THE STATE OF FACTORING ON QUANTUM COMPUTERS

arXiv:2410.14397

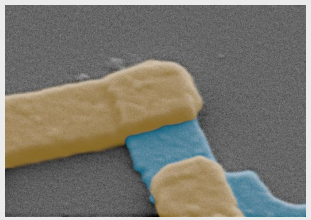
2024 I DR. DENNIS WILLSCH

supported by Bundesministerium für Bildung und Forschung
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

RESEARCH OVERVIEW

Simulating QCs

JUQCS (HPC)
Comput. Phys. Commun. 176, 121 (2007)
Comput. Phys. Commun. 237, 47 (2019)
Comput. Phys. Commun. 278, 108411 (2022)



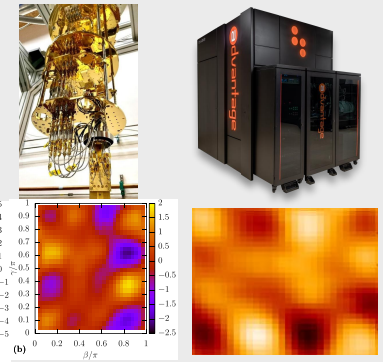
Superconducting Qubits (HPC)
Phys. Rev. A 96, 062302 (2017)
Phys. Rev. A 98, 052348 (2018)
PhD Thesis, arXiv:2008.13490 (2020)
Phys. Rev. A 101, 012327 (2020)
Phys. Rev. A 106, 022615 (2022)
Phys. Rev. A 108, 022604 (2023)

Benchmarking QCs

Benchmarking digital QCs
Comput. Phys. Commun. 220, 44 (2017)

Benchmarking the QAOA
Quantum Inf. Process. 19, 197 (2020)

Benchmarking analog QCs
Quantum Inf. Process. 21, 141 (2022)



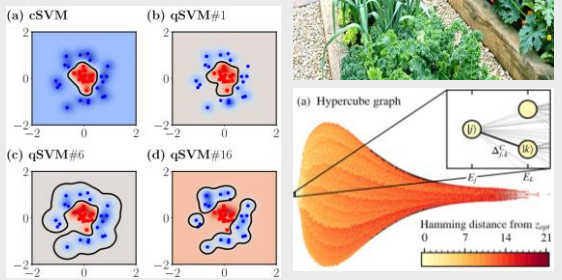
Algorithms on QCs

SVMs on Quantum Annealers
Comput. Phys. Commun. 248, 107006 (2020)

Garden Optimization
Quantum Inf. Process. 20, 305 (2021)

Unbalanced Penalization
Quantum Sci. Technol. 9, 025022 (2024)

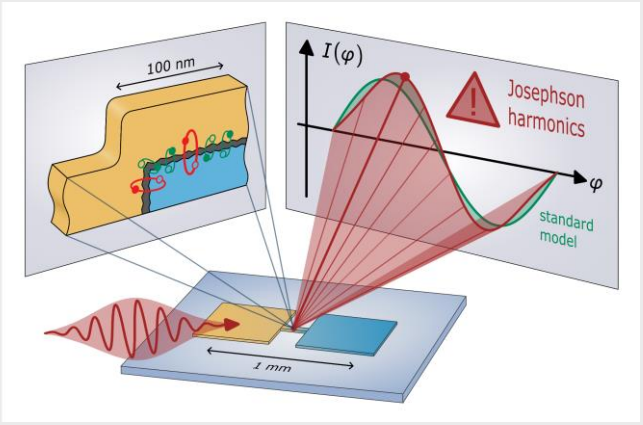
Guided Quantum Walk
Phys. Rev. Research 6, 013312 (2024)



Experiments with QCs

Fluxonium QND Readout
Phys. Rev. Applied 15, 064030 (2021)

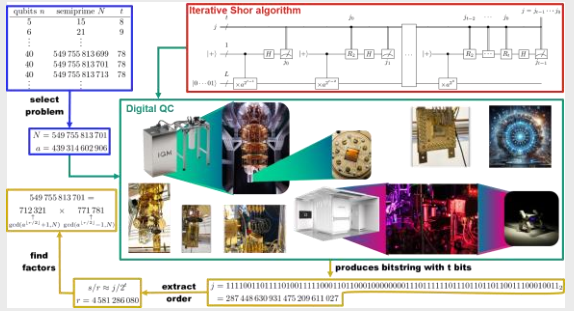
Josephson Harmonics
Nat. Phys. 20, 815 (2024)



Factoring on QCs

Shor's Algorithm
Mathematics 11, 4222 (2023)

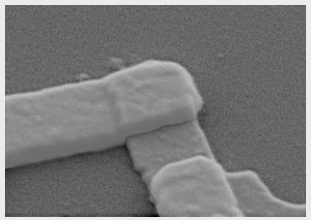
Quantum Factoring
arXiv:2410.14397 (2024)



RESEARCH OVERVIEW

Simulating QCs

JUQCS (HPC)
Comput. Phys. Commun. 176, 121 (2007)
Comput. Phys. Commun. 237, 47 (2019)
Comput. Phys. Commun. 278, 108411 (2022)



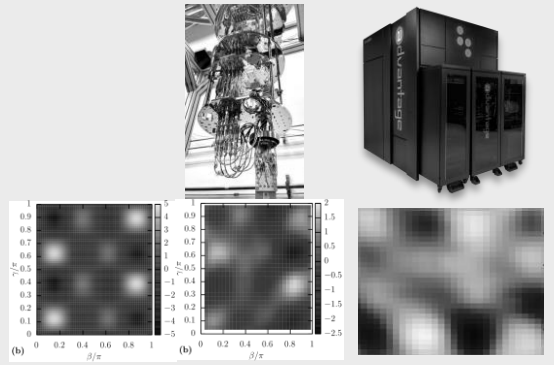
Superconducting Qubits (HPC)
Phys. Rev. A 96, 062302 (2017)
Phys. Rev. A 98, 052348 (2018)
PhD Thesis, arXiv:2008.13490 (2020)
Phys. Rev. A 101, 012327 (2020)
Phys. Rev. A 106, 022615 (2022)
Phys. Rev. A 108, 022604 (2023)

Benchmarking QCs

Benchmarking digital QCs
Comput. Phys. Commun. 220, 44 (2017)

Benchmarking the QAOA
Quantum Inf. Process. 19, 197 (2020)

Benchmarking analog QCs
Quantum Inf. Process. 21, 141 (2022)



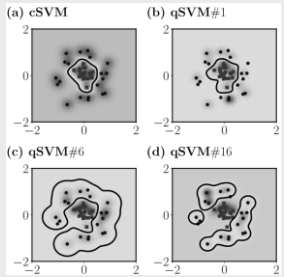
Algorithms on QCs

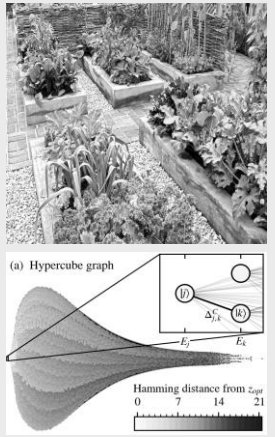
SVMs on Quantum Annealers
Comput. Phys. Commun. 248, 107006 (2020)

Garden Optimization
Quantum Inf. Process. 20, 305 (2021)

Unbalanced Penalization
Quantum Sci. Technol. 9, 025022 (2024)

Guided Quantum Walk
Phys. Rev. Research 6, 013312 (2024)

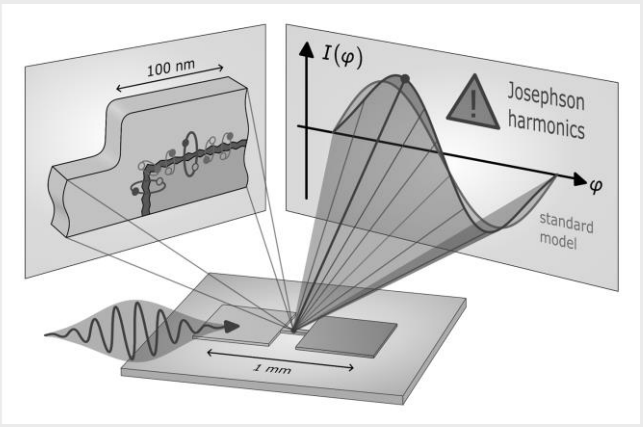




Experiments with QCs

Fluxonium QND Readout
Phys. Rev. Applied 15, 064030 (2021)

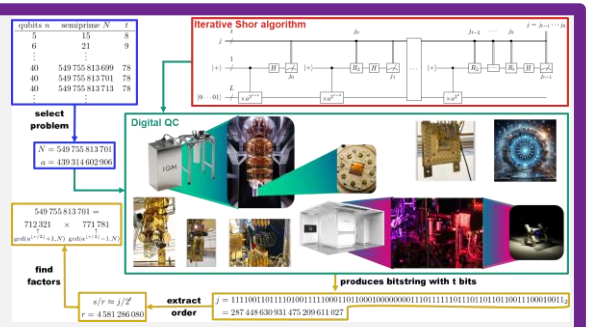
Josephson Harmonics
Nat. Phys. 20, 815 (2024)



Factoring on QCs

Shor's Algorithm
Mathematics 11, 4222 (2023)

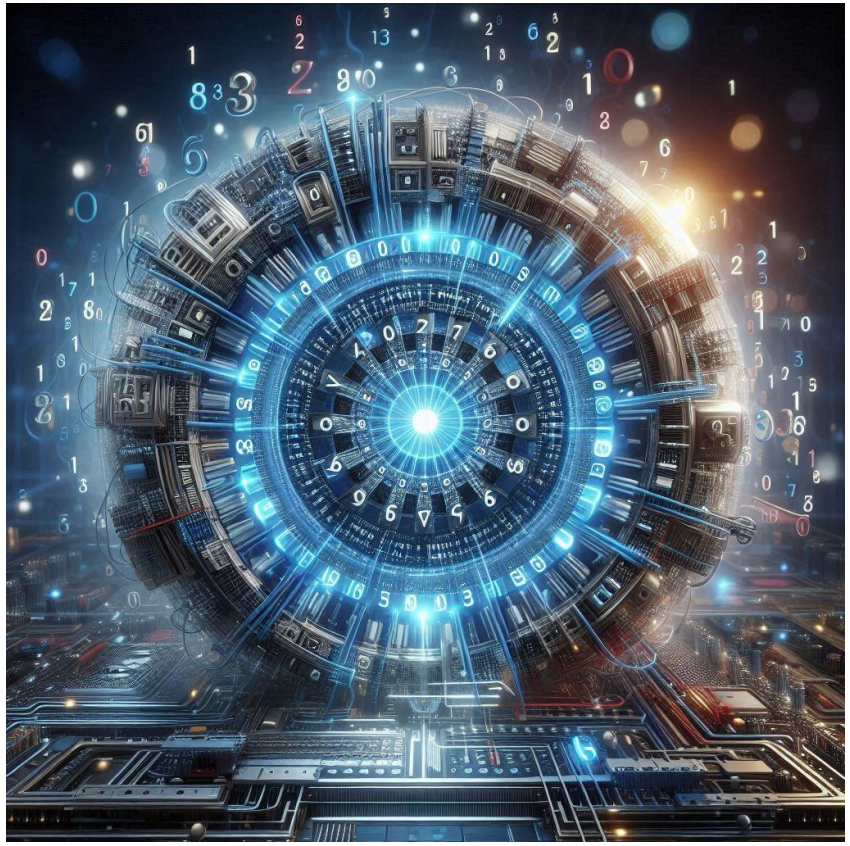
Quantum Factoring
arXiv:2410.14397 (2024)



THE STATE OF FACTORING ON QUANTUM COMPUTERS

Contents

1. Factoring Records
2. Factoring on Digital QCs
3. Factoring on Analog QCs
4. Future Perspectives



FACTORING PROBLEM

$$N = p \times q$$

Definition: Find a non-trivial factor of a composite L-bit integer N

Origin: One of the oldest mathematical problems with origins in ancient Greek times

Hardness: No classical polynomial-time algorithm known

Relevance: A lot of Internet security is based on this hardness

Public key cryptosystems like RSA used in TLS, SSH, …

FACTORING RECORDS

Digital QCs

Shor's Algorithm
N = 15, 21, (35) ~ 2^6

Martín-López et al., Nat. Photonics 6, 773 (2012)
Monz et al., Science 351, 1068 (2016)
Amico et al., Phys. Rev. A 100, 012305 (2019)

Careful: Oversimplified Shor's Algorithm
N ~ 2^{20000}

Smolin et al., Nature 499, 7457 (2013)
Gidney, algassert.com/post/2000 (2020)

Variational Quantum Factoring
N = 1099551473989 ~ 2^{41}

Anschuetz et al., arXiv:1808.08927 (2018)
Karamlou et al., npj Quantum Inf. 7, 156 (2021)

← Careful: preprocessed down to 3 qubits!

Schnorr's Algorithm
N = 261980999226229 ~ 2^{48}

Schnorr, cryptoeprint:2021/933 (2021)
Hegade and Solano, arXiv:2301.1105 (2023)

← seems not scalable? →

Ducas, github.com/lducas/SchnorrGate (2021)
Grebnev et al., IEEE Access 11, 134760 (2023)
Khattar and Yosri, arXiv:2307.09651 (2023)
Tesoro et al., arXiv:2410.16355 (2024)

Analog QCs

Direct Method
N = 1042441 ~ 2^{20}

Peng et al., Phys. Rev. Lett. 101, 220405 (2008)
Willsch et al., arXiv:2410.14397 (2024)

Multiplier Circuit
N = 8219999 ~ 2^{23}

Andriyash et al., Tech. Rep. 14-1002A-B (2016)
Jiang et al., Sci. Rep. 8, 17667 (2018)
Ding et al., Sci. Rep. 14, 3518 (2024)

Schnorr's Algorithm
N = 845546611823483 ~ 2^{50}

Schnorr, cryptoeprint:2021/933 (2021)
Yan et al., arXiv:2212.12372 (2022)
Wang et al., Chin. J. Comput. 47, 13015 (2024)

Simulated Digital QCs

Shor's Algorithm
N = 549755813701 ~ 2^{39}

Willsch et al., Mathematics 11, 4222 (2023)

Classical (Super)Computers

Number Field Sieve
N = RSA-250 ~ 10^{250} ~ 2^{829}

Boudot et al., CRYPTO 2020, 62 (2020)

Schnorr's Algorithm
N ~ 2^{100}

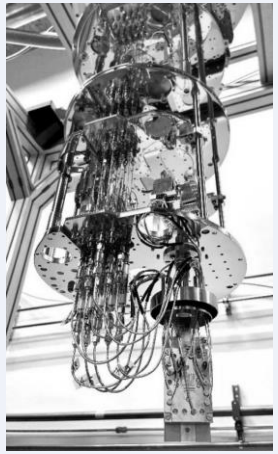
Tesoro et al., arXiv:2410.16355 (2024)

FACTORING RECORDS

Digital QCs

Shor's Algorithm
N = 15, 21, (35) ~ 2^6
Martín-López et al., Nat. Photonics 6, 773 (2012)
Monz et al., Science 351, 1068 (2016)
Amico et al., Phys. Rev. A 100, 012305 (2019)

Careful: Oversimplified Shor's Algorithm
N ~ 2^{20000}
Smolin et al., Nature 499, 7457 (2013)
Gidney, algassert.com/post/2000 (2020)



Variational Quantum Factoring
N = 1099551473989 ~ 2^{41}
Anschuetz et al., arXiv:1808.08927 (2018)
Karamlou et al., npj Quantum Inf. 7, 156 (2021)

← Careful: preprocessed down to 3 qubits!

Schnorr's Algorithm
N = 261980999226229 ~ 2^{48}
Schnorr, cryptoeprint:2021/933 (2021)
Hegade and Solano, arXiv:2301.1105 (2023)

← seems not scalable? →
Ducas, github.com/lducas/SchnorrGate (2021)
Grebnev et al., IEEE Access 11, 134760 (2023)
Khattar and Yosri, arXiv:2307.09651 (2023)
Tesoro et al., arXiv:2410.16355 (2024)

Analog QCs

Direct Method
N = 1042441 ~ 2^{20}
Peng et al., Phys. Rev. Lett. 101, 220405 (2008)
Willsch et al., arXiv:2410.14397 (2024)

Multiplier Circuit
N = 8219999 ~ 2^{23}
Andriyash et al., Tech. Rep. 14-1002A-B (2016)
Jiang et al., Sci. Rep. 8, 17667 (2018)
Ding et al., Sci. Rep. 14, 3518 (2024)

Schnorr's Algorithm
N = 845546611823483 ~ 2^{50}
Schnorr, cryptoeprint:2021/933 (2021)
Yan et al., arXiv:2212.12372 (2022)
Wang et al., Chin. J. Comput. 47, 13015 (2024)

Simulated Digital QCs

Shor's Algorithm
N = 549755813701 ~ 2^{39}
Willsch et al., Mathematics 11, 4222 (2023)

Classical (Super)Computers

Number Field Sieve
N = RSA-250 ~ 10^{250} ~ 2^{829}
Boudot et al., CRYPTO 2020, 62 (2020)

Schnorr's Algorithm
N ~ 2^{100}
Tesoro et al., arXiv:2410.16355 (2024)

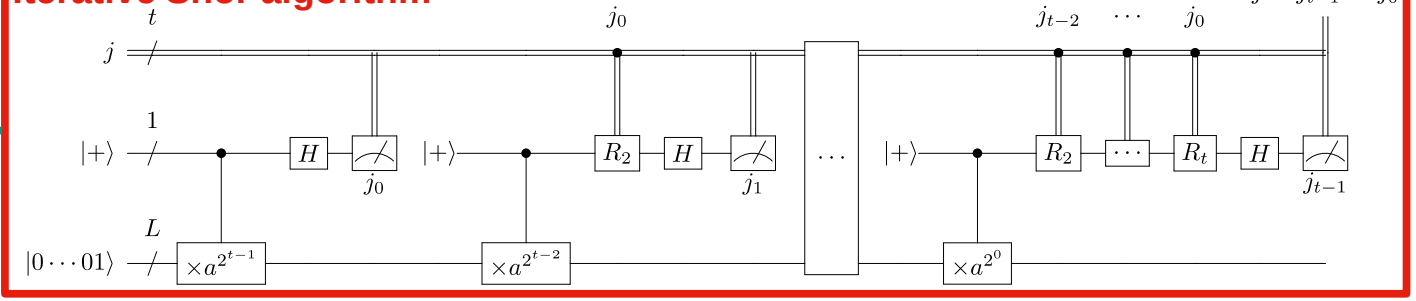
DIGITAL QCS: SHOR'S FACTORING ALGORITHM

qubits n	semiprime N	t
5	15	8
6	21	9
⋮	⋮	
40	549 755 813 699	78
40	549 755 813 701	78
40	549 755 813 713	78
⋮	⋮	

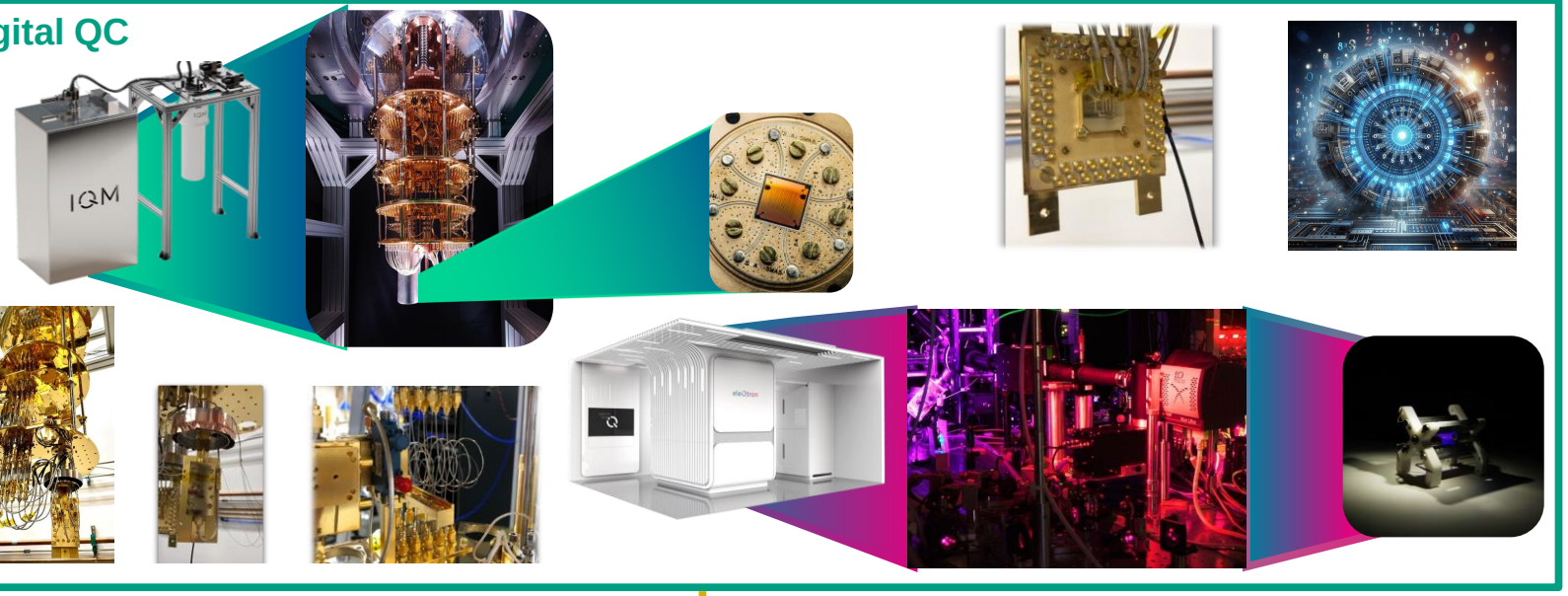
select problem

$N = 549\,755\,813\,701$
$a = 439\,314\,602\,906$

Iterative Shor algorithm



Digital QC



produces bitstring with t bits

$j = 11110011011110100111110001101100010000000011101111101110110110110011100010011_2$
$= 287\,448\,630\,931\,475\,209\,611\,027$

extract order

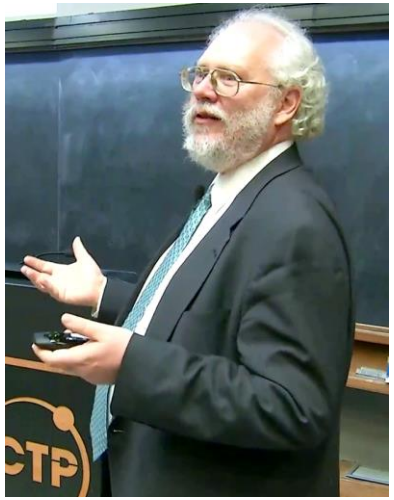
$s/r \approx j/2^t$
$r = 4\,581\,286\,080$

find factors

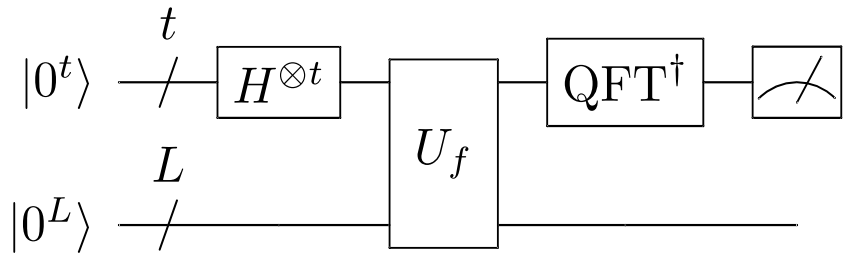
$549\,755\,813\,701 =$
$712\,321 \times 771\,781$
$\gcd(a^{\lfloor r/2 \rfloor}+1, N)$ $\gcd(a^{\lfloor r/2 \rfloor}-1, N)$

SHOR'S FACTORING ALGORITHM

The quantum part



- **Conventional** Shor algorithm needs 3L qubits

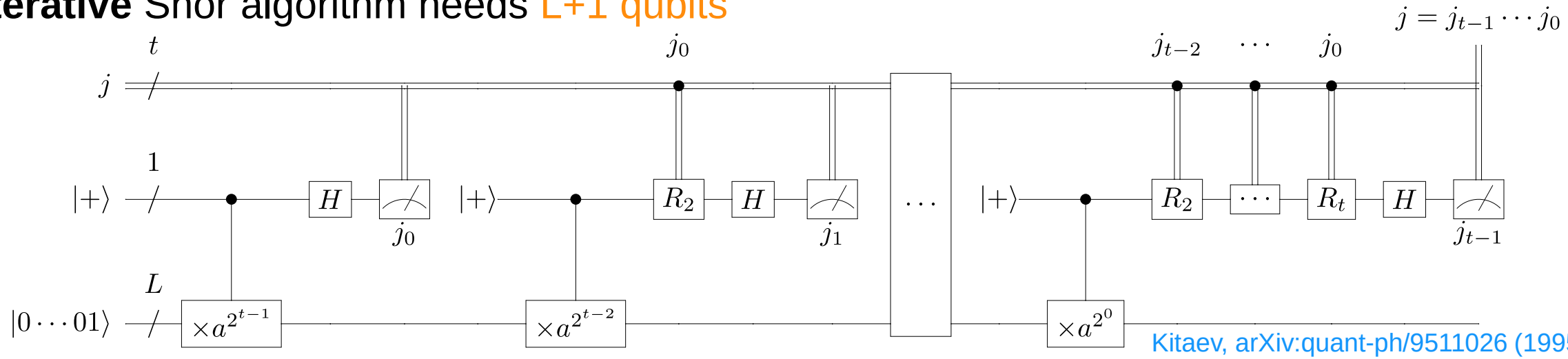


$$t \approx 2L$$

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus (a^x \bmod N)\rangle$$

Shor, Proc. Found. Comp. Sci. 35, 124 (1994)
Shor, SIAM J. Comput. 26, 1484 (1997)

- **Iterative** Shor algorithm needs L+1 qubits



Kitaev, arXiv:quant-ph/9511026 (1995)
Griffiths and Niu, PRL 76, 3228 (1996)

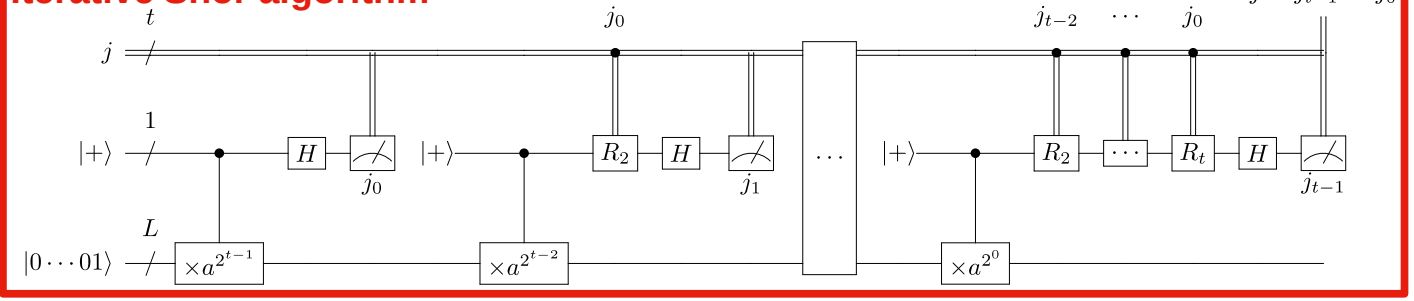
SHOR'S FACTORING ALGORITHM — SIMULATION

qubits n	semiprime N	t
5	15	8
6	21	9
⋮	⋮	
40	549 755 813 699	78
40	549 755 813 701	78
40	549 755 813 713	78
⋮	⋮	

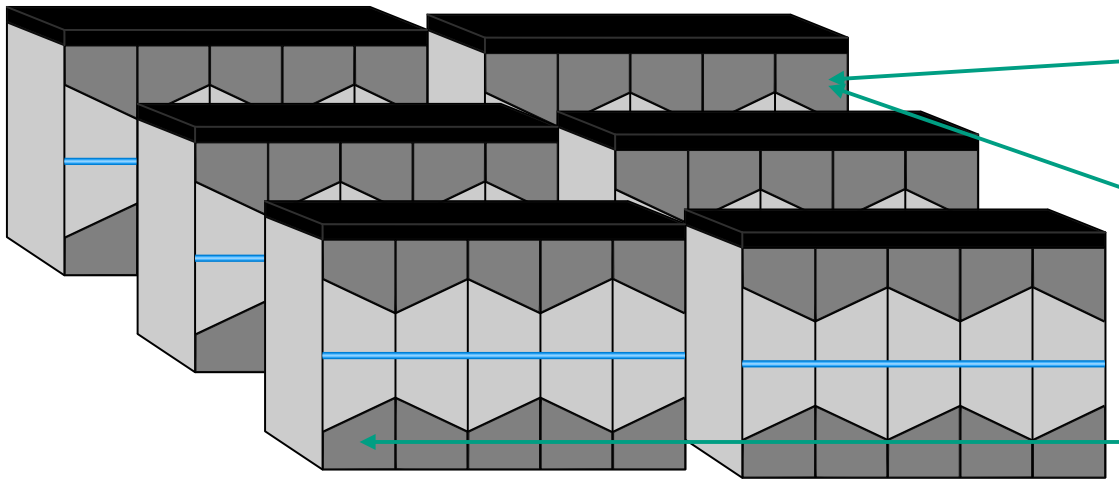
select problem

$N = 549\,755\,813\,701$
$a = 439\,314\,602\,906$

Iterative Shor algorithm



Simulation on 2048 GPUs



GPU #0

$$\begin{pmatrix} \psi_{00000000000\,0\cdots0} \\ \vdots \\ \psi_{00000000000\,1\cdots1} \end{pmatrix}$$

GPU #1

$$\begin{pmatrix} \psi_{00000000001\,0\cdots0} \\ \vdots \\ \psi_{00000000001\,1\cdots1} \end{pmatrix}$$

GPU #2047

$$\begin{pmatrix} \psi_{11111111111\,0\cdots0} \\ \vdots \\ \psi_{11111111111\,1\cdots1} \end{pmatrix}$$

Large-Scale Simulation of Shor's Quantum Factoring Algorithm, **Mathematics** 11, 4222 (2023)

produces bitstring with t bits

$j = 11110011011110100111110001101100010000000011101111101110110110110011100010011_2$
$= 287\,448\,630\,931\,475\,209\,611\,027$

extract order

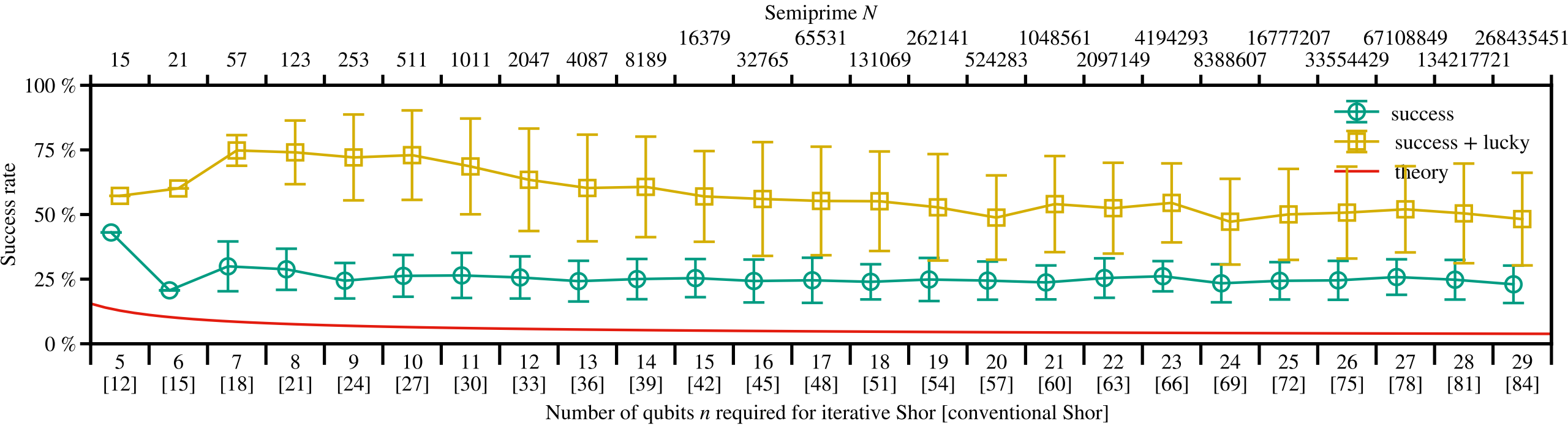
$s/r \approx j/2^t$
$r = 4\,581\,286\,080$

find factors

$549\,755\,813\,701 =$
$712\,321 \times 771\,781$
$\gcd(a^{\lfloor r/2 \rfloor}+1, N)$ $\gcd(a^{\lfloor r/2 \rfloor}-1, N)$

SHOR'S FACTORING ALGORITHM

Simulation Results



- **Average shows:** Performance much better than predicted by theory
- Success rate approaches ~ 50 % with so-called "lucky" cases
- **More information:**
  Large-Scale Simulation of Shor's Quantum Factoring Algorithm, **Mathematics** 11, 4222 (2023)

"lucky":
Conditions not satisfied—
But factoring works anyway!

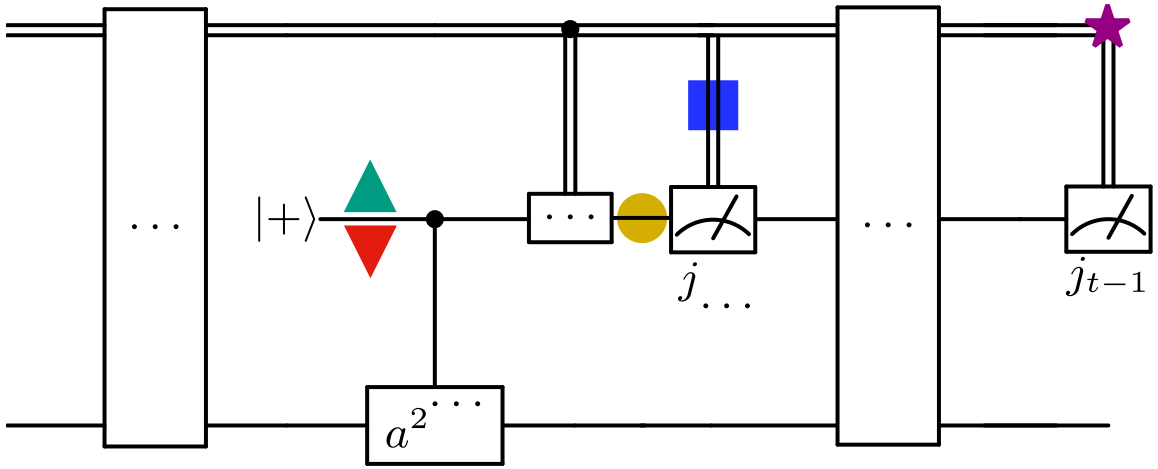
SHOR'S FACTORING ALGORITHM

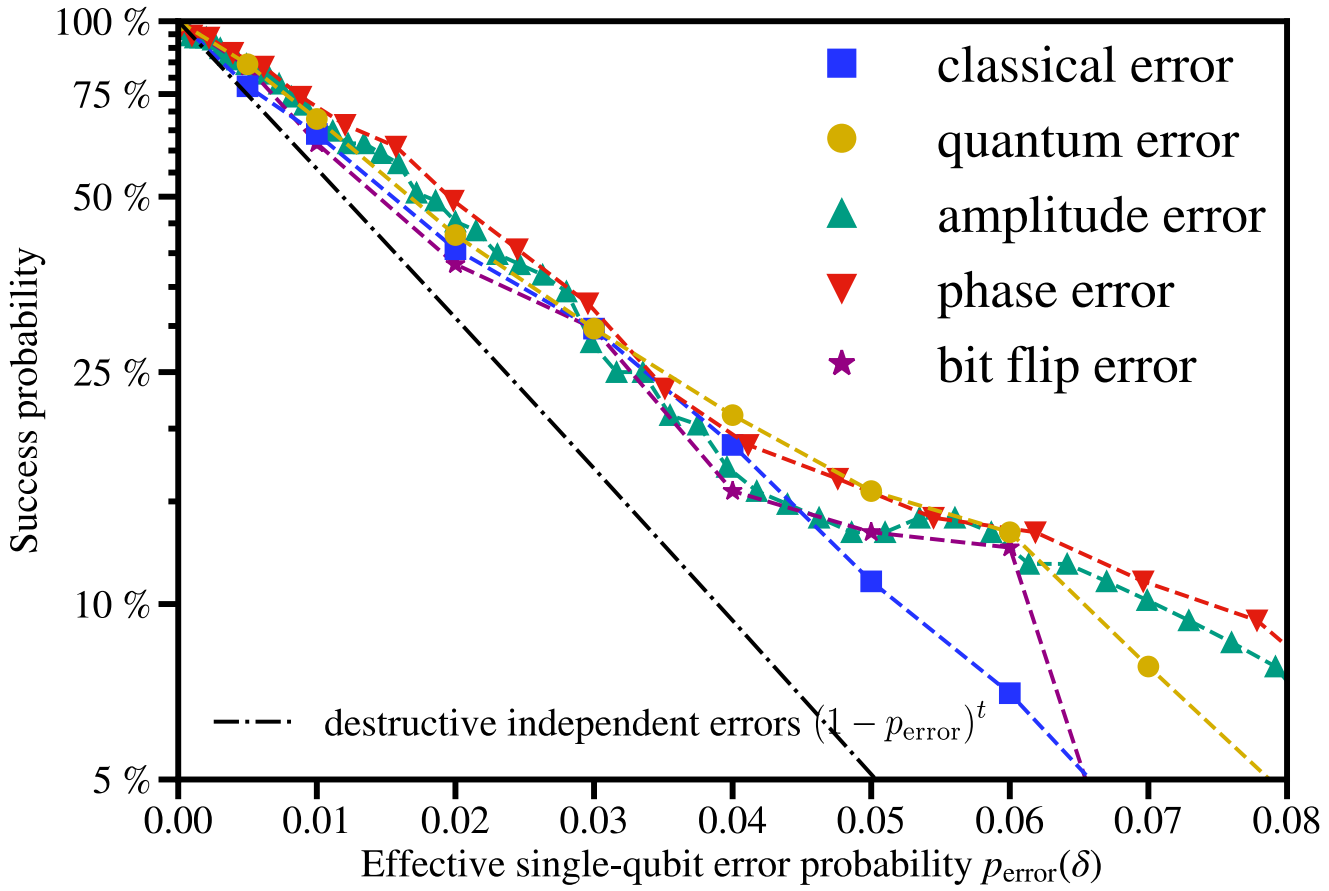
Performance under errors

- **Efficient post-processing** can bring success arbitrarily close to 100%

  Ekerå, Quantum Inf. Process. 20, 205 (2021)
  Ekerå, ACM Trans. Quantum Comput. 5, 11 (2024)

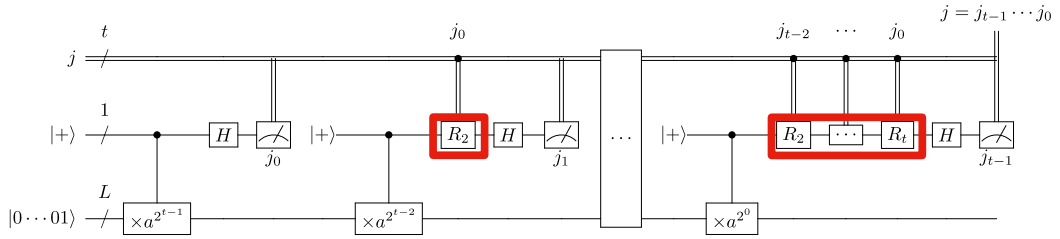
- But what happens under **errors**?





SHOR'S FACTORING ALGORITHM

A particularly interesting error



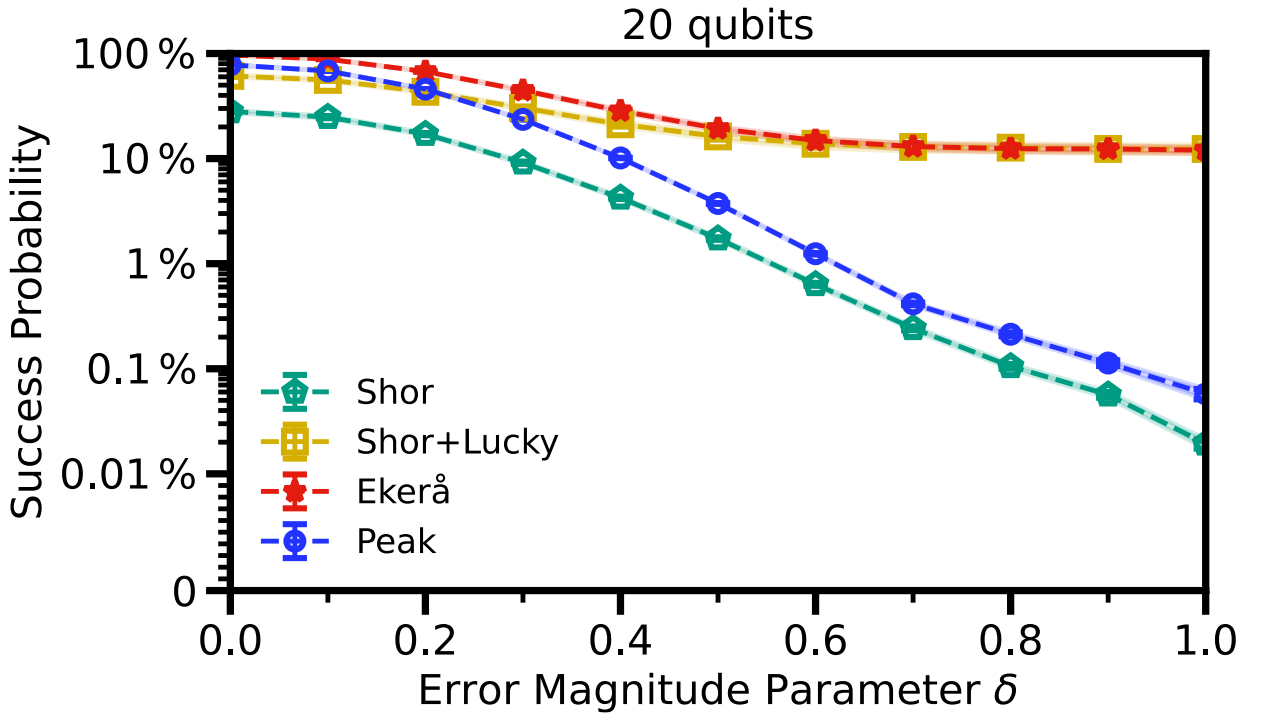
- Gaussian noise on rotation gates:

$$\widetilde{R_k} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(1+\delta r)/2^k} \end{pmatrix}$$

- Cai can **formally prove** that Shor fails!

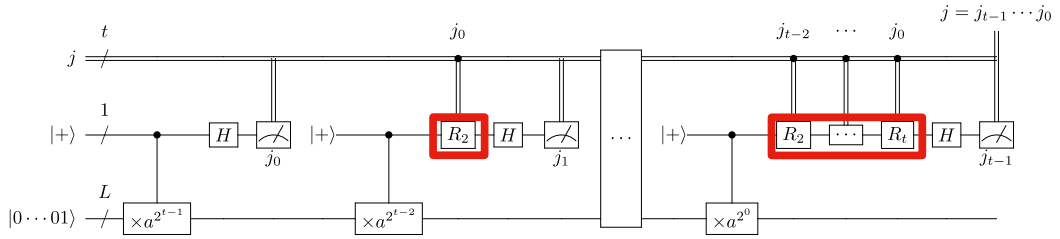
  Cai, Sci. China Inf. Sci. 67, 1 (2024)

- **Question:** Does that also affect the Ekerå-post-processed and the "lucky" cases?



SHOR'S FACTORING ALGORITHM

A Particular "Software" Error

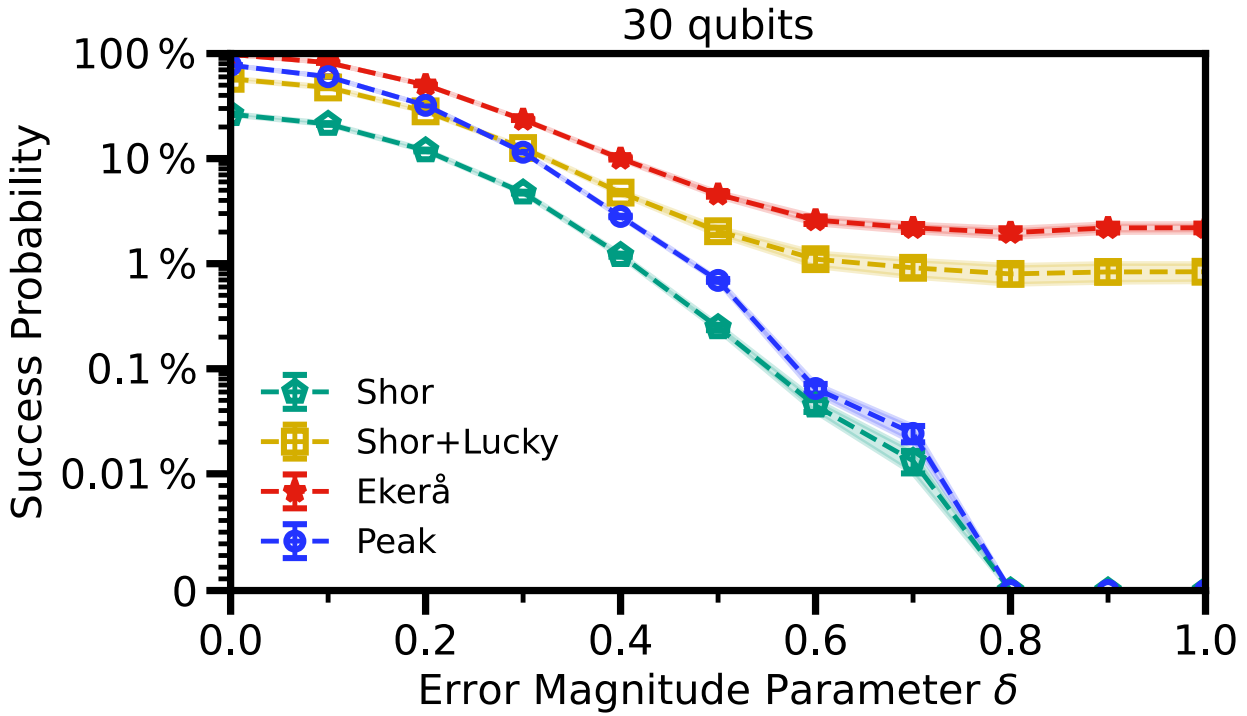


- Gaussian noise on rotation gates:

$$\widetilde{R_k} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(1+\delta r)/2^k} \end{pmatrix}$$

- Cai can **formally prove** that Shor fails!

  Cai, Sci. China Inf. Sci. 67, 1 (2024)



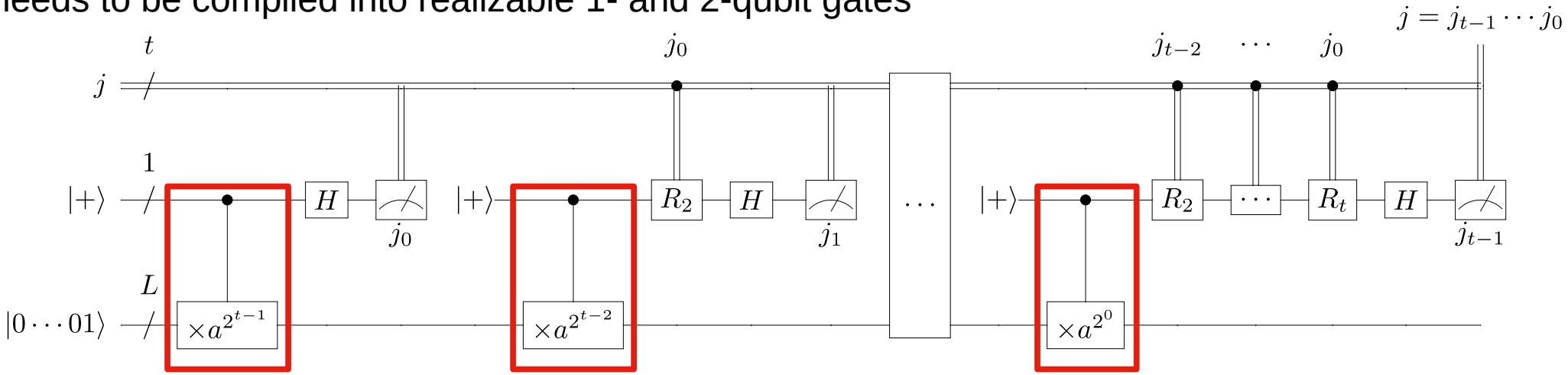
- **Question:** Does that also affect the Ekerå-post-processed and the "lucky" cases?
- **Conclusion:** Not as severely!
- **But:** General consensus is that quantum error correction is required

arXiv:2410.14397

SHOR'S FACTORING ALGORITHM

Hardware challenges

- Algorithm needs to be compiled into realizable 1- and 2-qubit gates



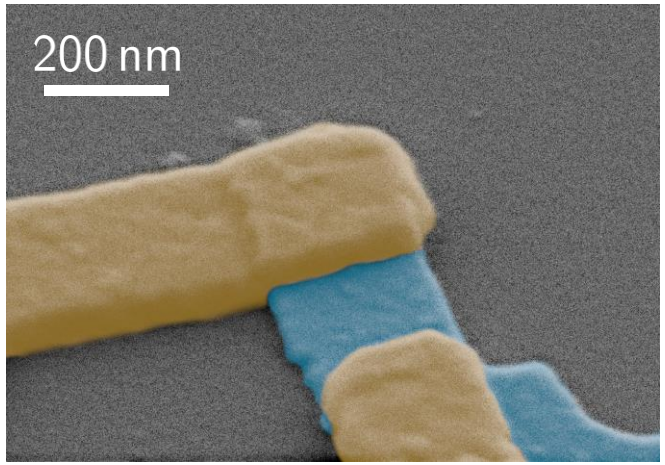
- Takes 2L+3 or 2L+1 qubits
  Beauregard, Quantum Inf. Comput. 3, 175 (2003)
  Gidney, arXiv:1706.07884 (2018)
  (or ~ 1.5L qubits with a trick)
  Zalka, arXiv:quant-ph/0601097 (2006)
  instead of L+1 qubits
- **Recent new development:** Maybe only L/2 qubits?
  Chevignard, Fouque and Schrottenloher, cryptoeprint:2024/022 (2024)

But still: Massive increase in number of gates!

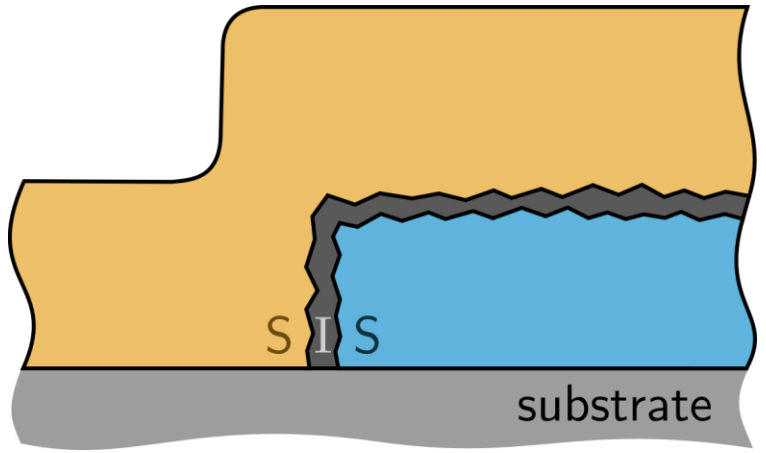
Bits in N	N	# Gates
4	15	9 308
10	1007	181 652
25	33554089	4 657 463

HARDWARE CHALLENGES: JOSEPHSON HARMONICS

Josephson (1962)



?



Experiments with QCs

Fluxonium QND Readout
Phys. Rev. Applied 15, 064030 (2021)

Josephson Harmonics
Nat. Phys. 20, 815 (2024)

$$H = 4E_C n^2 - \cancel{E_J \cos\varphi} - \sum_m E_{Jm} \cos\, m\varphi$$

Paper: Willsch & Rieger et al.,
Nat. Phys. 20, 815 (2024)

Talk: https://youtu.be/dWu3lCwyXBM

Conclusion: Standard Model does not work!

- Fundamental challenge!
- But also an opportunity?

HARDWARE CHALLENGES: ERRORS

Idea: Erroneous NISQ devices
→ Try variational algorithm?

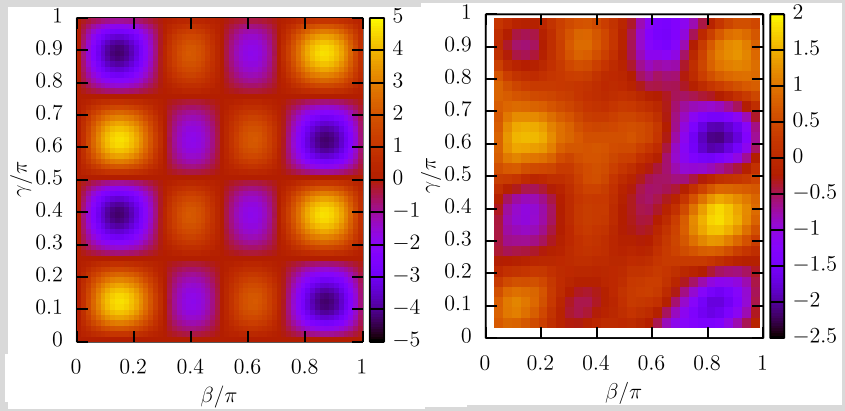
Variational Quantum Factoring
N = 1099551473989 ~ 2^{41}
Anschuetz et al., arXiv:1808.08927 (2018)
Karamlou et al., npj Quantum Inf. 7, 156 (2021)

Careful: only 3 qubits!

Benchmarking QCs

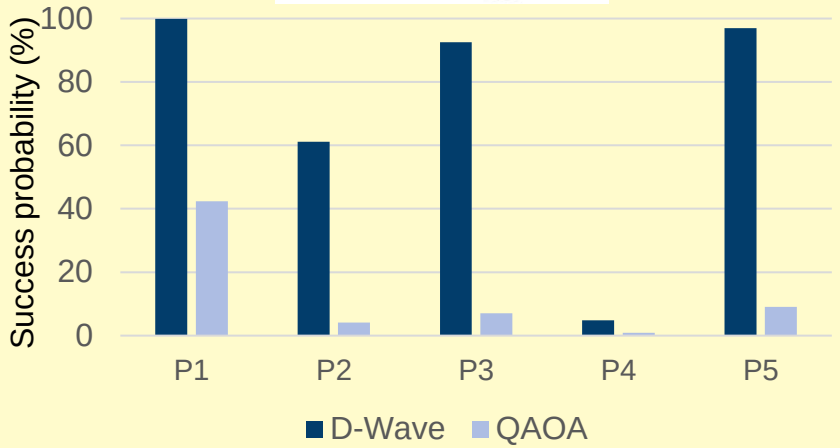
Benchmarking digital QCs
Comput. Phys. Commun. 220, 44 (2017)
Benchmarking the QAOA
Quantum Inf. Process. 19, 197 (2020)
Benchmarking analog QCs
Quantum Inf. Process. 21, 141 (2022)

Gate-based quantum computer



Simulation IBM-Q device

Quantum annealer



Conclusion:

- If the problem is already in QUBO/Ising form
  - Do not use digital QCs
  - Try analog QCs

The D-Wave quantum annealer (= experiment) outperforms QAOA executed on a simulator (= under optimal conditions)

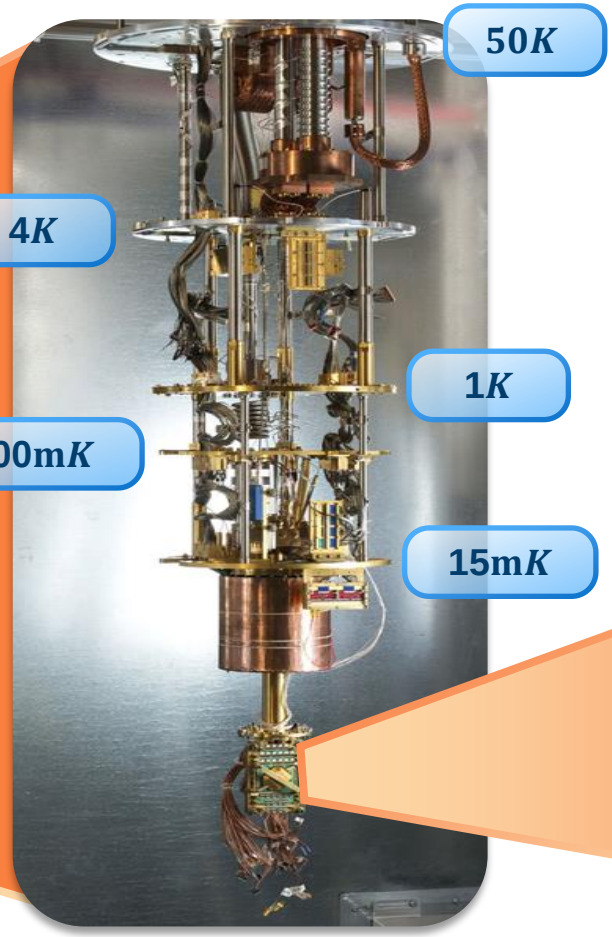
ANALOG QCS

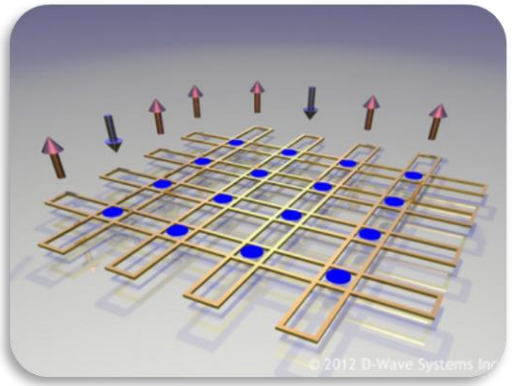
Device: D-Wave “Advantage” Quantum Annealer

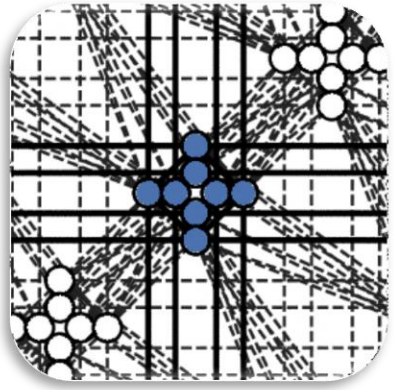
D-Wave The Quantum Computing Company™ **Advantage**

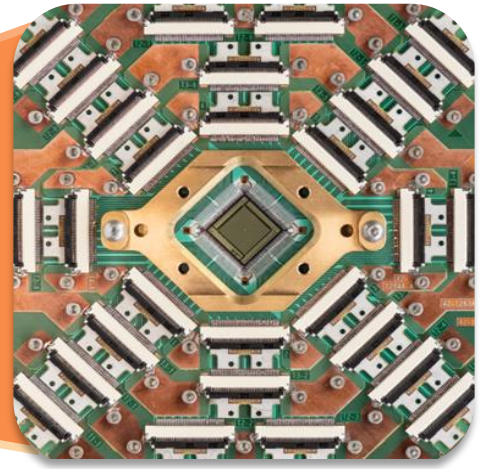
Quantum Processing Unit

5640 superconducting qubits
Pegasus topology with 40.484 couplers









FACTORING ON ANALOG QCS

Mehtods

- Problem needs to be expressed as QUBO / Ising
- We investigated **3 approaches**:

QUBO: $\min_{x_i=0,1} \left(\sum_{i \leq j}^{N-1} x_i Q_{ij} x_j + c \right)$

Ising: $\min_{s_i=\pm 1} \left(\sum_{i=0}^{N-1} h_i s_i + \sum_{i<j}^{N-1} J_{ij} s_i s_j + C \right)$

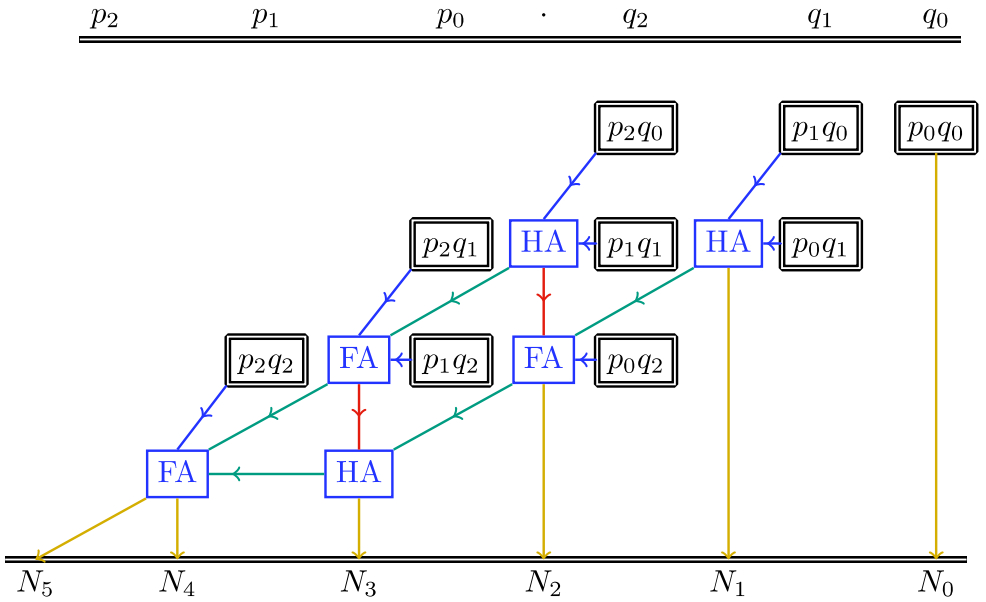
Direct Method

Peng et al., Phys. Rev. Lett. 101, 220405 (2008)

$$\min_{p,q} (N - pq)^2$$

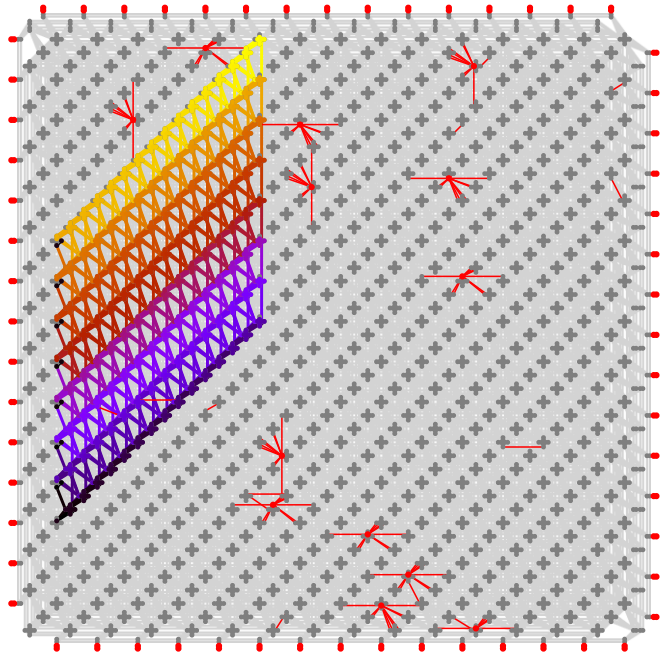
Multiplication Circuit Method

Andriyash et al, D-Wave TR 14-1002A-B (2016)



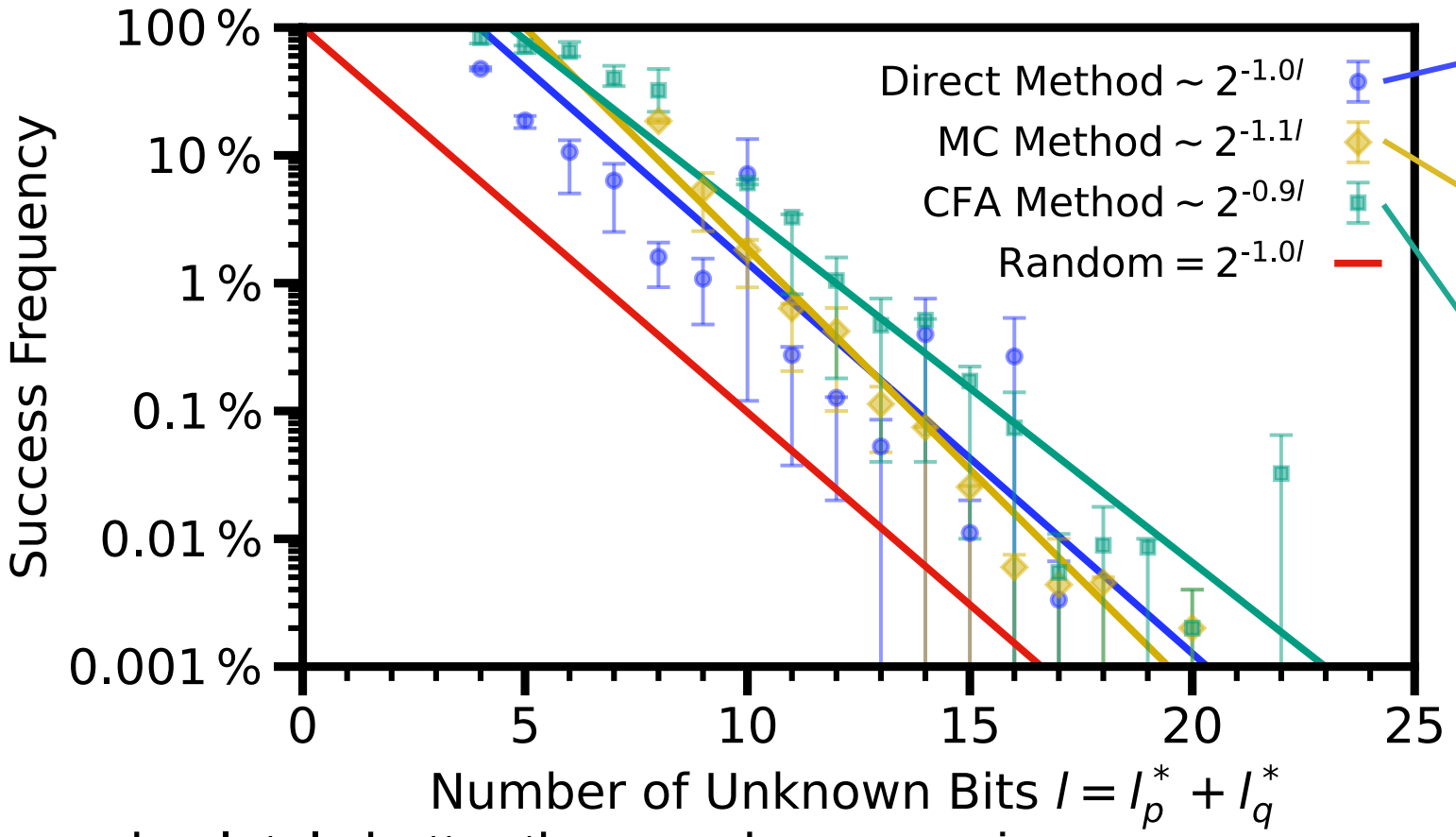
Controlled Full-Adder Method

Ding et al., Sci. Rep. 14, 1 (2024)

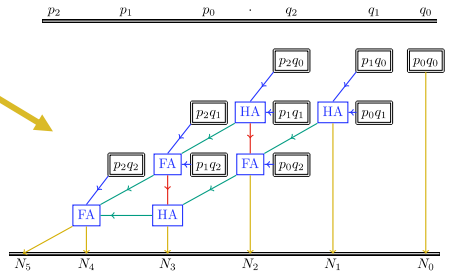


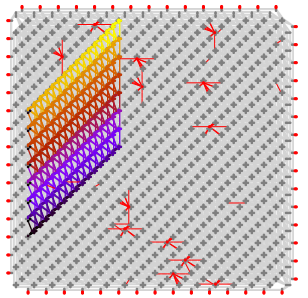
ANALOG QCS

Results



$$\min_{p,q} (N - pq)^2$$

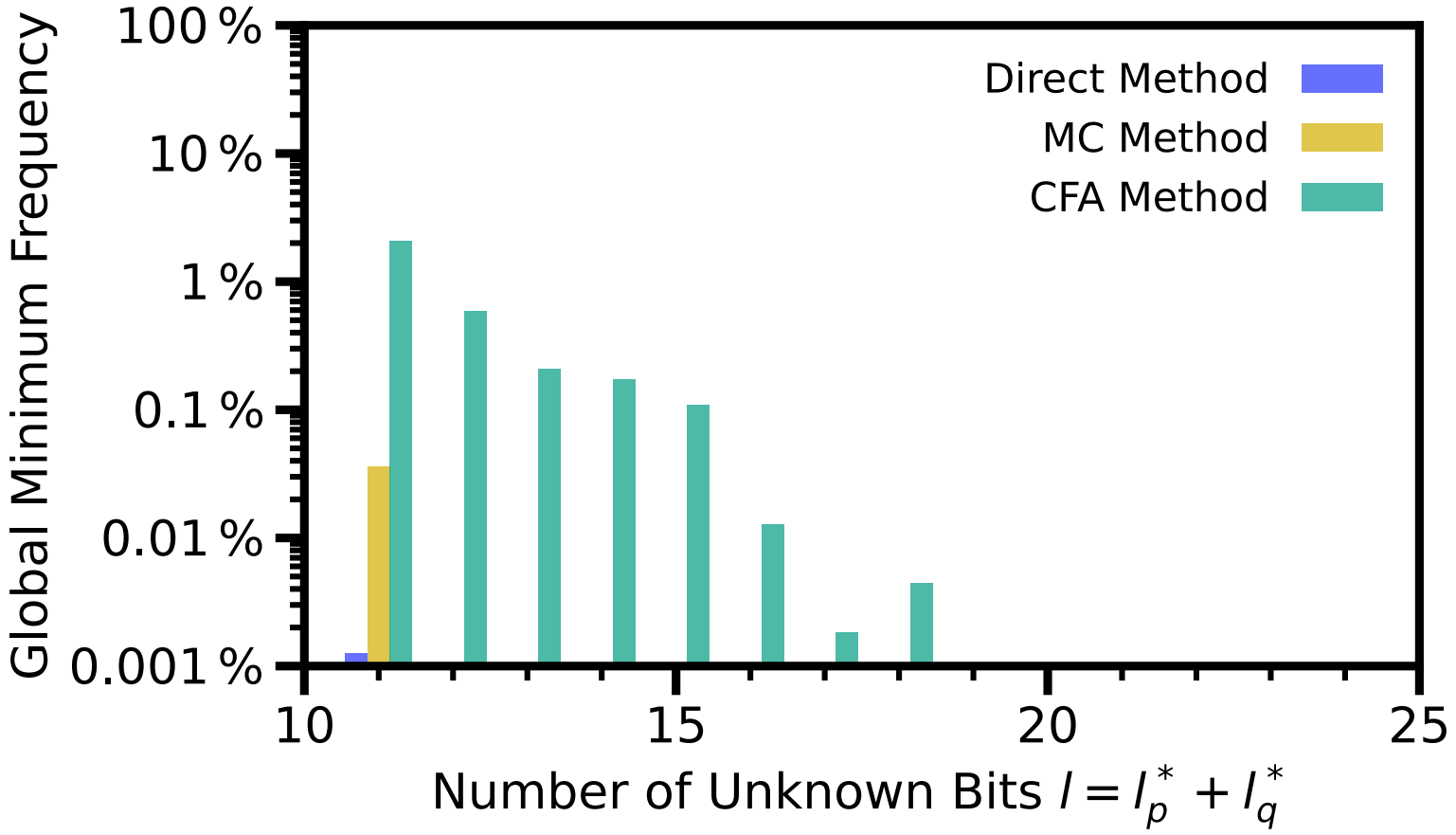


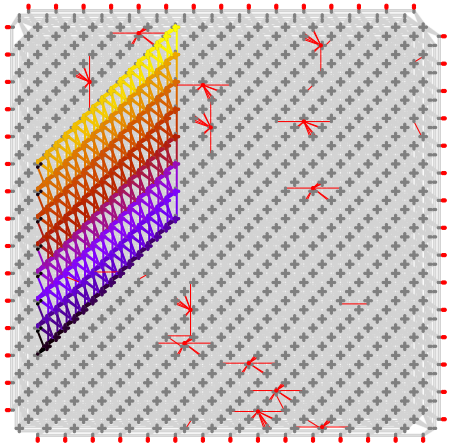


- All methods are absolutely better than random guessing
- CFA method also scales better
- **BUT:** All methods scale exponentially!

ANALOG QCS

Results





- CFA method finds true ground state much more often!
- **Reason:** Custom embedding on the hardware

SUMMARY

Factoring on Quantum Computers

- **Many different approaches**

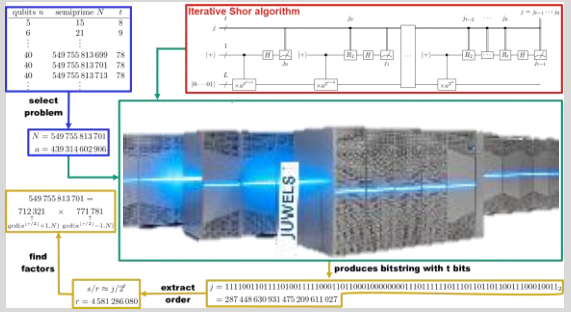
Future perspectives:

- Large RSA integers
  - Likely require quantum error correction
  - Likely require millions of qubits

Gidney and Ekerå, Quantum 5, 433 (2021)

  - Likely not factorizable anytime soon

- **But:** Larger semiprimes than we can factor with Shor on HPC maybe soon ☺



- <u>Present evidence:</u> Only Shor and derivatives seem to scale

Shor, Proc. Found. Comp. Sci. 35, 124 (1994)
Ekerå and Håstad, PQCrypto 2017, 347 (2017)
CFS, cryptoeprint:2024/022 (2024)

- **Many challenges**
  - Software and hardware errors on digital QCs
  - New method on analog QCs

THANK YOU FOR YOUR ATTENTION

Further References:

Willsch et al., Mathematics 11, 4222 (2023)
Hanussek, DOI:10.34734/FZJ-2024-05254 (2024)
Hanussek, jugit.fz-juelich.de/qip/jupsifactoring (2024)
Willsch et al., arXiv:2410.14397 (2024)