Quantum Computing
A historical overview and recent frontiers

Matteo De Francesco

ALGO Seminar

22nd May 2026

Plan

1: Origins **1920s–1982**

Quantum mechanics, EPR paradox, Bell inequalities, Feynman's proposal

2: First Algorithms **1984–1997**

BB84, Simon's, Shor's, Grover, BBBV lower bound

3: Complexity Theory **1997–2010**

BQP, *Kitaev's* QMA-*completeness*, QIP = PSPACE

4: The Sampling Paradigm **2009–2016**

BosonSampling, QAOA, Forrelation

5: Recent Frontiers **2017–2026**

Raz-Tal, RCS, PoQ, Yamakawa-Zhandry, Quantum crypto

Origins & Motivation

Why Quantum?

Quantum mechanics: a fundamentally different description of nature. How particles at smaller scales behave?

Double-slit experiment (1801): First evidence that particles *interferes*

1920s: Pauli exclusion principle (Pauli), Matrix formalization of quantum mechanics (Born) continuous description (Schrödinger)

Qubit and quantum state

A **qubit** is a unit vector in $\mathbb{C}^2$: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. A state of n qubits lives in $\mathbb{C}^{2^n}$:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle, \qquad \sum_x |\alpha_x|^2 = 1.$$

Few rules: $|0\rangle = (1\ 0)^T$ and $|1\rangle = (0\ 1)^T$. Only unitaries $U \in \mathbb{C}^{2^n\times 2^n}$ can be applied to $|\psi\rangle$. *Measuring* $|\psi\rangle$ collapses it into a single bitstring $x \in \{0,1\}^n$ with probability $|\alpha_x|^2$.

Entanglement & Bell Inequalities

EPR paradox (Einstein-Podolsky-Rosen, 1935): is quantum mechanics *complete*, or are there hidden variables that restore classical determinism?

Bell 1964

No local hidden variable theory can reproduce all predictions of quantum mechanics. Bell's inequality provides a *testable* criterion.

Bell state: $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This state is entangled: it cannot be written as $|\phi\rangle \otimes |\psi\rangle$.
Motivated the *CHSH* and *GHZ* games.

Aspect's experiment (1982): first conclusive experimental violation of Bell inequalities $\Rightarrow$ *entanglement is real, non-local, and unavoidable*.

Legenda: $|\Phi^+\rangle$ is a 2-qubit state (2^2 possibilities) where the two qubits are (with prob. $1/2$) both in 0, and (with prob. $1/2$) both in 1

Feynman's Proposal (1981) and Deutsch's Model (1985)

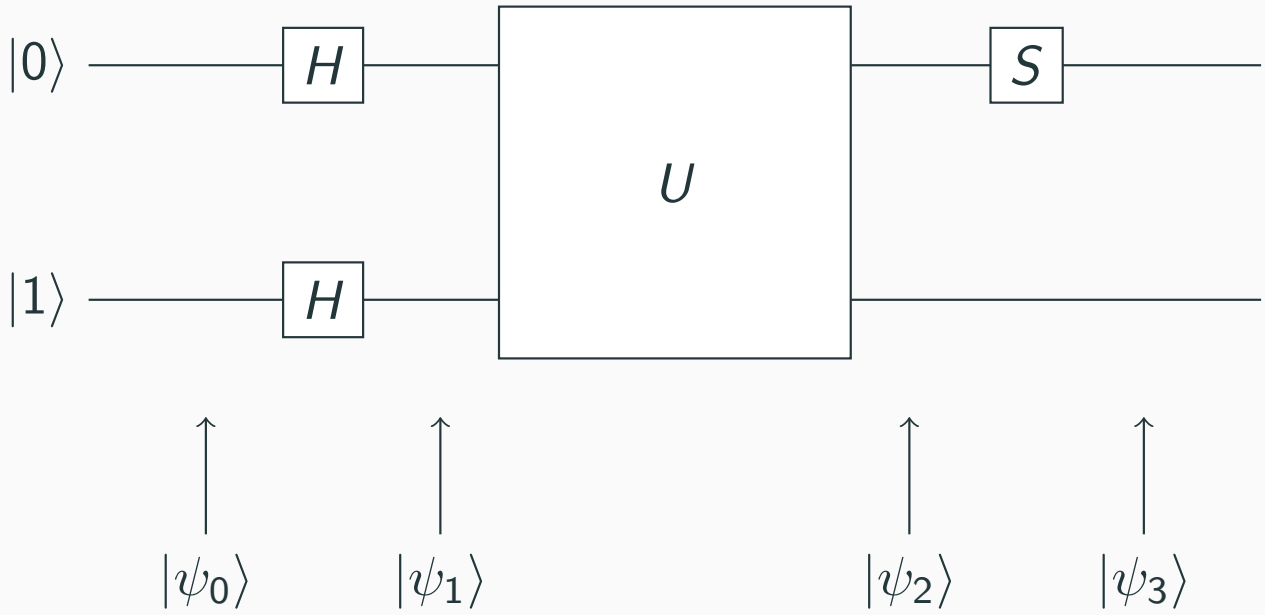
Feynman's observation: Storing $|\psi\rangle$ in a classical computer requires *keeping track* of $N = 2^n$ amplitudes... why not use a quantum system to simulate another quantum system efficiently?

Deutsch (1985): formalizes Feynman's idea.

- Defines the **quantum Turing machine**
- Proves the first quantum speedup: the **Deutsch-Jozsa problem** (1992) (determine if $f : \{0,1\}^n \to \{0,1\}$ is constant or balanced in one query vs. $\Omega(2^{n-1})$ classical)

Important: a quantum computer is **not** a massively-parallel classical machine! Exponentially many answers, but you can only observe a single one!

The Quantum Circuit model



H, S, U are called gates. H and S are specific gates, while U is an arbitrary unitary operation

First Algorithms

BB84: Quantum Key Distribution (1984) - Turing Award 2025!

Bennett & Brassard [1]: first quantum *protocol*:

1. Alice encodes random bits in random bases: $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$
2. Bob measures each qubit in a randomly chosen basis
3. **Sifting:** publicly compare bases, keep bits where they agree
4. **Error check:** sample a subset to estimate eavesdropping

Key insight

Any eavesdropper (Eve) must measure the qubits; measuring in the wrong basis disturbs the state and is detectable with high probability.

Security: information-theoretic (unconditional), not computational. The no-cloning theorem + quantum indistinguishability do the work.

Legenda: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is a 1-qubit state (1/2 prob. of being 0 and 1/2 prob. of being 1).

The no-cloning theorem is a fundamental theorem in q.m.: given a state $|\psi\rangle$, it is impossible to copy it!

Simon's Algorithm (1994)

Simon's problem [2]: given $f : \{0,1\}^n \to \{0,1\}^n$ promised to satisfy $f(x) = f(y) \iff x \oplus y \in \{0^n, s\}$ for some hidden $s \in \{0,1\}^n$, find s.

Simon 1994

Simon's algorithm finds s using $O(n)$ quantum queries. Any classical randomized algorithm requires $\Omega(2^{n/2})$ queries.

Quantum strategy:

1. Prepare $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|0\rangle$, query f: $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$
2. Measure second register: collapses to $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$
3. Apply $H^{\otimes n}$: yields y with $y \cdot s \equiv 0 \pmod 2$. Repeat $O(n)$ times.

Key insight

First exponential quantum speedup over classical computation. Directly inspired Shor's algorithm.

Shor's Algorithm (1994)

Shor 1994 [3]

Integer factorization is in BQP. Given N, Shor's algorithm produces a non-trivial factor in time $O(\text{poly}(\log N))$.

Reduction to period finding: given $N = pq$, pick a coprime to N and find the period r of $f(x) = a^x \bmod N$. Then $\gcd(a^{r/2} \pm 1, N)$ gives a factor with high probability.

Quantum Fourier Transform: Extracts the period r using $O(\log^2 N)$ gates.

$$\text{QFT}_N|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$$

Impact: breaks RSA!

Shor's algorithm requires a full fault-tolerant quantum computer, a very large number of qubits and long decoherence times

Grover's Algorithm and the BBBV Lower Bound

Unstructured search: find x^* with $f(x^*) = 1$ among $N = 2^n$ inputs.

Grover 1996 [4]

Grover's algorithm solves unstructured search in $O(\sqrt{N})$ quantum queries. Classical algorithms require $\Theta(N)$ queries.

Grover iterate: $G = D_f \cdot O_f$, where $O_f|x\rangle = (-1)^{f(x)}|x\rangle$. Each application rotates the state by $2\theta \approx 2/\sqrt{N}$ toward $|x^*\rangle$. After $O(\sqrt{N})$ steps the amplitude of $|x^*\rangle$ is ≈ 1.

Bennett-Bernstein-Brassard-Vazirani (BBBV) 1994 [5]

Any quantum algorithm requires $\Omega(\sqrt{N})$ queries for unstructured search.

Key insight

BBBV is the first major quantum lower bound and rules out polynomial-time black-box NP solvers. Only a modest quadratic speedup for NP *brute-force* search.

Complexity Theory

The Quantum Complexity Landscape

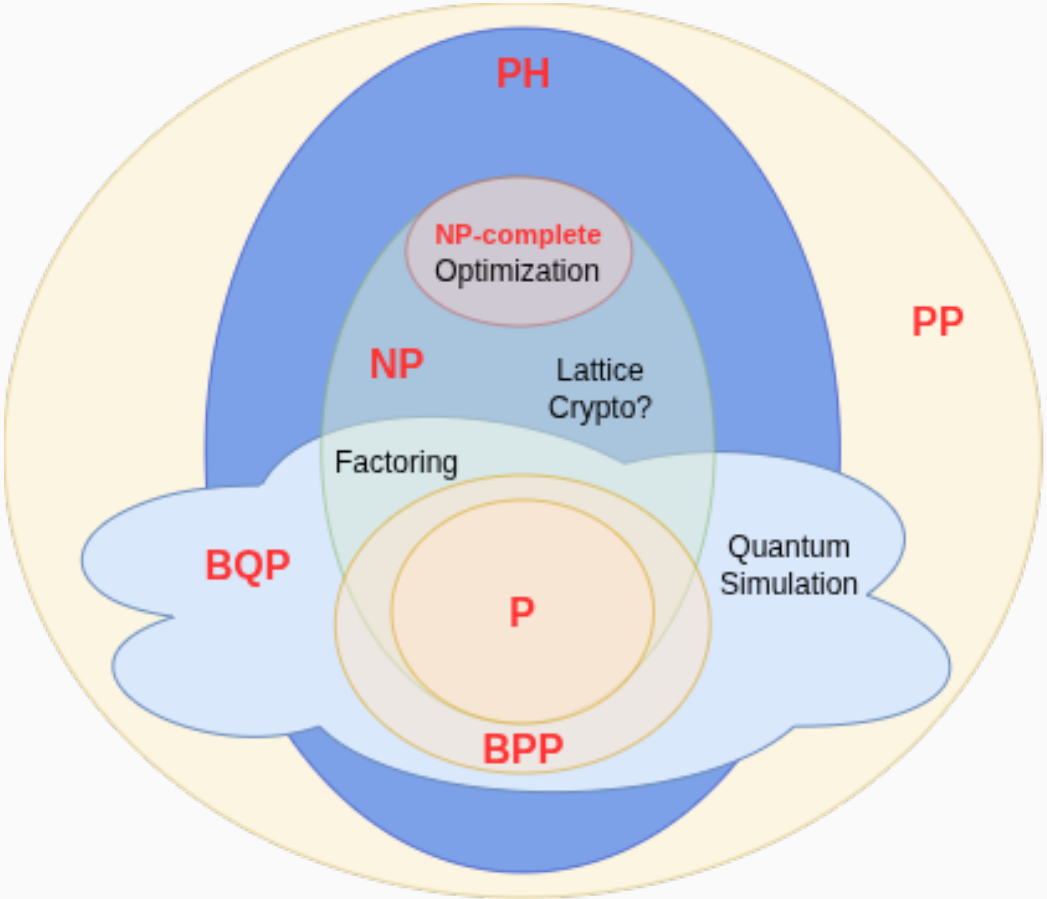
BQP

Bounded-error Quantum Polynomial time: the class of decision problems solvable by a uniform family of polynomial-size quantum circuits with two-sided error. (the analogous of the class BPP)

Known inclusions:

$$\begin{aligned} \mathrm{P} &\subseteq \mathrm{BPP} \\ &\subseteq \mathrm{BQP} \\ &\subseteq \mathrm{PP} \\ &\subseteq \mathrm{PSPACE} \end{aligned}$$

PH (Polynomial hierarchy): alternation of $\exists, \forall, \exists \ldots$ quantifiers over a decision problem



QMA and the k-Local Hamiltonian Problem

QMA

Quantum Merlin-Arthur: the class of decision problems verifiable by a polynomial-time quantum verifier given a *quantum* witness $|\psi\rangle$. The quantum analogue of NP (or more precisely MA).

Known: NP $\subseteq$ QMA $\subseteq$ PP.

k-Local Hamiltonian [6]

Given a k-local Hamiltonian $H = \sum_i H_i$ on n qubits (each H_i acts on at most k qubits) and rationals $a < b$ with $b - a \geq 1/\text{poly}(n)$, deciding whether the ground state energy is $\leq a$ or $\geq b$ is QMA-complete for $k \geq 2$.

This is the quantum Cook-Levin theorem:

- Establishes QMA as natural and robust
- Connects quantum complexity directly to quantum physics (ground states, local interactions)

Solovay-Kitaev and Gottesman-Knill

Solovay-Kitaev $\sim$1995-97 [7]

Any single-qubit unitary U can be approximated to precision ε using $O(\text{polylog}(1/\varepsilon))$ gates from any fixed finite universal gate set.

Consequence: the model is robust: the choice of gate set is irrelevant up to polynomial overhead. That's quantum analogue of universality of AND and NOT.

Gottesman-Knill 1998 [8]

Any quantum circuit consisting solely of Clifford gates $\{H, \text{CNOT}, S\}$ can be simulated on a classical computer in polynomial time.

- Clifford circuits can produce maximal entanglement yet are classically simulable via the **stabilizer formalism**
- The resource for universality is magic (non-Clifford gates, e.g. the T gate)

QIP = PSPACE **(Jain-Ji-Upadhyay-Watrous 2010)**

QIP

Quantum Interactive Proofs: a quantum prover and quantum verifier exchange polynomially many quantum messages. QIP(k) denotes k rounds of interaction.

Known: QIP(1) = QMA, QIP(3) = QIP, IP = PSPACE (Shamir 1992).

QIP = PSPACE, Jain-Ji-Upadhyay-Watrous 2010 [9]

Quantum interactive proof systems are no more powerful than PSPACE, regardless of the number of rounds. Quantum communication between prover and verifier adds no extra power.

The Sampling Paradigm

A Shift in Perspective

Classical paradigm: quantum algorithms for decision/search problems (factoring, search, simulation...).

New question: is there a problem of independent utility that could give a *quantum advantage*? Perhaps through sampling?

Sampling problem

Output a sample from a target distribution $\mathcal{D}$. A *sampler solves* it if its output is ε-close to $\mathcal{D}$ in total variation distance.

- Measuring a quantum circuit's output *is* sampling
- Certain distributions (outputs of quantum circuits) appear classically intractable

Contradiction: an efficient classical sampler for a quantum output distribution would imply $\mathsf{P}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{NP}}$ (Toda's theorem $\implies$ collapse of the PH to the third level!)

BosonSampling

BosonSampling, Aaronson-Arkhipov 2011 [10]: send n single photons through an m-mode linear-optical network.

Theorem

Sampling from the output distribution is classically hard unless PH collapses, because output amplitudes involve the **permanent** (#P-complete!):

$$\Pr[\text{outcome } S] = \frac{|\mathrm{Perm}(U_S)|^2}{s_1! \cdots s_m!}$$

- Drawbacks: the Theorem holds in the case of exactly sampling from the distribution!
- We cannot hope for a perfect machine that *exactly* samples, but only approximately.
- Under certain assumptions, even approximate sampling implies collapse!

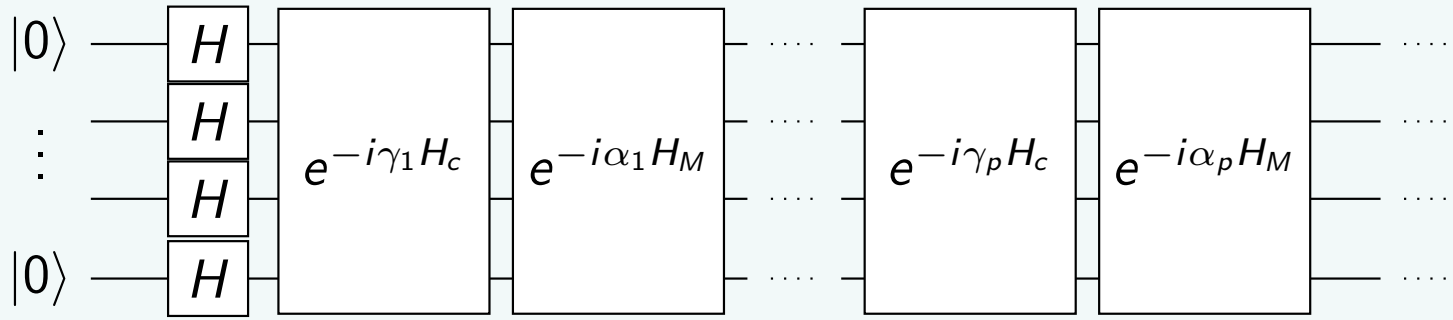
QAOA: Quantum Approximate Optimization (2014)

Setting: combinatorial optimization (e.g. MaxCut, Min-VC) is NP-hard in the worst case. Can a quantum circuit find *good approximate* solutions efficiently?

Inspired by the quantum adiabatic Theorem. No *proven* advantage (yet)

QAOA circuit, Farhi-Goldstone-Gutmann 2014 [11]

Given a cost Hamiltonian H_C encoding the objective function C, a mixer hamiltonian $H_M = \sum_j X_j$, iteratively apply:



Output many samples from the circuit; estimate the average C value; classically optimize the $2p$ parameters (γ, α).

Quantum Machine Learning: Promise and Caveats

The hope: quantum algorithms should speed up expensive linear-algebra subroutines at the heart of many ML methods.

HHL algorithm, Harrow-Hassidim-Lloyd 2009

A system of linear equations $Ax = b$ (with A an $N \times N$ sparse matrix) can be solved in time $O(\kappa^2 \log N/\varepsilon)$ on a quantum computer, where κ is the condition number. Classical algorithms run in $O(N^3)$.

Caveats:

- Many quantum ML speedups rely on quantum RAM (QRAM) for data access;
- **Dequantization (Tang [12]):** with *classical* sample-and-query access to data, classical algorithms match the quantum running time

Challenge: QML algorithms that *cannot* be dequantized must exploit some sampling hardness (like BosonSampling proposal!)
$\rightarrow$ `arxiv:2604.07639`: maybe not in processing time, but QML can yield exponential saving in space!

Forrelation (Aaronson-Ambainis 2015)

Forrelation [13]

Given oracle access to $f, g : \{0,1\}^n \to \{\pm 1\}$, estimate

$$\Phi(f,g) \;=\; \frac{1}{2^{3n/2}} \sum_{x,y \in \{0,1\}^n} f(x)\,(-1)^{x \cdot y}\, g(y).$$

Decide if $\Phi(f,g) \geq 3/5$ or $|\Phi(f,g)| \leq 1/100$.

Quantum algorithm (1 query): prepare $H^{\otimes n}|0\rangle$, apply O_f, apply $H^{\otimes n}$, apply O_g, measure. Interference computes $\Phi(f,g)$ directly.

Aaronson-Ambainis 2015

Any classical randomized algorithm for Forrelation requires $\Omega\left(\sqrt{N}/\log(N)\right)$ queries. Largest known quantum-classical query separation.

Forrelation $\in$ BQP. Is it $\in$ PH?

Recent Frontiers

Raz-Tal: BQP $\not\subset$ PH Relative to a Random Oracle (2019)

Raz-Tal 2019 [14]

There exists an oracle $\mathcal{O}$ (constructed via a random oracle) relative to which $\mathrm{BQP}^{\mathcal{O}} \not\subset \mathrm{PH}^{\mathcal{O}}$. Explicitly: Forrelation $\notin \mathrm{AC}^0$, hence Forrelation $\notin$ PH in the random oracle model.

Proof strategy:

1. Forrelation is in BQP with $O(1)$ queries (Aaronson-Ambainis)
2. AC^0 functions have Fourier mass concentrated on *low-degree* coefficients (Håstad's switching lemma)
3. Forrelation's Fourier weight is concentrated at *high* degree ($\approx \sqrt{2^n}$) $\Rightarrow$ no AC^0 algorithm $\Rightarrow$ Forrelation $\notin$ PH

Key insight

First unconditional (relativized) separation of BQP from the polynomial hierarchy. No hardness assumptions needed: only the Forrelation structure and Fourier analysis!

Random Circuit Sampling and Quantum Supremacy

Random Circuit Sampling (RCS): sample from the output distribution of a pseudo-random quantum circuit on n qubits with d layers.

Hardness argument [15]:

- The output distribution *anti-concentrates*: most outcomes have probability $\approx 1/2^n$
- Approximating the distribution in total variation distance is believed hard (formal reduction to worst-case #P hardness, under average-case conjectures)

Google (Arute et al., 2019) [16]: 53-qubit Sycamore processor. RCS task claimed to take 200 seconds on the device vs. 10^4 years on a classical supercomputer.

Drawbacks:

- Full verification still remains exponential;
- RCS is the current empirical benchmark for quantum advantage.

Proof of Quantumness

Question: can a *classical* verifier certify that an untrusted device is genuinely quantum?

Proof of Quantumness (PoQ)

It is an interactive protocol where a quantum prover *passes* with high probability, while any classical prover *fails* with high probability.

Brakerski-Christiano-Mahadev-Vazirani-Vidick 2018 [17]

A PoQ protocol exists under the hardness of Learning With Errors (LWE), based on *trapdoor claw-free functions*.

- A quantum prover prepares a superposition over a claw and answer correctly the challenge of the verifier
- A classical prover must find a claw, which requires breaking LWE (which is assumed to be hard)
- Adding further messages, allows the verifier to recover *truly random bits*

Yamakawa-Zhandry: Quantum Advantage for an NP Problem (2022)

Prior state of affairs: IQP, BosonSampling, RCS all give *sampling* separations under collapse assumptions. Can we get an advantage for a *search* problem with a *provable* separation?

Yamakawa-Zhandry 2022 [18]

There exists an NP search problem (relative to a random oracle) solvable by a polynomial-time quantum algorithm, yet requiring $\Omega(2^{n/2})$ queries for any classical randomized algorithm.

Construction based on the **NullCodeword** framework.

- **Quantum:** amplitude amplification finds a solution in poly(n) time
- **Classical:** the random oracle hides all structure; $\Omega(2^{n/2})$ queries are necessary

First provable (in the random oracle model) quantum advantage for an NP search problem: $\mathrm{BQP}^{\mathcal{R}} \neq \mathrm{BPP}^{\mathcal{R}}$ relative to a random oracle $\mathcal{R}$.

Quantum Cryptography Without One-Way Functions

Classically: all non-trivial cryptographic primitives require existence of one-way functions (OWFs). If P = NP, OWFs do not exist.

Quantumly: strong cryptographic primitives may exist without OWFs $\implies$ we could live in `Algorithmica`, yet we would still be able to do some sort of quantum cryptography!

Pseudorandom states (PRSs): quantum analogous of PRGs

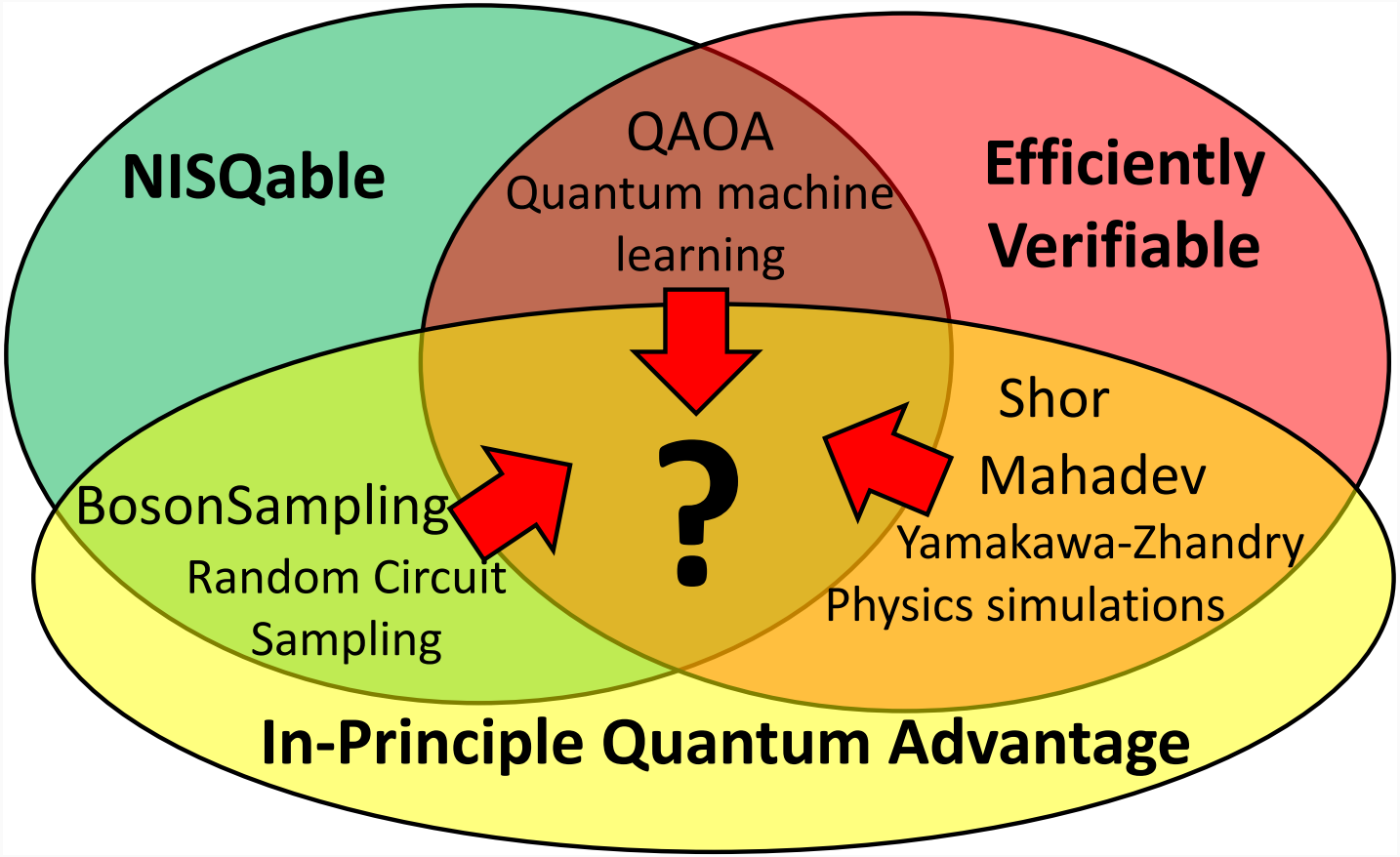
Kretschmer et al 2024 [19]

There exists a classical oracle $\mathcal{O}$ relative to which $\mathrm{P}^{\mathcal{O}} = \mathrm{NP}^{\mathcal{O}}$ yet single-copy PRS exists.

Many quantum cryptographic primitives introduced. Notably

- PRSs are broken by a PP machine.
- EFI are not known to be broken by any classical machine.

The big picture



Some *very recent* proposals for the center: OTOCs, Peaked Circuits, Fermi-Hubbard model

Picture credits: `https://arxiv.org/pdf/2404.14493`

Open Problems

Open Problem 1: BQP **vs.** NP

Is NP $\subseteq$ BQP? Is BQP $\subseteq$ NP? Arguably the main open problem since the beginning. Evidence suggests that they are incomparable.

Open Problem 2/3: Quantum nature + Unitary synthesis

The fact that EFI have no classical way to distinguish them, suggests the need for defining classes with quantum input/output. This has links with the unitary synthesis problem: can any unitary U be implemented with BQP^f where f is an arbitrary Boolean function f?

Open Problem 4: Minimal assumptions for quantum cryptography

Is quantum crypto *strictly weaker* (in terms of assumption) than classical crypto?

My Takeaway

Quantum power

Every result in the past achieving a provable, qualitative separation exploits:

1. **Interference:** probability amplitudes cancel and reinforce in ways inaccessible to any classical probability distribution
2. **Fourier duality:** quantum circuits naturally live in a "dual space"; the QFT is a *change of computational basis*
3. **Sampling & search:** the act of measuring *is* sampling; this should be exploited
4. **Nature:** quantum mechanics have some intrinsic natural properties (no-cloning, entanglement)

My conviction: future quantum algorithms, separations or cryptographic constructions must use at least one of the four previous super powers

Chase problems that exhibit at least one of these 4 flavours!

Conclusions

Thanks!
Questions?

References

[1] C. H. Bennett and G. Brassard, **"Quantum cryptography: Public key distribution and coin tossing,"** *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241.

Bibliography ii

[2] D. R. Simon, **"On the power of quantum computation,"** *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1474–1483, 1997. DOI: 10.1137/S009753979629637. eprint: https://doi.org/10.1137/S009753979629637. [Online]. Available: https://doi.org/10.1137/S009753979629637.

[3] P. Shor, **"Algorithms for quantum computation: Discrete logarithms and factoring,"** in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

Bibliography iii

[4] L. K. Grover, **"A fast quantum mechanical algorithm for database search,"** in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219, ISBN: 0897917855. DOI: 10.1145/237814.237866. [Online]. Available: https://doi.org/10.1145/237814.237866.

[5] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, **"Strengths and weaknesses of quantum computing,"** *SIAM J. Comput.*, vol. 26, no. 5, pp. 1510–1523, Oct. 1997, ISSN: 0097-5397. DOI: 10.1137/S0097539796300933. [Online]. Available: https://doi.org/10.1137/S0097539796300933.

Bibliography iv

[6] J. Kempe, A. Kitaev, and O. Regev, **"The complexity of the local hamiltonian problem,"** *SIAM Journal on Computing*, vol. 35, no. 5, pp. 1070–1097, 2006. DOI: 10.1137/S0097539704445226. eprint: https://doi.org/10.1137/S0097539704445226. [Online]. Available: https://doi.org/10.1137/S0097539704445226.

[7] A. Y. Kitaev, **"Quantum computations: Algorithms and error correction,"** *Russian Mathematical Surveys*, vol. 52, no. 6, p. 1191, Dec. 1997. DOI: 10.1070/RM1997v052n06ABEH002155. [Online]. Available: https://doi.org/10.1070/RM1997v052n06ABEH002155.

[8] D. Gottesman, **The heisenberg representation of quantum computers,** 1998. arXiv: quant-ph/9807006 [quant-ph]. [Online]. Available: https://arxiv.org/abs/quant-ph/9807006.

Bibliography v

[9] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, **"Qip = pspace,"** *J. ACM*, vol. 58, no. 6, Dec. 2011, ISSN: 0004-5411. DOI: 10.1145/2049697.2049704. [Online]. Available: https://doi.org/10.1145/2049697.2049704.

[10] S. Aaronson and A. Arkhipov, **"The computational complexity of linear optics,"** in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, ser. STOC '11, San Jose, California, USA: Association for Computing Machinery, 2011, pp. 333–342, ISBN: 9781450306911. DOI: 10.1145/1993636.1993682. [Online]. Available: https://doi.org/10.1145/1993636.1993682.

[11] E. Farhi, J. Goldstone, and S. Gutmann, **A quantum approximate optimization algorithm,** 2014. arXiv: 1411.4028 [quant-ph]. [Online]. Available: https://arxiv.org/abs/1411.4028.

Bibliography vi

[12] E. Tang, **"A quantum-inspired classical algorithm for recommendation systems,"** in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC '19, ACM, 2019, pp. 217–228. DOI: 10.1145/3313276.3316310. [Online]. Available: http://dx.doi.org/10.1145/3313276.3316310.

[13] S. Aaronson and A. Ambainis, **"Forrelation: A problem that optimally separates quantum from classical computing,"** in *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, ser. STOC '15, Portland, Oregon, USA: Association for Computing Machinery, 2015, pp. 307–316, ISBN: 9781450335362. DOI: 10.1145/2746539.2746547. [Online]. Available: https://doi.org/10.1145/2746539.2746547.

[14] R. Raz and A. Tal, **"Oracle separation of bqp and ph,"** *J. ACM*, vol. 69, no. 4, Aug. 2022, ISSN: 0004-5411. DOI: 10.1145/3530258. [Online]. Available: https://doi.org/10.1145/3530258.

[15] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, **"On the complexity and verification of quantum random circuit sampling,"** *Nature Physics*, vol. 15, no. 2, pp. 159–163, Oct. 2018, ISSN: 1745-2481. DOI: 10.1038/s41567-018-0318-2. [Online]. Available: http://dx.doi.org/10.1038/s41567-018-0318-2.

[16] F. Arute *et al.*, **"Quantum supremacy using a programmable superconducting processor,"** *Nature*, vol. 574, no. 7779, pp. 505–510, 2019. DOI: 10.1038/s41586-019-1666-5. arXiv: 1910.11333 [quant-ph].

Bibliography viii

[17] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, **"A cryptographic test of quantumness and certifiable randomness from a single quantum device,"** *J. ACM*, vol. 68, no. 5, Aug. 2021, ISSN: 0004-5411. DOI: 10.1145/3441309. [Online]. Available: https://doi.org/10.1145/3441309.

[18] T. Yamakawa and M. Zhandry, **"Verifiable quantum advantage without structure,"** *J. ACM*, vol. 71, no. 3, Jun. 2024, ISSN: 0004-5411. DOI: 10.1145/3658665. [Online]. Available: https://doi.org/10.1145/3658665.

Bibliography ix

[19] W. Kretschmer, L. Qian, and A. Tal, **"Quantum-computable one-way functions without one-way functions,"** in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, ser. STOC '25, Prague, Czechia: Association for Computing Machinery, 2025, pp. 189–200, ISBN: 9798400715105. DOI: 10.1145/3717823.3718144. [Online]. Available: https://doi.org/10.1145/3717823.3718144.

Bibliography x

[20] M. J. Bremner, R. Jozsa, and D. J. Shepherd, **"Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy,"** *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 467, no. 2126, pp. 459–472, Aug. 2010, ISSN: 1364-5021. DOI: 10.1098/rspa.2010.0301. eprint: https://royalsocietypublishing.org/rspa/article-pdf/467/2126/459/789839/rspa.2010.0301.pdf. [Online]. Available: https://doi.org/10.1098/rspa.2010.0301.

[21] Z. Ji, Y.-K. Liu, and F. Song, **"Pseudorandom quantum states,"** in *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III*, Santa Barbara, CA, USA: Springer-Verlag, 2018, pp. 126–152, ISBN: 978-3-319-96877-3. DOI: 10.1007/978-3-319-96878-0_5. [Online]. Available: https://doi.org/10.1007/978-3-319-96878-0_5.

Bibliography xii

[22] W. Kretschmer, **"Quantum Pseudorandomness and Classical Complexity,"** in *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, M.-H. Hsieh, Ed., ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 197, Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 2:1–2:20, ISBN: 978-3-95977-198-6. DOI: 10.4230/LIPIcs.TQC.2021.2. [Online]. Available: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.TQC.2021.2.

[23] H. Zhao, A. Zlokapa, H. Neven, *et al.*, **Exponential quantum advantage in processing massive classical data,** 2026. arXiv: 2604.07639 [quant-ph]. [Online]. Available: https://arxiv.org/abs/2604.07639.