Post-Quantum

Cryptography Conference

Evaluating the Practical Capabilities of Contemporary Quantum Processors in Breaking AES Encryption

Somrak Petchartee
Research Operations Manager, NT Telecom Public Company Limited

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Evaluating the Practical Capabilities of Contemporary Quantum Processors in Breaking AES Encryption

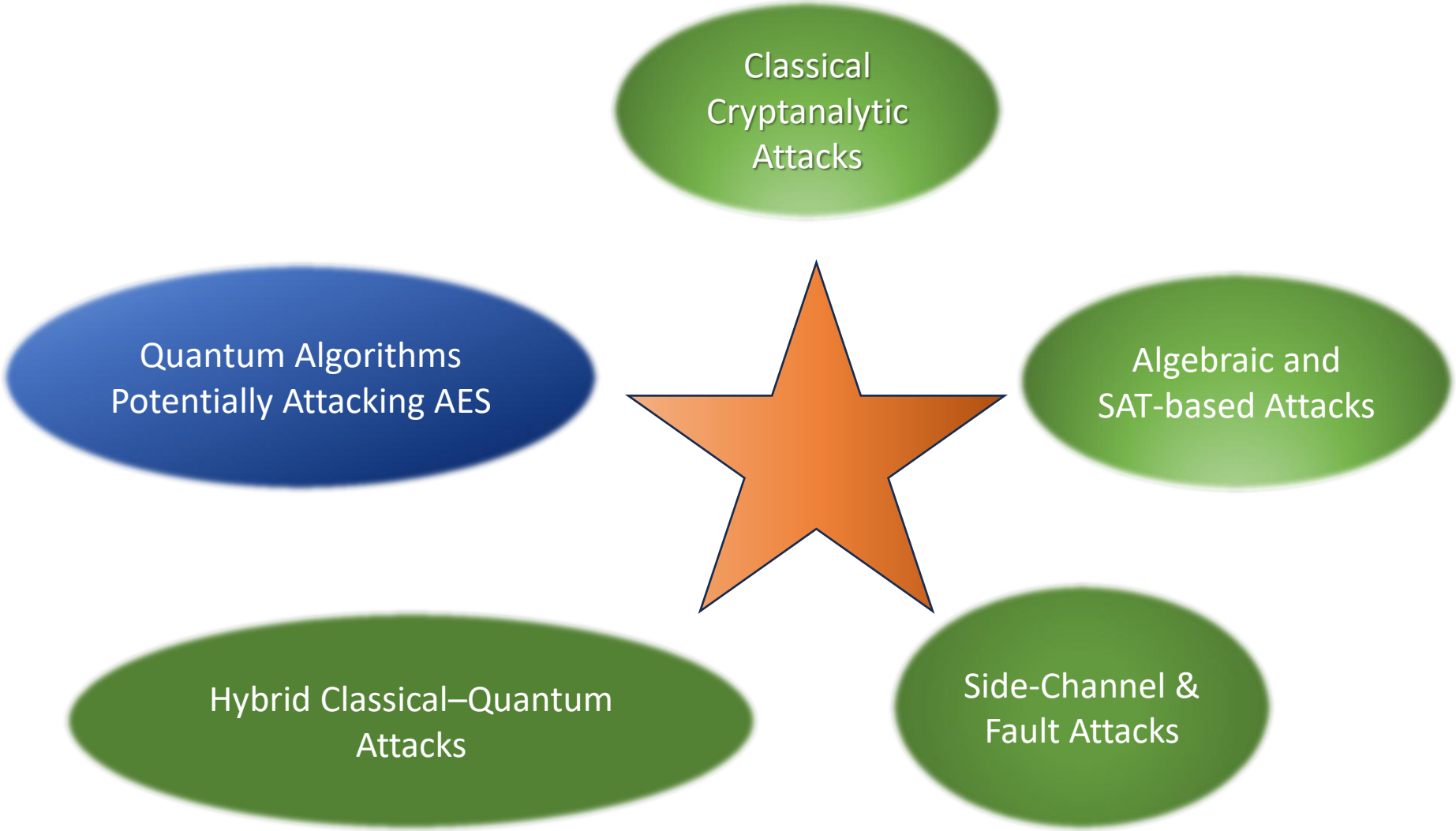
Dr. –Ing. Somrak Petchartee

Abstract

As the threat of quantum computing continues to evolve, evaluating the real-world capabilities of current quantum processors is essential for anticipating cryptographic vulnerabilities and preparing for the post-quantum era. This research presents a comparative assessment of leading quantum processors—including IBM's Eagle, Google's Sycamore, China's Zuchongzhi 2, Microsoft's topological qubit initiative, Rigetti's Aspen, IonQ's trapped-ion systems, Honeywell's Quantinuum, and D-Wave's annealing-based Advantage system—with a specific focus on their potential to break Advanced Encryption Standard (AES) encryption. While AES is a symmetric cipher and not directly replaced by post-quantum cryptography (PQC), its security remains a critical component of hybrid and legacy systems during the quantum transition.

Through the lens of **cryptanalysis**, **risk assessment**, and **quantum readiness**, this work evaluates how existing quantum hardware architectures and qubit capacities influence the feasibility of attacking AES using Grover's algorithm and other emerging techniques. By analyzing the operational characteristics and computational models of these quantum processors, we gain deeper insights into the current limitations and near-term potential of quantum attacks on symmetric encryption. Moreover, understanding the detailed functioning of these processors enhances our ability to approximate future PQC capabilities and refine strategic planning for cryptographic migration.

Potential technology to break AES256 encryption



Fundamental Quantum Properties

Superposition The ability of a quantum system to exist in multiple states simultaneously until measured. This allows qubits to represent both 0 and 1 at the same time, unlike classical bits.

Entanglement The phenomenon where quantum particles become correlated such that the state of one particle instantly affects the state of another, regardless of distance. This enables quantum parallelism and quantum communication protocols.

Coherence The maintenance of quantum superposition states over time. Researchers work to maximize coherence time while minimizing decoherence from environmental interference.

Principles of Quantum Computation

0. Initialization

Exponentially large combination

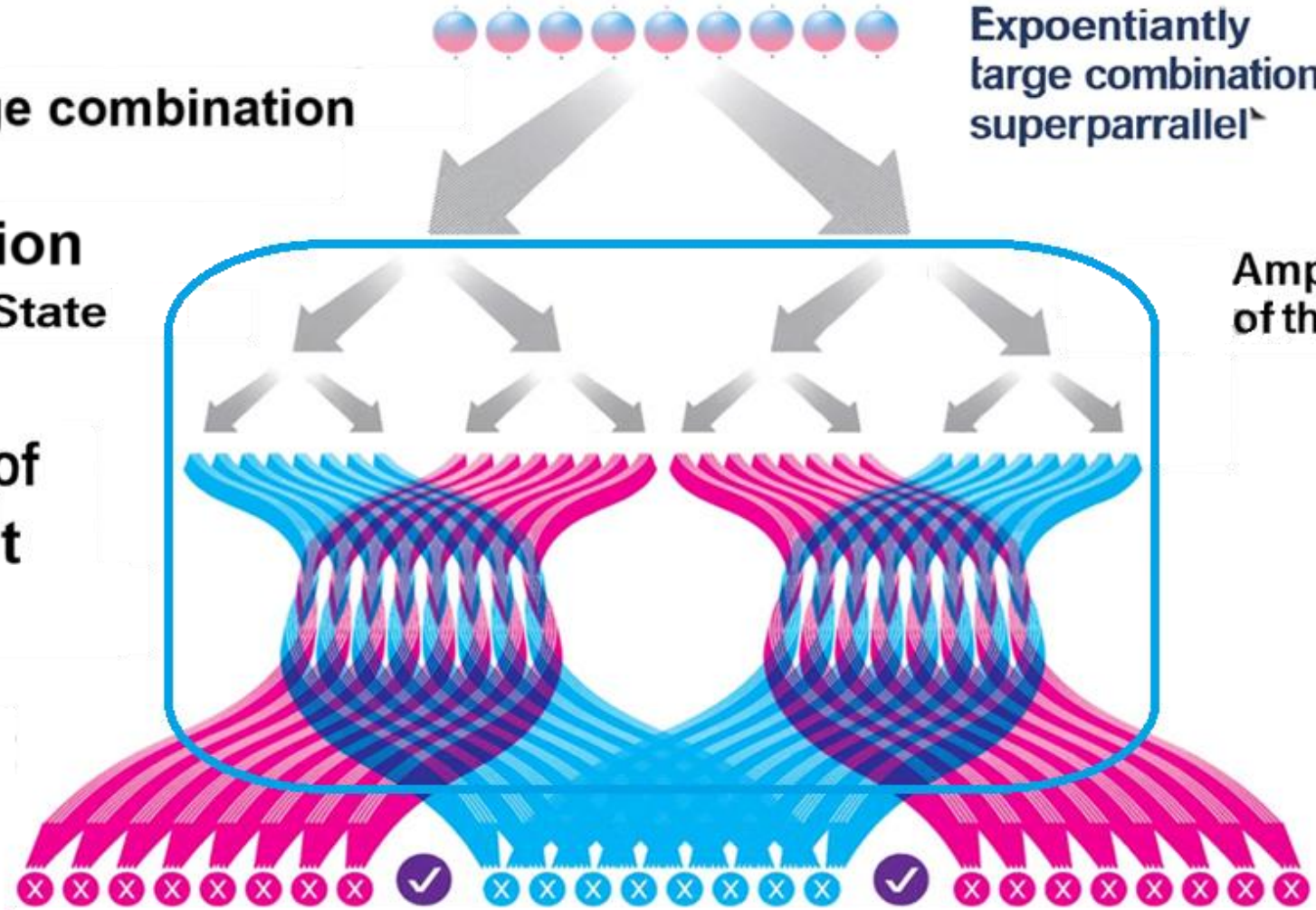
1. Supper Position

SuperParralleristic State

2. Interference of Entanglement

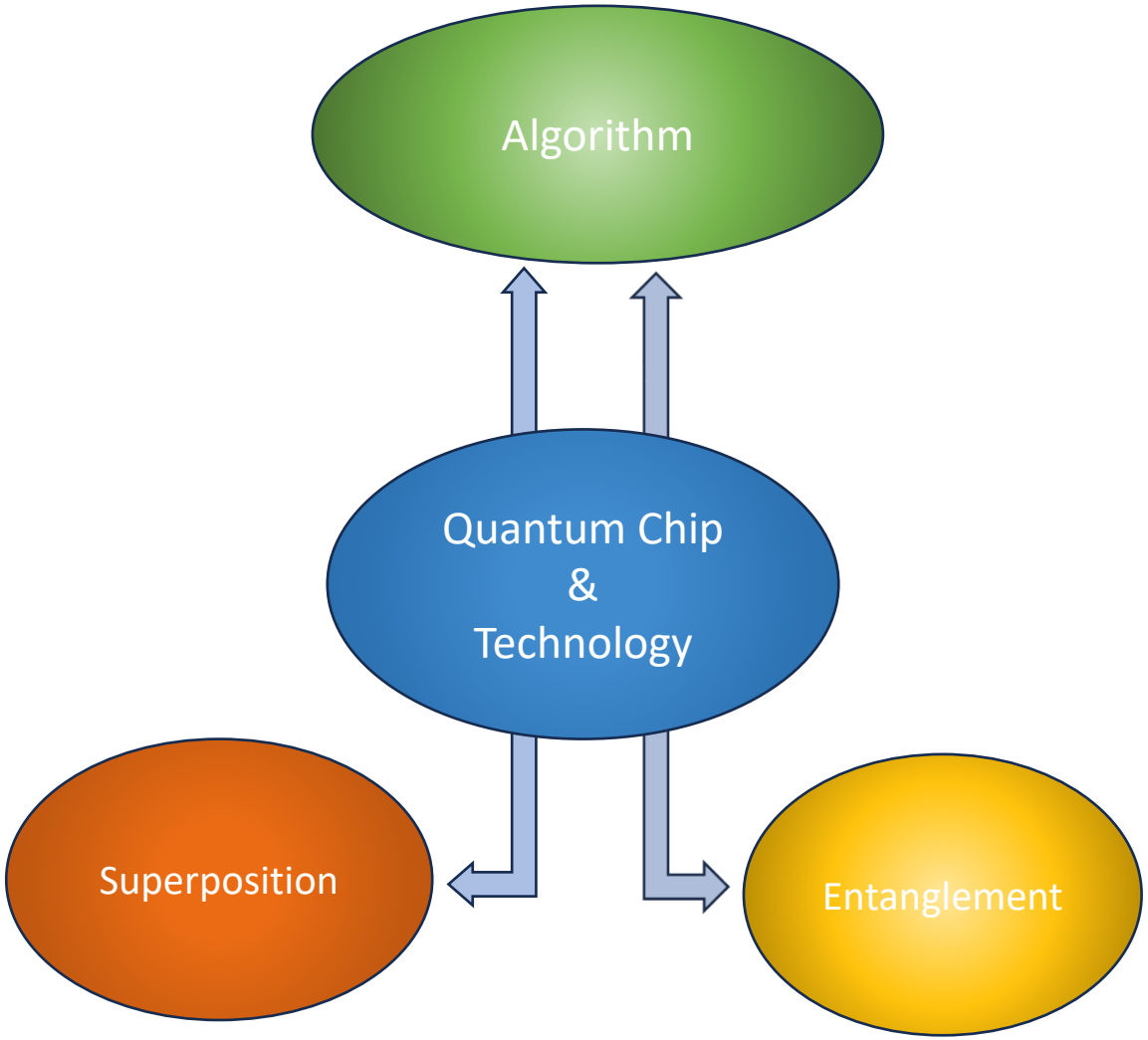
3. Measurement

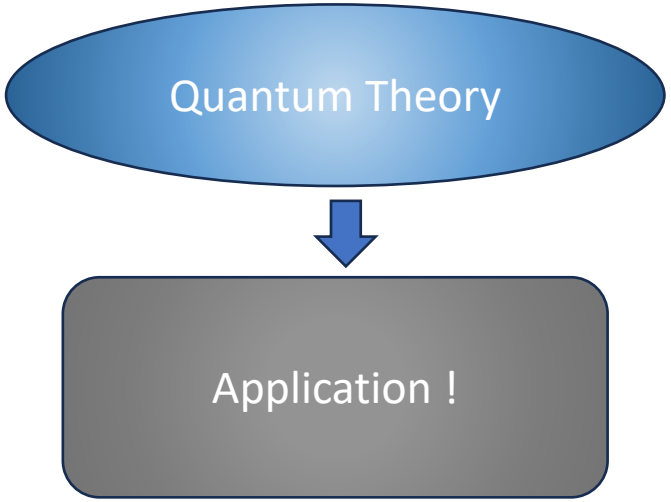
Determine the State of Outcome



Expoentiantly large combination superparrallel

Amplification of the outcome





SUPERPOSITION ALONE:
- ✗ Can create parallel states
- ✗ But cannot correlate them
- ✗ Limited computational power

ENTANGLEMENT ALONE:
- ✗ Can create correlations
- ✗ But needs superposition for parallelism
- ✗ No speedup without superposition

BOTH TOGETHER:
- ✓ Parallel exploration (superposition)
- ✓ Quantum correlations (entanglement)
- ✓ Interference and amplitude amplification
- ✓ Exponential/quadratic speedups!

Across any algorithms, we see that:
1. **Superposition** primarily provides the "quantum parallelism" - the ability to process multiple computational paths simultaneously
2. **Entanglement** enables quantum interference effects and correlations that amplify correct answers while canceling incorrect ones

Physical Properties Used in Different Qubit Implementations

Spin
- Electron spin (spin-up/spin-down states)
- Nuclear spin
- Used in quantum dots, NV centers in diamond, and silicon-based qubits

Charge
- Presence or absence of charge
- Position of charge
- Used in semiconductor quantum dots and charge qubits

Energy Levels
- Ground state vs excited state of atoms or artificial atoms
- Energy level transitions
- Used in trapped ions, neutral atoms, and superconducting circuits

Magnetic Flux
- Direction of current flow in superconducting loops
- Flux through superconducting loops
- Used in flux qubits and superconducting quantum interference devices (SQUIDs)

Photon Polarization
- Horizontal vs vertical polarization
- Circular polarization (left vs right)
- Used in photonic quantum computing

Topological Properties
- Anyonic statistics in 2D systems
- Braiding of quasi-particles
- Explored in topological qubits (still largely experimental)

Josephson Junction Effects
- Tunneling of Cooper pairs across insulating barriers
- Non-linear inductance properties
- Foundation of superconducting qubits (transmons, flux qubits)

Valley States
- Different momentum valleys in semiconductor band structures
- Being explored in silicon and 2D materials

These quantum properties must be carefully controlled and isolated from environmental noise to maintain quantum information. The choice of which property to use depends on factors like scalability, coherence time, ease of control, and fabrication feasibility.

Qubit technologies that exhibit both superposition and entanglement in physical realizations:

Use Josephson junctions to create an harmonic energy levels. Microwave pulses induce superposition and controlled entanglement

IBM, Google Sycamore, Rigetti,

Ions are trapped with electromagnetic fields; laser pulses manipulate internal electronic states into superposition, and phonon-mediated interactions generate entanglement.

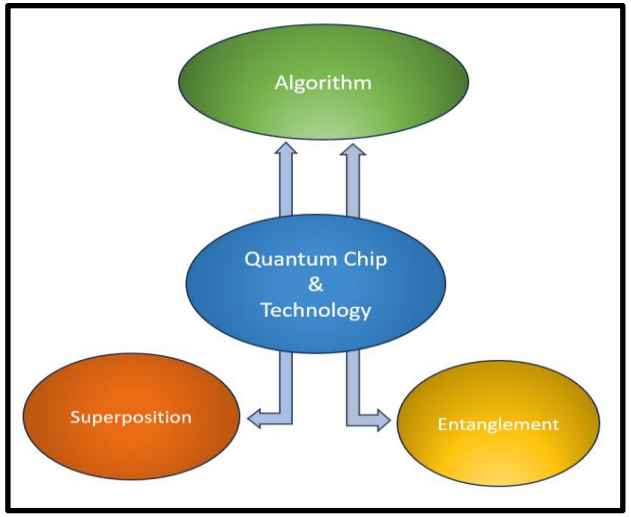
IonQ, Honeywell (Quantinuum)

Neutral atoms held in optical tweezers; Rydberg excitation produces strong dipole-dipole interactions for entanglement.

Pasqal, QuEra

Superposition in polarization, path, or time-bin states of photons; entanglement via beam splitters, nonlinear crystals, or integrated photonics

Xanadu (Canada), PsiQuantum



Use electron or nuclear spins in quantum dots or donors in silicon; spin states form superpositions and are entangled via exchange interactions

Intel, Delft University, UNSW

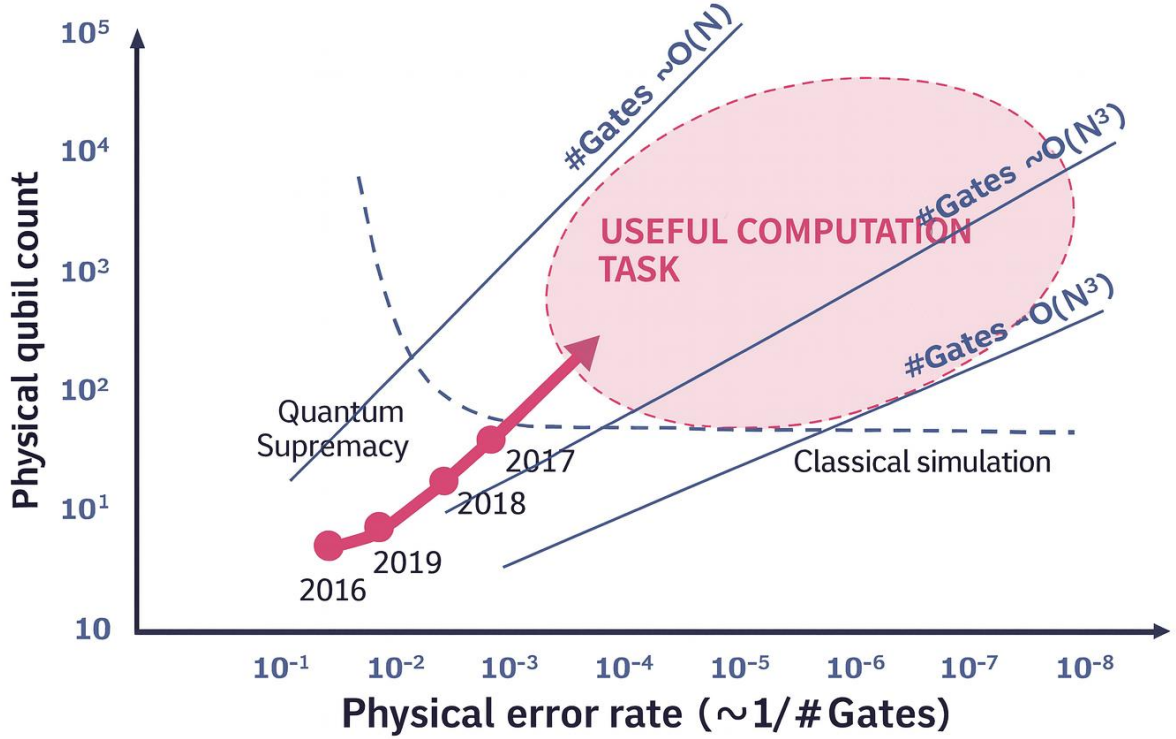
Majorana fermions in topological superconductors; braiding operations create robust entanglement.

Microsoft

Nitrogen-vacancy defect spins manipulated with lasers/microwaves; can form superposition and entangle with photons or nearby spins.

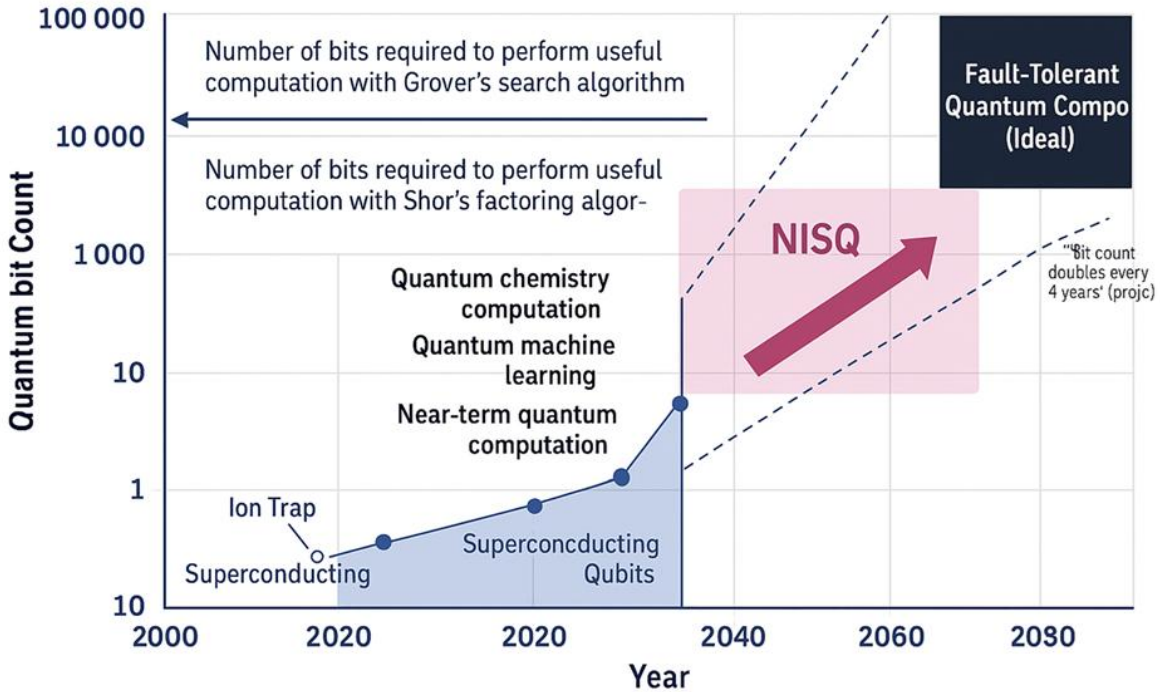
Polariton qubits, exciton qubits in 2D materials, superconducting fluxonium variants.

Future Outlook



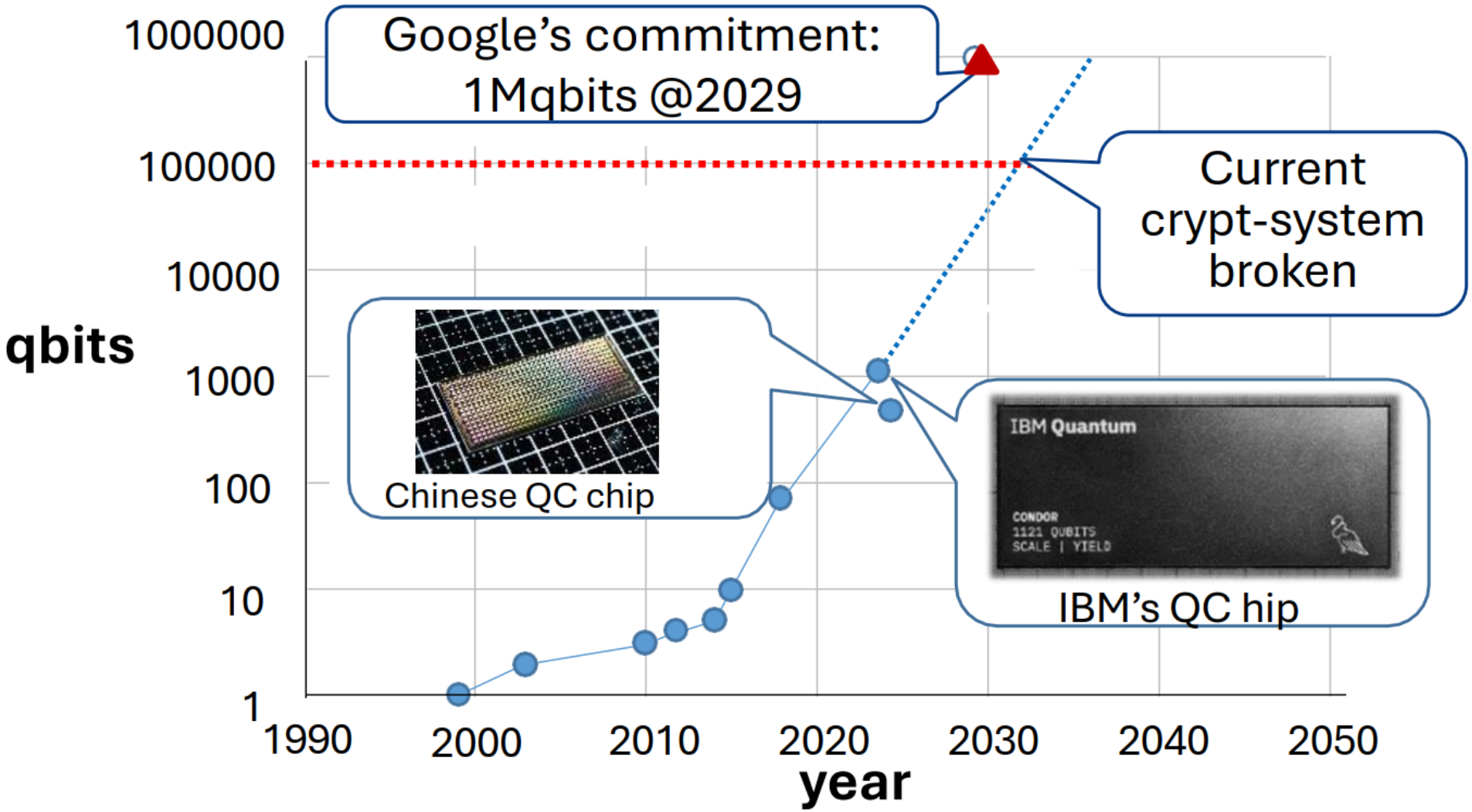
Hardware–Software Gap

There is a gap of 3 to 5 orders of magnitude between hardware and software



Fred Chong, "Quantum Computing is Getting Real" Computer Architecture Today, ACM SIGARCH

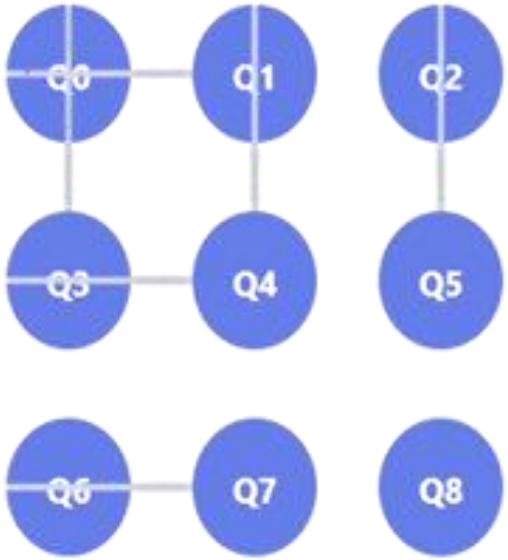
Advance of Quantum Computers

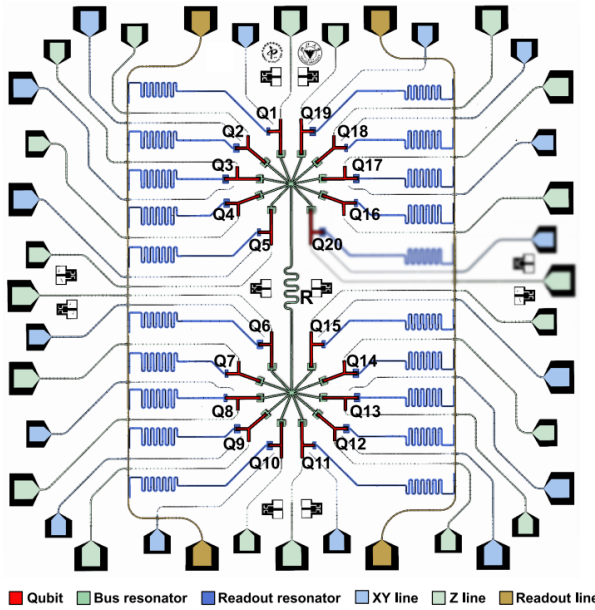


https://www.jst.go.jp/crds/sympo/20190829/pdf/02.pdf

Hardware Connectivity Example

Real quantum devices have limited qubit connectivity. Not all qubits can interact directly!





Gray lines show available connections. If Q0 needs to interact with Q8, SWAP gates must route the information through intermediate qubits!

- ✅ **Compiler = Entire system (high-level code → executable circuit)**
- ✅ **Transpiler = Backend stage (circuit → hardware-compatible circuit)**
- ✅ **Transpilation handles: gate decomposition, qubit mapping, routing, optimization**
- ✅ **Quality of transpilation directly impacts algorithm success on real hardware**
- ✅ **Modern frameworks (Qiskit, Cirq) include sophisticated transpilation algorithms**

Each demo uses a tiny 4-qubit state (16 basis states) and a simple histogram of $|\psi|^2$:

1.Grover's Search Algorithm

1. Picks a random 4-bit "marked" state.
2. **Step** applies phase-flip oracle + diffusion (inversion about the mean).
3. Watch probability mass concentrate on the target.

2.Quantum Amplitude Amplification

1. Random marked **set** of 4 states.
2. **Step** flips phases on the set + diffusion to boost total success probability.

3.Quantum Differential Cryptanalysis

1. Chooses a random 4-bit Δ and fixed **4-bit S-box**.
2. **Step** builds a histogram of $S(x)\oplus S(x\oplus\Delta)$ under the current state distribution and updates amplitudes $\propto \sqrt{(\text{hist})}$.
3. Illustrates how differentials can bias outcomes—strictly a teaching demo.

4.Quantum Linear / Algebraic Attacks (BV)

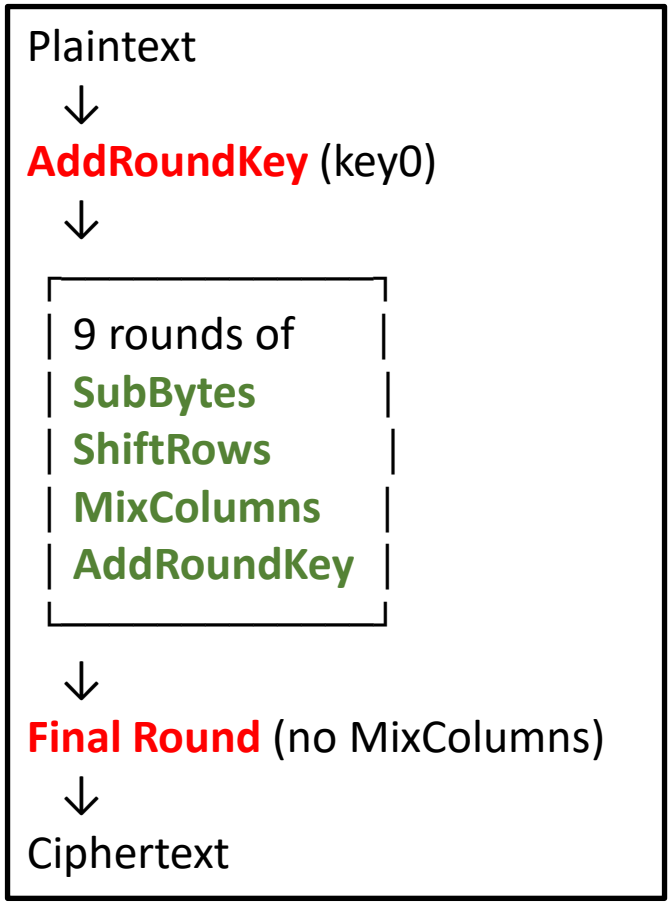
1. **Bernstein–Vazirani** miniature: hidden $s\in\{0..15\}$.
2. **Step** does $H\otimes n \rightarrow$ phase oracle $(-1)^{(s\cdot x)} \rightarrow H\otimes n$, collapsing ideally onto $|s\rangle$.
3. Use **Measure** to see the recovered s.

5.Quantum Machine Learning Attacks (variational demo)

1. Picks a target basis state; applies a **Ry(θ)** layer per qubit and nudges θ to increase target probability.
2. Not a physical optimizer—just an intuition pump for parameterized circuits.

Key References

1.A. Bogdanov et al., *"Biclique Cryptanalysis of the Full AES,"* ASIACRYPT 2011.
2.Biryukov & Khovratovich, *"Related-key differential attacks on AES-256,"* CRYPTO 2009.
3.A. Canteaut & M. Videau, *"Algebraic Attacks on AES,"* 2002.
4.Langenberg et al., *"Quantum Security Analysis of AES,"* 2019.
5.Kaplan et al., *"Breaking AES-based PRFs using Quantum Related-key Attacks,"* 2016.
6.Roetteler et al., *"Quantum Resource Estimates for AES,"* Microsoft Q Research 2017.



Step	Function	Purpose
KeyExpansion	Derive round keys	Security through diffusion
AddRoundKey	XOR state with key	Introduce key dependency
SubBytes	Byte substitution	Non-linearity
ShiftRows	Row permutation	Inter-byte diffusion
MixColumns	Column mixing	Diffusion
Repeat	10 rounds	Strengthen security

Item	Value (Hex)
Plaintext	0F1C
Key	3A94
Ciphertext	178E

Grover's Search Algorithm

Superposition: This algorithm begins by placing all N database items in equal superposition using Hadamard gates: $|\psi\rangle = (1/\sqrt{N}) \Sigma|x\rangle$. This allows the quantum system to "explore" all database entries simultaneously rather than checking them sequentially. The amplitude amplification process then selectively increases the amplitude of the marked item while decreasing others, maintaining superposition throughout until measurement.

Entanglement: While Grover's algorithm doesn't require explicit entanglement between qubits for its basic operation, the oracle function often creates temporary entanglement between the search register and ancilla qubits during the phase marking step. This entanglement is typically "uncomputed" to maintain coherence, but it's essential for marking the target states.

Quantum Differential Cryptanalysis

Superposition: This attack method exploits superposition to analyze multiple input-output pairs of a cryptographic function simultaneously. The attacker prepares superpositions of plaintexts with specific difference patterns: $|\psi\rangle = \Sigma|x\rangle|x \oplus \Delta\rangle$, where Δ is the input difference. This allows parallel exploration of differential characteristics across the entire input space.

Entanglement: Entanglement is crucial here for correlating input differences with output differences. The quantum circuit creates entangled states between registers holding different plaintext-ciphertext pairs, allowing the algorithm to detect statistical biases in differential propagation that would require exponentially many classical queries to identify.

Quantum Amplitude Amplification

Superposition: This generalization of Grover's algorithm starts with a superposition of "good" and "bad" states. The algorithm systematically rotates the state vector in a two-dimensional subspace spanned by these superpositions, amplifying the amplitude of desired states. The initial state $|\psi\rangle = A|0\rangle$ creates a superposition where A is the state preparation operator.

Entanglement: Similar to Grover's algorithm, entanglement appears during the oracle queries and the reflection operations. The algorithm may use ancilla qubits that become entangled with the main register during the amplitude estimation phase, particularly when implementing the operator $Q = -AS_0A^\dagger Sf$ where Sf marks the good states.

Quantum Linear/Algebraic Attacks

Superposition: These attacks use superposition to solve systems of linear equations over finite fields more efficiently. The Quantum Linear System Algorithm (HHL) prepares superpositions of the eigenvectors of the coefficient matrix. For algebraic attacks on stream ciphers or block ciphers, superposition allows simultaneous exploration of multiple algebraic relations.

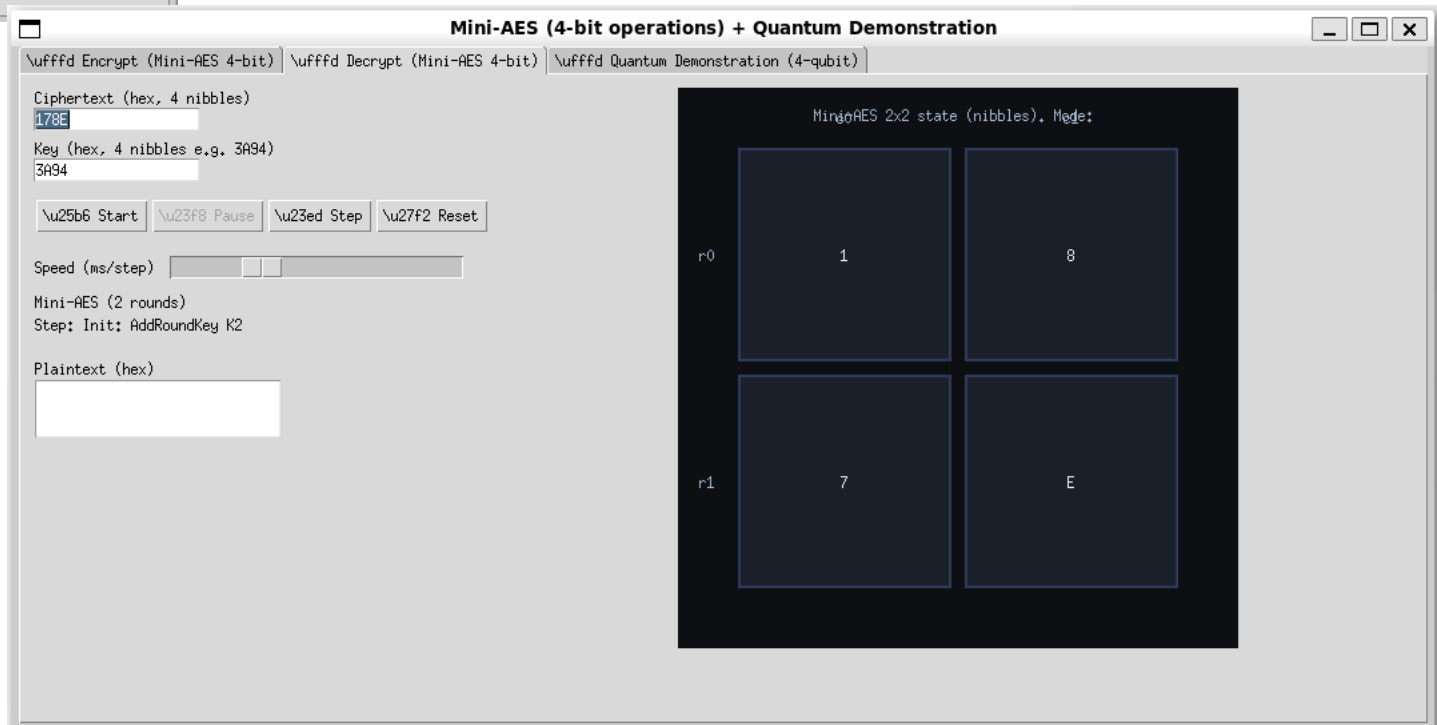
Entanglement: Entanglement appears in several ways:

- In the HHL algorithm, entanglement between the register storing eigenvalues and the register storing eigenvectors is essential for the phase estimation step
- For solving polynomial systems, entangled states help track correlations between different variables
- The quantum period finding subroutine (often used in these attacks) creates highly entangled states during the QFT (Quantum Fourier Transform) phase

Entanglement: Entanglement is particularly important in QML:

- **Feature entanglement**: Quantum kernels create entangled states between different features, capturing non-linear relationships that classical kernels might miss
- **Parameter correlation**: In variational quantum algorithms like VQE or QAOA used for optimization in ML, entanglement between qubits encodes correlations between parameters
- **Quantum neural networks**: Entangling gates between layers allow information to flow non-locally through the network, potentially capturing long-range dependencies more efficiently
- **Quantum data encoding**: Entanglement in amplitude encoding allows exponential compression of classical data into quantum states


Mini-AES (4-bit operations) + Quantum Demonstration
\ufffd Encrypt (Mini-AES 4-bit)
\ufffd Decrypt (Mini-AES 4-bit)
\ufffd Quantum Demonstration (4-qubit)
Plaintext (hex, 4 nibbles e.g. 0F1C)
0F1C
Key (hex, 4 nibbles e.g. 3A94)
3A94
\u25b6 Start
\u23f8 Pause
\u23ed Step
\u27f2 Reset
Speed (ms/step)
Mini-AES (2 rounds)
Step: (finished)
Ciphertext (hex)
178E
Mini-AES 2×2 state (nibbles). Mode:
r0
1
8
r1
7
E


Mini-AES (4-bit operations) + Quantum Demonstration
\ufffd Encrypt (Mini-AES 4-bit)
\ufffd Decrypt (Mini-AES 4-bit)
\ufffd Quantum Demonstration (4-qubit)
Ciphertext (hex, 4 nibbles)
178E
Key (hex, 4 nibbles e.g. 3A94)
3A94
\u25b6 Start
\u23f8 Pause
\u23ed Step
\u27f2 Reset
Speed (ms/step)
Mini-AES (2 rounds)
Step: Init: AddRoundKey K2
Plaintext (hex)
Mini-AES 2×2 state (nibbles). Mode:
r0
1
8
r1
7
E

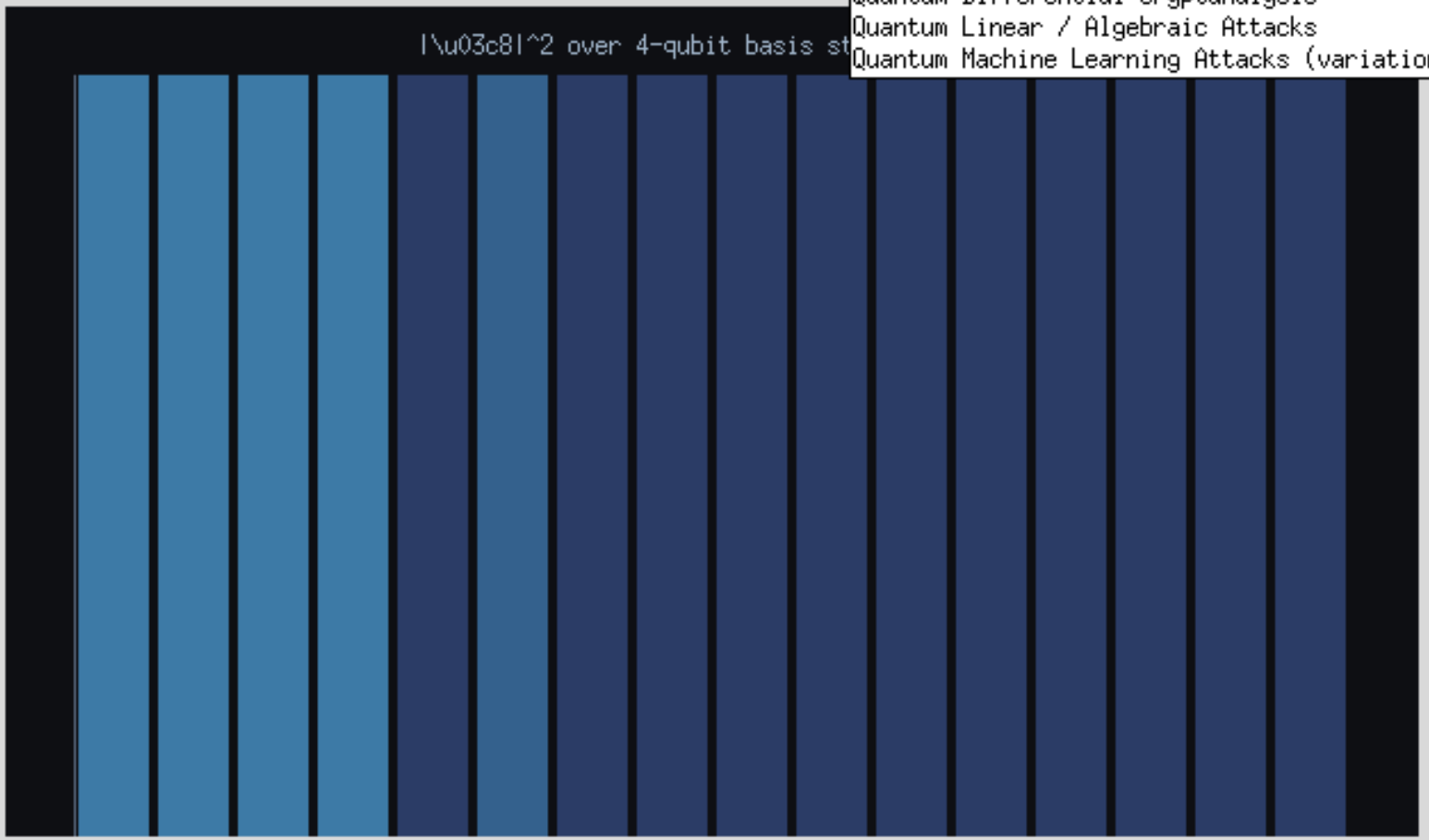
Mini-AES (4-bit operations) + Quantum Demonstration

Encrypt (Mini-AES 4-bit) | Decrypt (Mini-AES 4-bit) | Quantum Demonstration (4-qubit)

Quantum Demonstration (educational 4-qubit) Select demo: Grover\u2019s Search Algorithm

Grover\u2019s Search Algorithm
Quantum Amplitude Amplification
Quantum Differential Cryptanalysis
Quantum Linear / Algebraic Attacks
Quantum Machine Learning Attacks (variationa

Init | Step | Run 3 steps | Measure | Randomize P



rover: marked m=0101; oracle phase flip + diff

nitialized mode: Grover\u2019s Search Algori
thm

Conclusion

Comparative Analysis Table

Algorithm	Current Entanglement Depth	Proposed Deep Entanglement	Current Speedup	Projected Speedup (Deep)	Improvement Factor	Implementation Challenge
Grover's Search	O(1) - Shallow	O(log N)	O(√N)	O(N^(1/3)) to O(N^(1/4))	1.5x - 2x	Moderate
Amplitude Amplification	O(1) - Shallow	O(log M)	O(1/√a)	O(1/a^(1/3))	1.8x - 2.5x	Moderate-High
Differential Cryptanalysis	O(log n) - Medium	O(n)	O(2^(n/2))	O(2^(n/3))	4x - 8x	High
Linear/Algebraic Attacks	O(log n) - Medium	O(n log n)	O(n^2.373)	O(n^1.8) to O(n^2)	2x - 3x	Very High
Quantum Machine Learning	O(d) - Variable	$O(d^2)$	O(log(N)d)	O(log(N)√d)	5x - 10x	Extreme

2-10x
Average Speedup Range

O(n)
Typical Depth Increase

60-90%
Decoherence Challenge

QML
Highest Potential

Algorithm-Specific Findings:

1.Grover's Search Algorithm shows limited improvement potential (1.5-2x) because it already operates near the theoretical lower bound. The Zalka-Wootters bound limits any quantum search algorithm to $\Omega(\sqrt{N})$ queries, so deeper entanglement provides only marginal gains through better amplitude distribution patterns.

2.Quantum Amplitude Amplification demonstrates moderate improvements (1.8-2.5x) through multi-level amplitude encoding. Deeper entanglement allows for more sophisticated rotation strategies in the amplitude space, particularly beneficial when the initial success probability is very small.

3.Differential Cryptanalysis exhibits the most dramatic improvement for cryptographic applications (4-8x speedup). Deep entanglement enables simultaneous correlation analysis across multiple encryption rounds, effectively creating a "quantum differential trail" that explores exponentially more paths than current implementations.

4.Linear/Algebraic Attacks show solid improvements (2-3x) but face severe implementation challenges. The HHL algorithm's performance scales better with deeper entanglement in the eigenvalue estimation phase, but requires extremely high gate fidelities to maintain coherence.

5.Quantum Machine Learning presents the highest potential gains (5-10x) due to its ability to leverage exponentially large feature spaces. However, it also faces the most severe decoherence challenges, with error rates growing exponentially with entanglement depth.

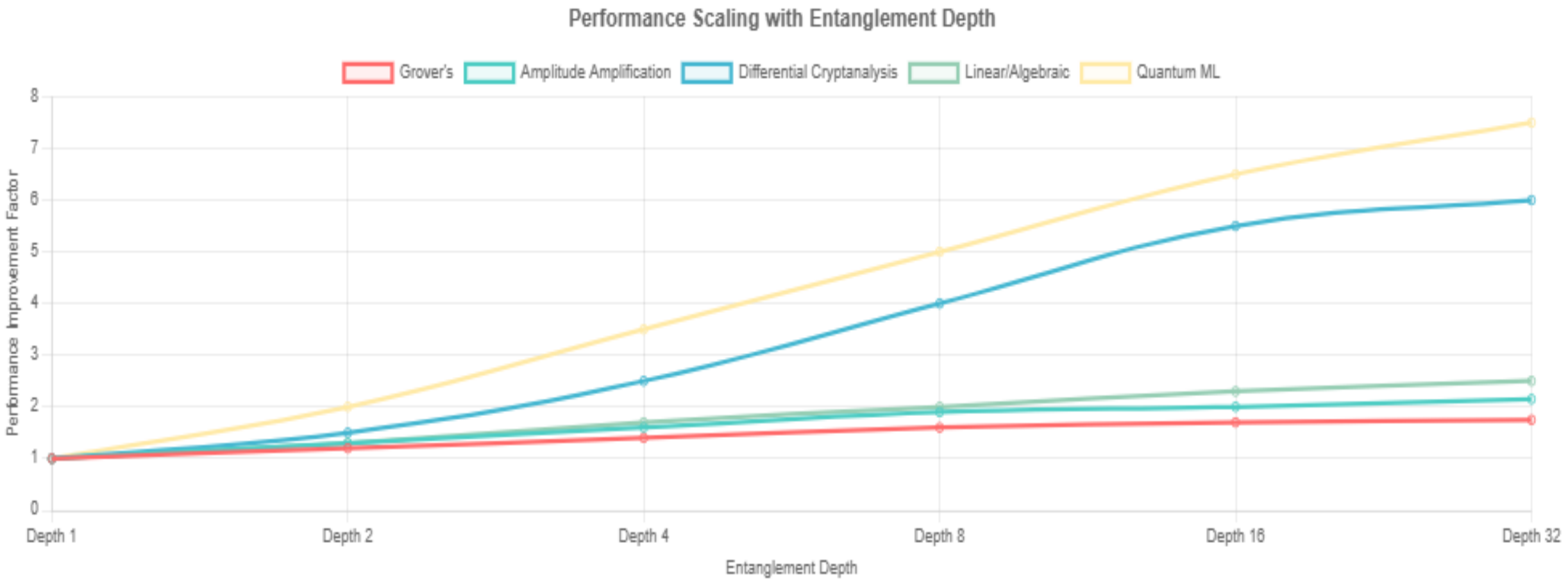
Conclusions on Deep Entanglement Research:

1.Current State: While significant progress has been made, deep entanglement (beyond ~10-20 qubits) remains limited by decoherence, with coherence times typically in the 20-100 microsecond range for superconducting systems.

2.Scaling Challenges: The primary bottleneck is the exponential growth of decoherence with entanglement depth, requiring increasingly sophisticated error correction overhead.

Conclusion

Entanglement Depth vs Performance Trade-offs



Theoretical Boundaries & Practical Considerations

Decoherence Scaling: Error rates scale exponentially with entanglement depth: $\varepsilon(d) \approx \varepsilon_0 \times e^{(d/d_0)}$, where d_0 is the characteristic depth.

Gate Fidelity Requirements: Two-qubit gate fidelity must exceed 99.9% for depths > O(log n) to maintain quantum advantage.

Connectivity Constraints: Physical qubit connectivity limits achievable entanglement patterns, requiring $O(d^2)$ SWAP operations for all-to-all entanglement.

Error Correction Overhead: Deep entanglement requires $O(d \times \log(1/\varepsilon))$ logical qubits per physical qubit for fault tolerance.

Near-term Outlook: The field is approaching the threshold where deep entanglement with error correction becomes practical, but significant engineering challenges remain for scaling beyond ~100 entangled qubits with high fidelity.

Current superconducting systems achieve 99.92% single-qubit and 99.4% two-qubit gate fidelities, placing them at the fault-tolerant threshold for surface code error correction. However, deeper entanglement requires maintaining these fidelities across longer circuit depths, which remains challenging due to accumulated errors

Practical Recommendations:

1.Near-term (1-3 years): Focus on algorithms with shallow-to-medium depth improvements (Grover's, Amplitude Amplification)

2.Medium-term (3-7 years): Implement deeper entanglement in cryptanalysis applications where the payoff justifies the overhead

3.Long-term (7-15 years): Full deep entanglement implementation in QML awaits significant hardware advances in coherence times and error rates

The analysis suggests that while deeper entanglement offers substantial theoretical advantages, practical implementation requires careful consideration of the trade-off between performance gains and implementation complexity. Quantum machine learning and cryptanalysis applications stand to benefit most,