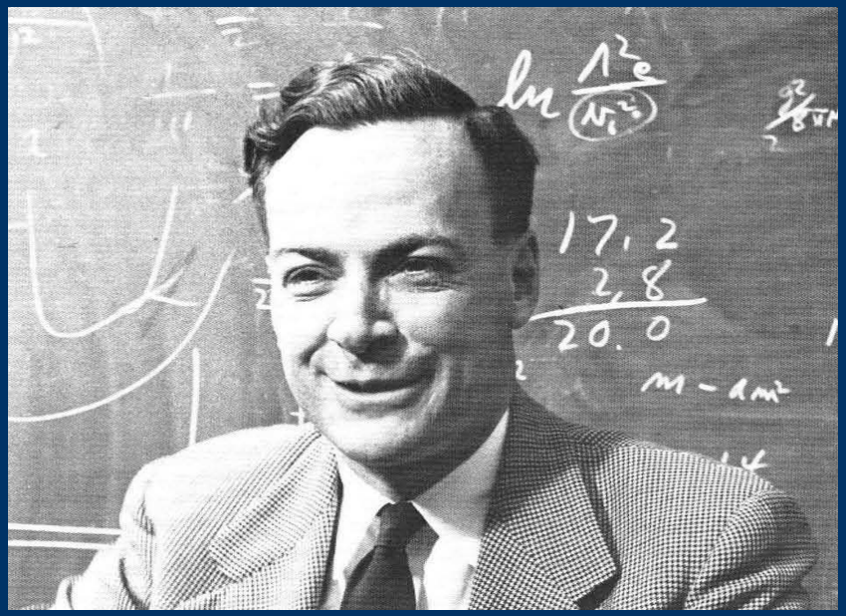
Wie funktioniert ein Quantencomputer ?

Oliver Vornberger
Institut für Informatik
Universität Osnabrück



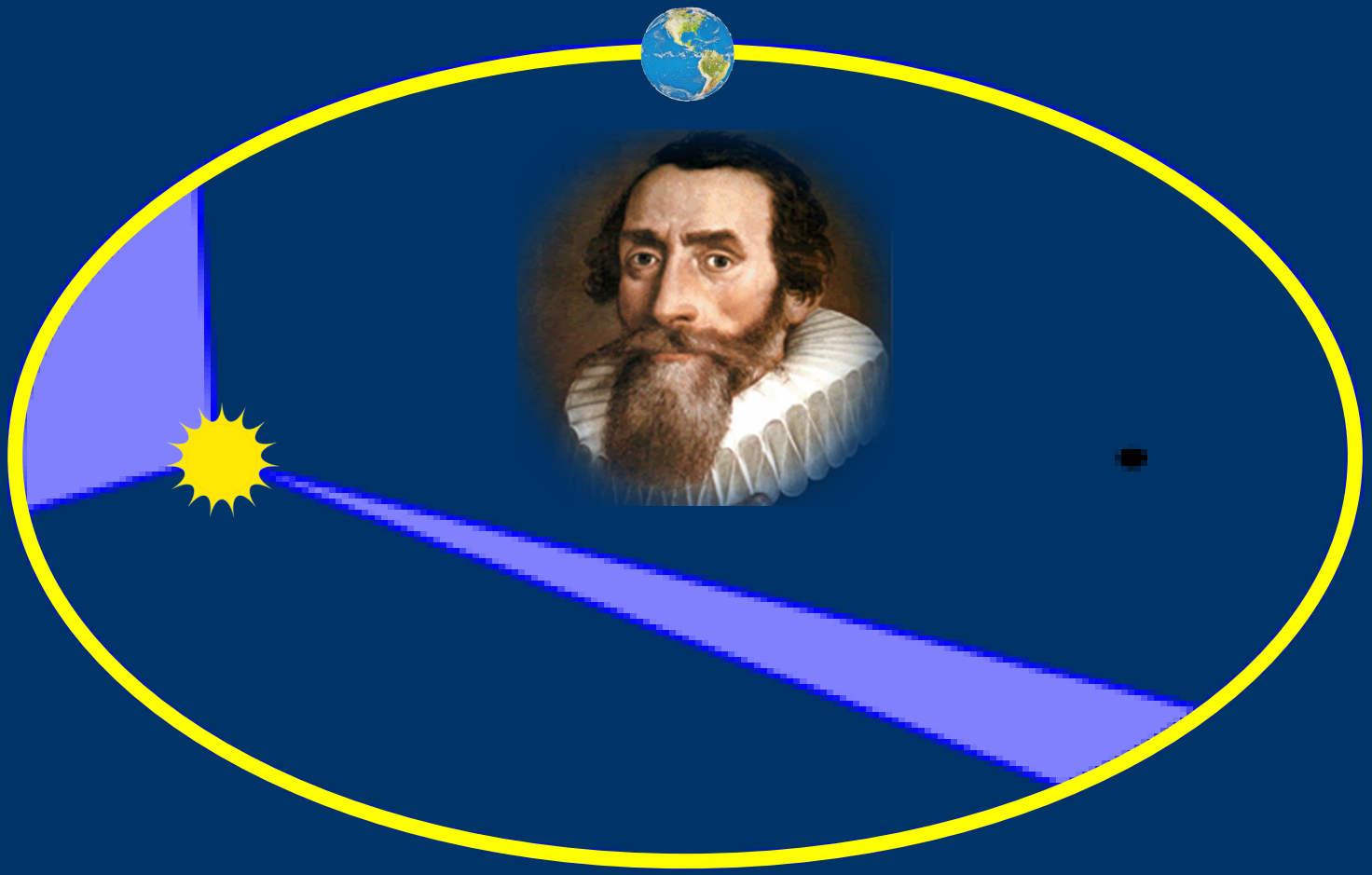
Richard Feynman

Nobelpreis für Physik in 1965:

If you think you understand quantum mechanics,
you don't understand quantum mechanics.

* 1571 Johannes Kepler

Ellipse



In gleichen Zeiten gleiche Flächen

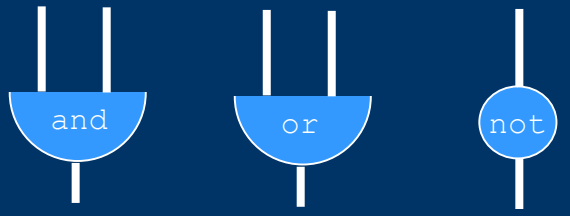
$$f : \mathbb{R} \to \mathbb{R}^3$$

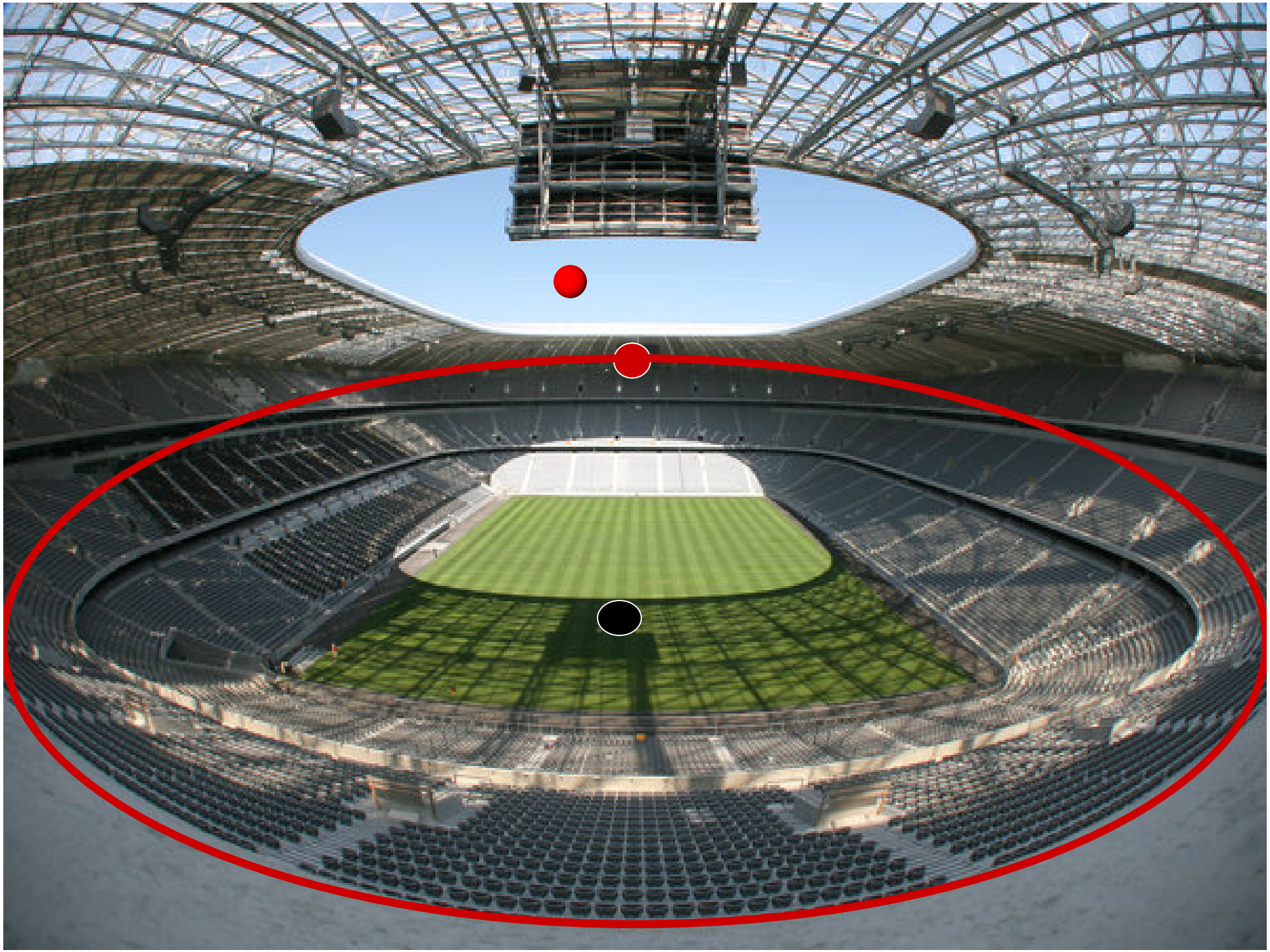
$$\frac{T_1^2}{T_2^2} = \frac{a_1^3}{a_2^3}$$

Digitalrechner

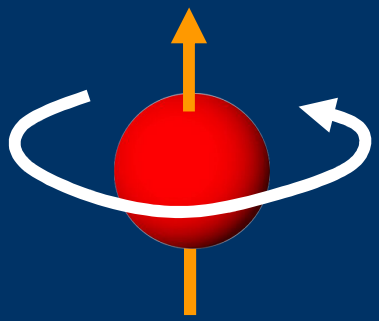
A = B + C

14						
27	1	1	1	1		
41	**1**	**0**	**1**	**0**	**0**	**1**

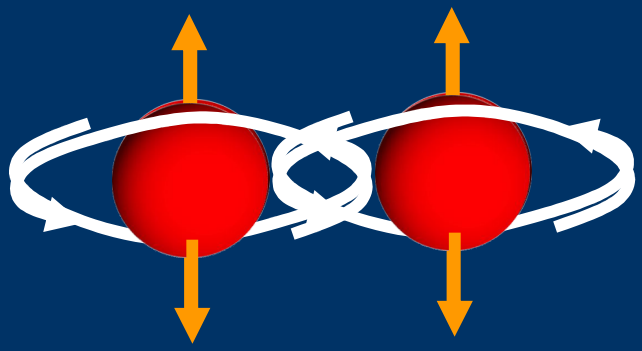


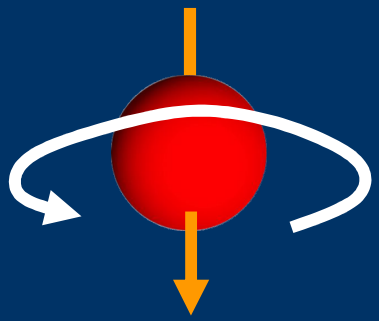


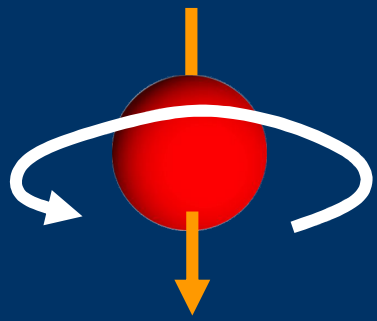
Überlagerung / Superposition



Verschränkung







Qubit

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

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

$$\begin{pmatrix} a \cdot \alpha + b \cdot \beta \\ c \cdot \alpha + d \cdot \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Hadamard

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Register mit 2 Qubits

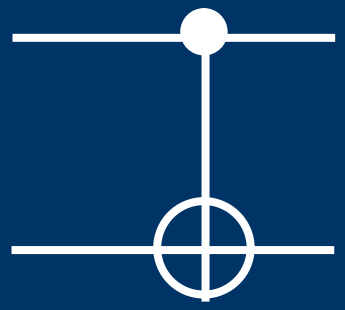
$$\alpha|0\rangle + \beta|1\rangle \qquad\qquad \gamma|0\rangle + \delta|1\rangle$$

$$\alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle$$

00
01
10
11

CNOT

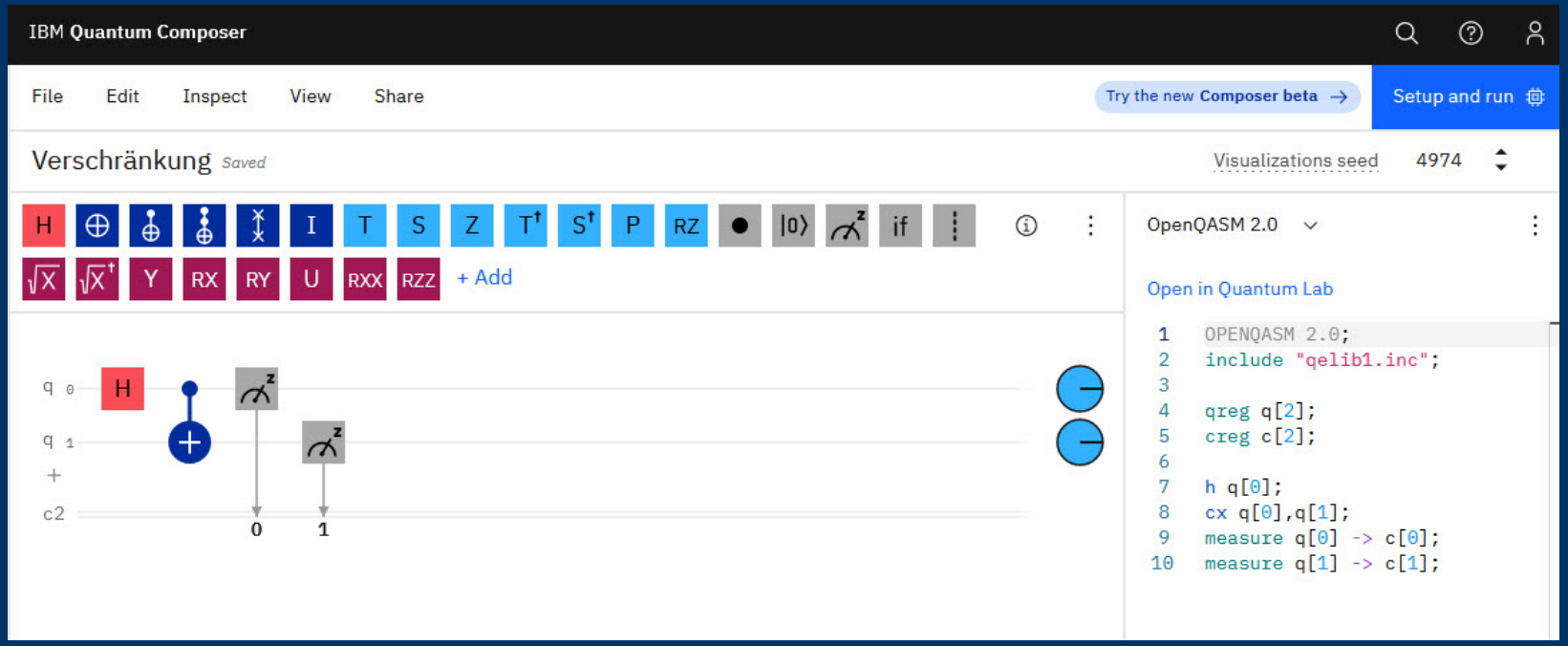
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Verschränkung

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

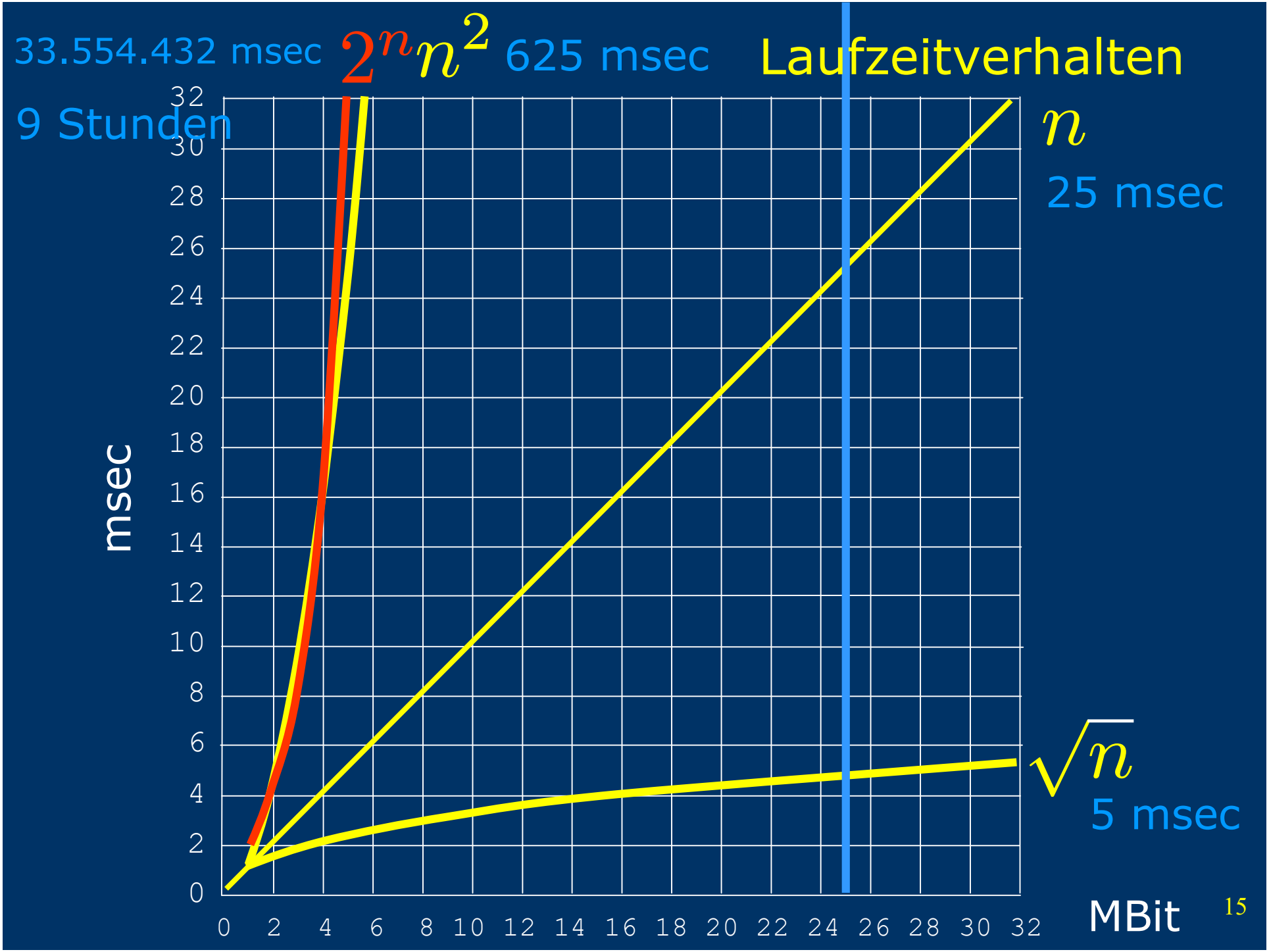
https://quantum-computing.ibm.com

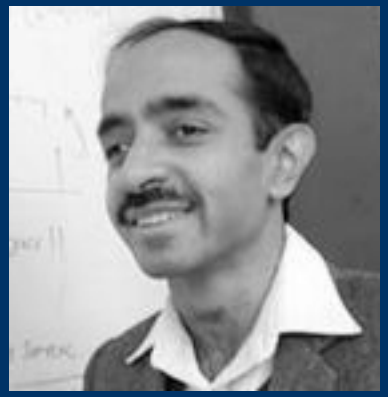


Lottozahlen

09.10.1955	3	12	13	16	23	41
16.10.1955	3	12	18	30	32	49
23.10.1955	12	14	23	24	34	36
30.10.1955	4	13	23	30	36	44
06.11.1955	5	6	31	39	44	49
13.11.1955	6	18	22	29	37	44
20.11.1955	4	8	12	16	27	44
27.11.1955	9	24	26	37	44	46
04.12.1955	5	20	21	26	31	47
11.12.1955	8	10	22	26	31	37
18.12.1955	8	14	26	36	39	42
25.12.1955	5	9	34	38	39	42
01.01.1956	4	22	27	36	38	46
08.01.1956	6	21	22	37	41	42
15.01.1956	1	9	16	19	29	49
22.01.1956	12	17	23	27	35	40
29.01.1956	5	6	18	22	38	43
05.02.1956	12	26	35	36	42	43
12.02.1956	1	14	23	27	30	33
19.02.1956	8	20	26	35	38	42
26.02.1956	1	30	32	42	45	48
04.03.1956	4	6	17	19	41	47
11.03.1956	6	9	20	22	26	28
18.03.1956	3	10	24	26	38	49
25.03.1956	3	16	18	19	37	42
02.04.1956	7	10	22	25	32	43
08.04.1956	2	19	25	30	32	39

09.02.2022	16	25	26	32	33	45
12.02.2022	2	13	17	31	39	48
16.02.2022	7	16	29	30	33	43
19.02.2022	2	3	10	24	27	45
23.02.2022	5	7	11	15	24	47
26.02.2022	6	16	33	43	45	49
02.03.2022	3	5	15	39	44	49
05.03.2022	10	22	25	26	28	41
09.03.2022	8	18	19	28	36	38
12.03.2022	1	9	20	32	35	36
16.03.2022	1	6	8	16	19	40
19.03.2022	1	5	17	26	28	41
23.03.2022	3	12	15	30	39	43
26.03.2022	14	16	19	45	46	48
30.03.2022	6	12	13	27	34	41
02.04.2022	14	37	38	40	46	49
06.04.2022	2	19	22	24	29	31
09.04.2022	5	17	27	33	43	45
13.04.2022	2	7	22	29	42	46
16.04.2022	7	8	14	19	24	44
20.04.2022	10	16	19	20	35	44
23.04.2022	13	29	32	34	38	47
27.04.2022	3	17	19	25	40	46
30.04.2022	2	14	20	25	44	48
04.05.2022	3	4	11	31	41	49
07.05.2022	5	14	26	34	35	43
11.05.2022	2	24	25	27	28	45
14.05.2022	25	30	34	37	39	49


33.554.432 msec
$2^n n^2$
625 msec
Laufzeitverhalten
9 Stunden
n
25 msec
msec
$\sqrt{n}$
5 msec
MBit
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32



Lov Grover *1960

Nadel im Heuhaufen

87 45 62 31 98 42 13 54

$|s\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle$

$0,972$

$0,883$

$0,353$

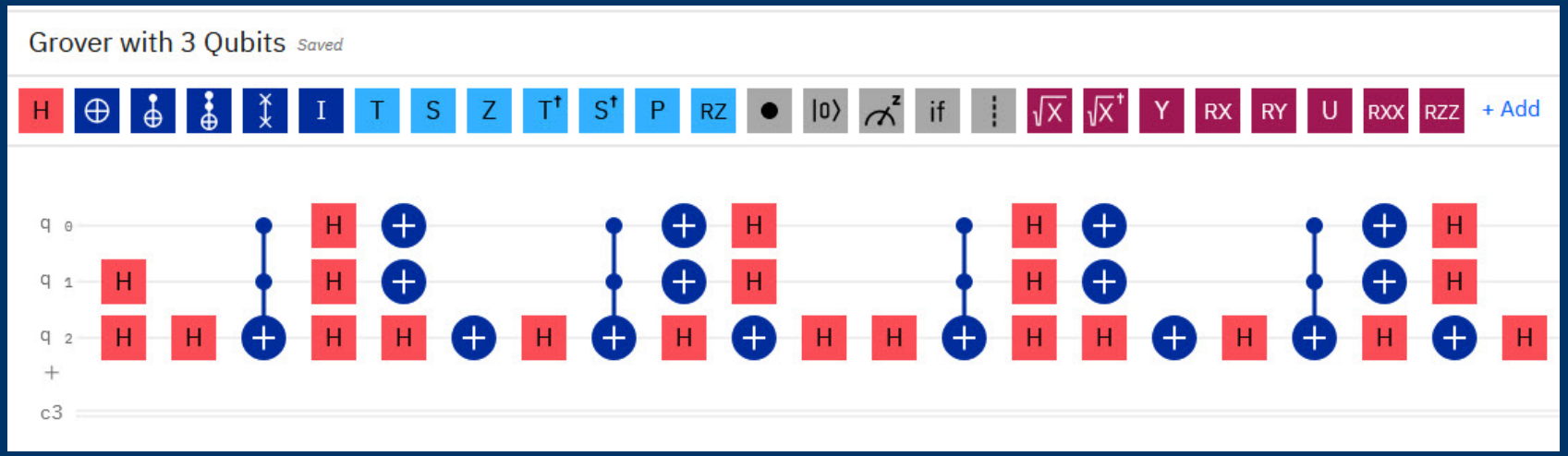
$m = \frac{1}{8}(\frac{7}{\sqrt{8}} - \frac{1}{\sqrt{8}}) = 0,265$

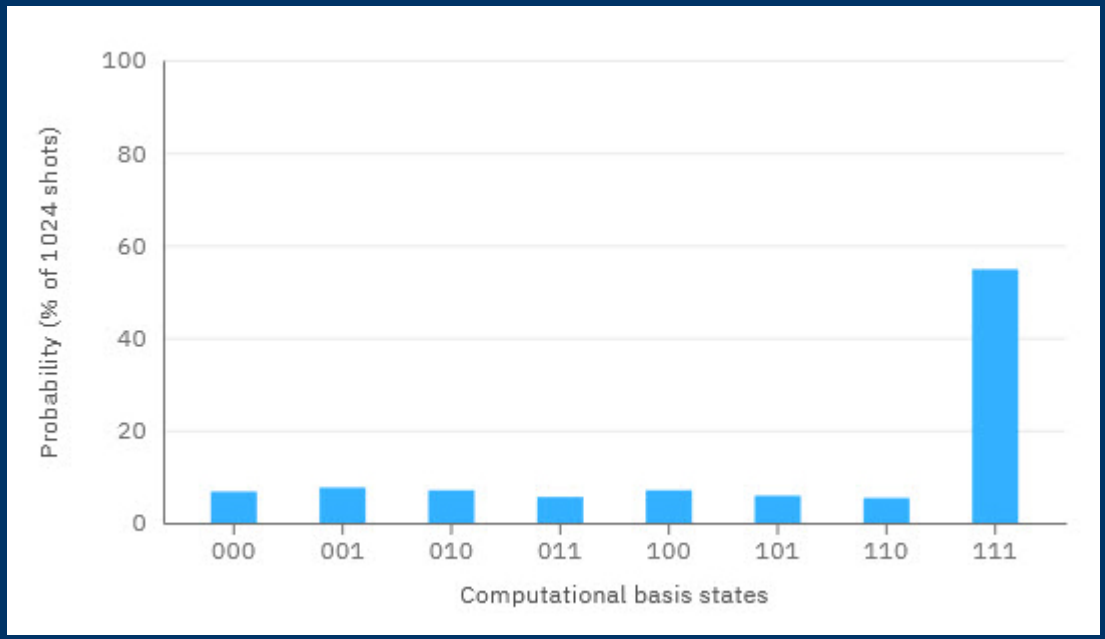
$\alpha \mapsto -\alpha + 2 \cdot m = 0,176$

$-0,08$

Laufzeit = $O(\sqrt{N})$

Grover mit 3 Qubits





Einwegfunktion

899095310588366277174404228586414024566849766837212553005901900739450280241887356469178?400144546069794935241533592195226090052854069740705333117963776189580061563580632285577739600649951333048633760 9

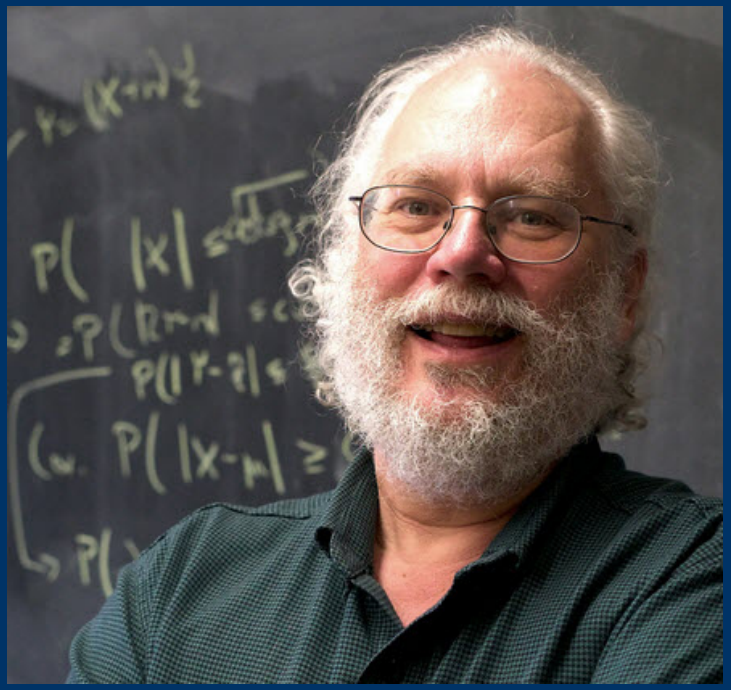
799021750781472446863793395126772763662312207522293560193498936718764209317443774306873?581268775424683010128229757471377245593393386776402256325179239344376990394831705016032169856102553287764768468 3

718396709185728164758130406575597352623217167087482423402776422026394961290886704476440994801319863981243307166157282762654782938524570528977832394574610476749833012203946414931566520673774507931502903050584619648991756886933554477735368981401645118938059505045083509169923154313966186550716311470774938467149320721564382277558501659803548182002418940885178176129421932040443775188846138890311614294 7

Faktorisierung

Exponentialzeit

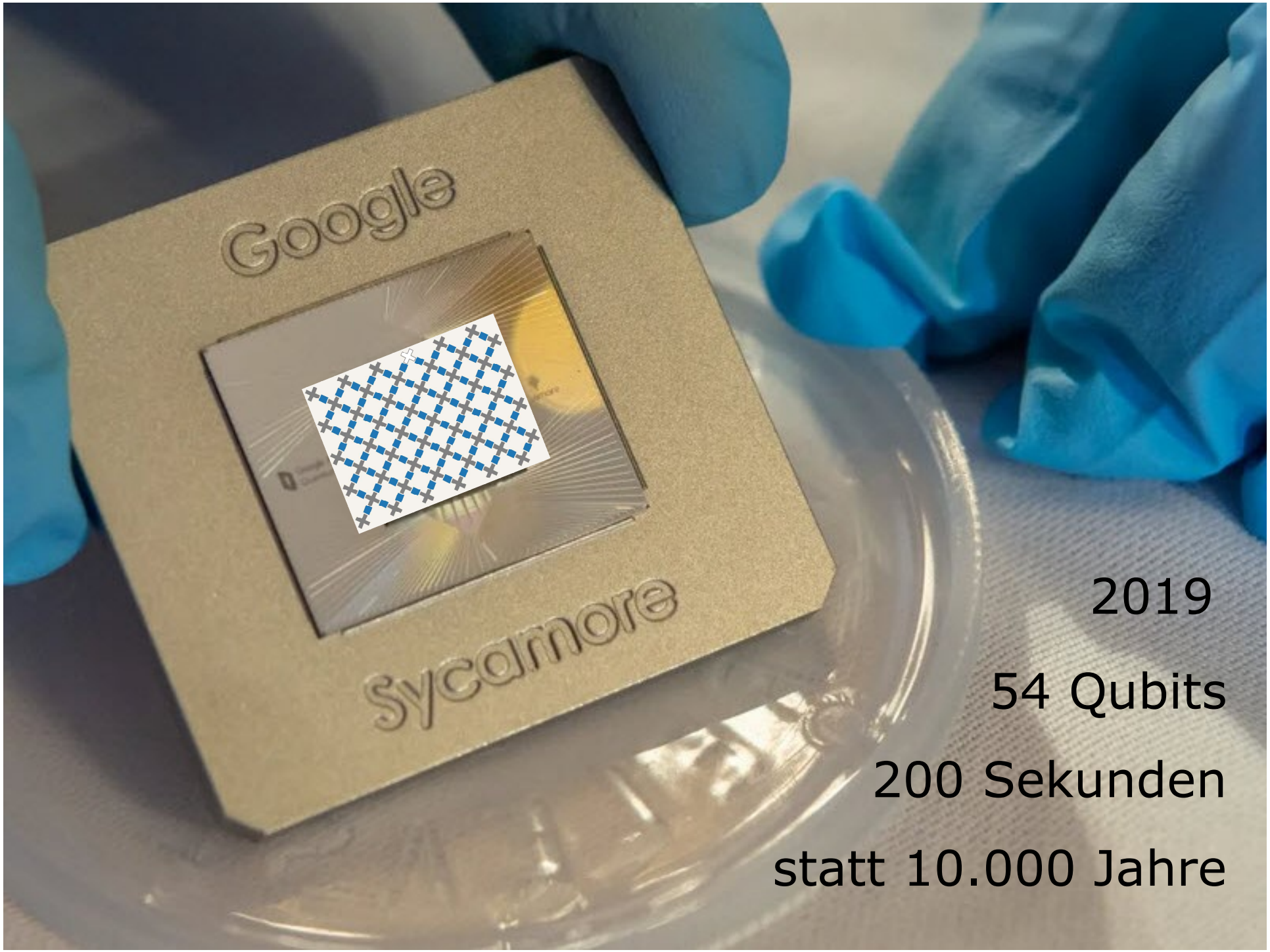
$\Rightarrow$ mehrere Jahre



1994: Peter Shor

Quantenalgorithmus in Polynomzeit

2001: IBM mit 7 Qubits: 15 = 5 * 3


Google
sycamore
2019
54 Qubits
200 Sekunden
statt 10.000 Jahre