ^{1,2,4}✉, William A. Simon ^{1,4}, Amara Katarawa¹, Travis L. Scholten³, Borja Peropadre¹ and Yudong Cao¹✉

In the near-term, hybrid quantum-classical algorithms hold great potential for outperforming classical approaches. Understanding how these two computing paradigms work in tandem is critical for identifying areas where such hybrid algorithms could provide a quantum advantage. In this work, we study a QAOA-based quantum optimization approach by implementing the Variational Quantum Factoring (VQF) algorithm. We execute experimental demonstrations using a superconducting quantum processor, and investigate the trade off between quantum resources (number of qubits and circuit depth) and the probability that a given biprime is successfully factored. In our experiments, the integers 1099551473989, 3127, and 6557 are factored with 3, 4, and 5 qubits, respectively, using a QAOA ansatz with up to 8 layers and we are able to identify the optimal number of circuit layers for a given instance to maximize success probability. Furthermore, we demonstrate the impact of different noise sources on the performance of QAOA, and reveal the coherent error caused by the residual ZZ-coupling between qubits as a dominant source of error in a near-term superconducting quantum processor.

npj Quantum Information (2021)7:156; <https://doi.org/10.1038/s41534-021-00478-z>



$$1099551473989 = 1048589 * 1048601$$

$$100000000000000000010011000000000000101000101 = 10000000000000000001101 * 100000000000000000011001$$

```

1 import numpy as np
2
3 n = 8219999          # Ding et al. 2024      - D-Wave pure QPU annealing
4 n = 549755813701    # Willsch et al. 2023    - GPU simulation of 40 qubit QPU
5 n = 1099551473989   # Karamlou et al. 2021 - 3 qubits of IBMQ Boeblingen
6 n = 261980999226229 # Yan et al. 2022      - 10 qubit QPU
7
8 for p in range(2,int(np.sqrt(n))):
9     if n%p==0: print(p,n//p)
10

```


A First Successful Factorization of RSA-2048 Integer by D-Wave Quantum Computer

Chao Wang, Jingjing Yu, Zhi Pei (✉), Qidi Wang, Chunlei Hong

Show Author Information ▼

Abstract

Integer factorization, the core of the Rivest–Shamir–Adleman (RSA) attack, is an exponential challenge. As of this year, a group of researchers' latest quantum supremacy chip released for cryptanalysis. Quantum annealing (QA) has a unique quantum tunneling advantage to escape local extremum in the exponential solution space, finding the global optimal solution with higher probability. Consequently, we consider it an effective method for attacking cryptosystems. According to Origin Quantum Computing, QA computers are able to factor numbers of magnitude larger than universal quantum computers. We try to transform the integer factorization problem in RSA attacks into a combinatorial optimization problem by using the QA algorithm on a quantum computer, and attack RSA-2048 which is composed of a class of special integers. This experiment factored this class of integers of size 2^{2048} , $N=p \times q$. As an example, the results of 10 RSA-2048 attacks in the appendix. This marks the first successful factorization of RSA-2048 by D-Wave quantum computer, regardless of employing mathematical or quantum techniques, despite dealing with special integers, exceeding $2^{1061}-1$ of California State University. This experiment verifies that the QA algorithm based on D-Wave is an effective method to attack RSA.

Keywords

quantum annealing

D-Wave

Rivest Shamir Adleman (RSA)

integer factorization

a constant-level solution space search problem, which greatly saves computational resources. The special integers discussed in this article is the product of two prime numbers differing at only 2 bits, it is worth mentioning that the special integers considered in this paper are all semi-prime numbers, that is, the decomposed factors are all prime numbers

$N=2344221089529646655151068154361983197810258179973661124697652159019189322413578902$
 $5070678051976867349306593323317287750867313641112828898759744515604087401460159349$
 $86990476214270640086817425581538170373870259313066583768903697048280641467367411589$
 $93910041461135601151339797803821866970974724786872772467600158490577052523497666938$
 $2895464232871732123454572174833964467804115311936850586791492844973560905229429892$
 $43892620418817449054375508097262165283165093027743111302874592959317102563951824995$
 $59212557763930782475197346665090557761529485013603452022242755996443865335294973$
 $2541506721438058592990053089448078211591$, and the obtained factors are as follows:

$p=153108493870511529343183982694581037554816693901893186090279800600449285091109272$
 $5780710664273360703216936015622744330985806196000996639054102790231481525239396500$
 $7161559607741351646932146648645492140456834249721659196143935406484425820073873243$
 $4241527208989488198329400820115825335921585482389611993667849543$,
 $q=153108493870511529343183982694581037554816693901893186090279800600449285091109272$
 $5780710664273360703216936015622744330985806196000996639054102790231481525239396500$
 $7161559607741351646932146648645492140456834249721659196143935406484425820073873243$
 $4241527208989488198329400820115825335921585482389611993667849537$.

