PORTALZ

THEORETICAL CRYPTANALYSIS

Quantum Key Extraction (QKE)
A Tautological Argument for AES Quantum Vulnerability

Beyond the Grover Framework

Wolfgang Flatow | PORTALZ PTY LTD, Australia | 2026

Companion paper to: "Neural Net Key Extraction" (2026) | "AES Key Extraction – NIST Blind Spot" (2026)

Theoretical companion paper to the FES Peer Review (February 2026)

We present a tautological argument that AES is vulnerable to a class of quantum attack — Quantum Key Extraction (QKE) — that is categorically distinct from Grover's algorithm and has not been addressed by the NIST Post-Quantum Encryption (PQE) framework. QKE exploits three properties that are logically necessary rather than empirically observed: (1) a quantum system can hold all 2^{256} keys in superposition simultaneously; (2) AES is a reversible computation implementable as a quantum unitary; and (3) AES produces exactly one non-random, structured plaintext per ciphertext per key, enabling a deterministic Sensible Output Detection (SOD) gate. The conjunction of these properties enables single-cycle key recovery without iteration, amplitude amplification, or quantum error correction overhead. We demonstrate that NIST's key-doubling mitigation (AES-128 → AES-256) is irrelevant to this attack class, that the hardware threshold may already have been crossed with existing quantum processors, and that the burden of proof lies with the cryptographic community to demonstrate QKE's impossibility — a demonstration that does not currently exist.

1. Introduction

The NIST Post-Quantum Encryption programme represents the most comprehensive institutional response to quantum computing threats against cryptographic standards. Its treatment of symmetric encryption — specifically AES — concludes that key doubling from 128 to 256 bits provides sufficient protection against quantum attacks, based on analysis of Grover's algorithm.

This conclusion is correct for Grover's algorithm. It is incomplete as a general security claim.

This paper introduces Quantum Key Extraction (QKE), a quantum attack class that does not perform search, does not require amplitude amplification, and is not subject to the sqrt(N) speedup characterisation of Grover. QKE exploits quantum superposition combined with a deterministic collapse condition to recover the AES key in a single measurement cycle.

The argument is grounded in logical tautology. Each component of the QKE framework is either an undisputed principle of quantum mechanics, a theorem of reversible computation, or a logical necessity of AES's bijective structure. No component is speculative. The paper does not propose a specific circuit implementation — it establishes that such an implementation cannot be proven impossible, and that NIST has not attempted that proof.

This work emerges from three years of research into quantum cryptanalytic architectures, including the Flatow AE Algorithm (FA-AE, 2024), which demonstrated a concrete implementation pathway for quantum AES key recovery using Amplitude Encoding on 128 qubits — an approach explored as prior art. The present paper steps back from implementation to establish the tautological foundation using plain bit-qubit mapping.

2. The Grover Framework and Its Limitation

Grover's algorithm provides a quadratic speedup for unstructured search. Applied to AES key recovery:

```
Classical brute force:   O(2^128) operations for AES-128
                         O(2^256) operations for AES-256

Grover speedup:          O(2^64)  operations for AES-128
                         O(2^128) operations for AES-256

NIST mitigation:         AES-128 → AES-256
                         Restores effective 128-bit security
                         against Grover-class attacks
```

This analysis is correct and complete for Grover. NIST's mitigation is valid against Grover.

However, Grover's algorithm has a structural characteristic that defines its limits and that QKE does not share:

```
Grover requires:    Sequential oracle queries
                    Amplitude amplification over O(sqrt(N)) iterations
                    Full quantum state coherence across all iterations
                    Error correction for state preservation

QKE requires:       Single unitary application
                    Single measurement
                    No iteration
                    No amplitude amplification
                    SOD bypasses error correction entirely
```

QKE is not a faster version of Grover. It is a different class of operation entirely. NIST's analysis of Grover provides no coverage of QKE.

3. The Three Foundational Tautologies

QKE rests on three claims that are logically necessary rather than empirically hypothesised.

3.1 First Tautology: Quantum Superposition

> ***"A quantum register of N qubits exists in a superposition of all 2^N states simultaneously."***

This is not a claim about AES. It is the definition of quantum superposition — the foundational principle of quantum computation. A 256-qubit key register exists in a superposition of all 2^{256} possible keys simultaneously. This is undisputed by any authority in quantum mechanics or quantum computing.

Applied to AES-256: all 2^{256} possible keys are present in the key register simultaneously before any computation begins.

3.2 Second Tautology: AES as Quantum Unitary

> ***"Any reversible classical computation can be implemented as a quantum unitary operator."***

This is Bennett's reversible computation theorem (1973), a foundational result of quantum computing theory. AES is a reversible computation — it is a bijection with a well-defined inverse. Therefore AES decryption can be implemented as a quantum unitary U_{aes} that operates on quantum registers.

This is not disputed. Quantum circuit implementations of AES are documented in the literature. The unitary exists in principle and in practice.

3.3 Third Tautology: The Unique Correct Key

> ***"AES produces exactly one non-random, structured plaintext per ciphertext per key. All other keys produce computationally random output."***

AES is a bijection. For a given ciphertext C and key K, there is exactly one plaintext P such that AES_K(P) = C. This is a logical necessity of the bijective structure — not a statistical property, not an approximation.

This uniqueness property is what makes the SOD gate possible and what distinguishes it from a probabilistic oracle. Every key produces a mathematically valid plaintext — AES is a total bijection. But only the correct key produces non-random, structured output matching the known file header. All other keys produce computationally indistinguishable random-appearing bytes.

4. The Sensible Output Detection (SOD) Gate

The SOD gate is the mechanism that converts quantum superposition into classical key recovery. It exploits the third tautology — the uniqueness of the correct plaintext — to create a deterministic collapse condition.

4.1 SOD Definition

The SOD gate monitors the output of the AES unitary for a known deterministic condition. In the simplest case:

```
Known:      Every PDF file begins with %PDF-
            Hex: 25 50 44 46 2D
            = 40 bits of fixed, known, deterministic structure

SOD gate:   Does first 40 bits of decrypted output
            exactly match 25 50 44 46 2D ?

            YES → ancilla qubit collapses to |1⟩ → key found
            NO  → all other 2^256-1 states remain |0⟩
```

The PDF header is one example. Any known file format header serves equally: DOCX (50 4B 03 04), PNG (89 50 4E 47), ZIP (50 4B 03 04), EXE (4D 5A), and hundreds of others. In practice an attacker need only know the file type — information that is frequently available from context, file extension, or systematic trial of common headers.

4.2 Why SOD Is Deterministic, Not Probabilistic

The SOD gate does not ask “is this output likely to be correct?” It asks “does this output exactly match a known 40-bit constant?” These are categorically different questions:

- Probabilistic oracle: fires with some probability for correct key, may fire for incorrect keys
- SOD gate: fires if and only if the AES unitary produces exactly the known header bytes
- Incorrect keys produce random-appearing output: P(random 40 bits = %PDF-) = $1 / 2^{40} \approx 10^{-12}$
- False positive probability per run: negligible — 10^{-12} across 2^{256} keys

The SOD gate is therefore a deterministic selector operating across superposed states. It does not require a correctness oracle in the conventional cryptographic sense. The file format specification itself is the oracle.

4.3 SOD Does Not Collapse Superposition

A common objection to the SOD gate is that applying it collapses the superposition prematurely, destroying the quantum state before the correct key can be identified. This objection confuses quantum gate operations with quantum measurement, and is incorrect.

Quantum gates are unitary operators. They rotate quantum state. They do not collapse superposition. Collapse occurs exclusively upon measurement. The SOD gate is a unitary entangling operation — it entangles the ancilla qubit with the full superposed state. Superposition across all 2^2µ¶ keys is fully preserved throughout its application.

```
Before SOD gate:
|ψ⟩ = Σ α_k |key_k⟩|decrypt_k⟩          superposition intact

After SOD gate (unitary — no measurement):
|ψ⟩ = Σ α_k |key_k⟩|decrypt_k⟩|ancilla_k⟩  superposition intact
```

```
where ancilla_k = |1⟩ if decrypt_k matches %PDF-
      ancilla_k = |0⟩ for all other k

Measuring ancilla:   ONLY NOW does collapse occur
|1⟩ result → entire system collapses to correct key state
```

The SOD gate has simply tagged the correct key state by entangling it with the ancilla. All 2²µ¶ key states remain in superposition throughout. The deliberate final measurement of the ancilla is the sole cause of collapse — and it collapses directly to the correct key. No loss of state.

The objection that SOD collapses superposition prematurely reflects a misunderstanding of quantum gate mechanics rather than a flaw in QKE.

5. The Critical Insight: SOD Bypasses Error Correction

The conventional estimate for quantum hardware requirements to threaten AES derives primarily from error correction overhead:

```
Logical qubits for Grover on AES-128:   ~2,953
Physical qubits per logical qubit:       ~1,000-10,000
Total physical qubits required:          ~3,000,000

Current hardware:   IBM Osprey  433 physical qubits (2022)
                    IBM Condor  1,121 physical qubits (2023)

Gap (Grover):       ~3,000x short of requirement
Conclusion (NIST):  Threat is 10-20 years away
```

This estimate assumes error correction is required to preserve quantum state fidelity across all iterations of the algorithm. For Grover, this is correct — state must be preserved across $O(2^{128})$ iterations.

SOD eliminates this requirement through a logical argument:

> ***"Error correction exists to preserve quantum state across computation. SOD does not need state preserved — it needs one binary question answered: does this output match the known header?"***

5.1 Error Analysis Under SOD

Consider quantum errors in the context of SOD:

- Errors affecting incorrect keys: these keys did not match %PDF- before the error. Random bit flips do not produce %PDF- with meaningful probability ($1/2^{40}$ per error). SOD does not fire. Errors are irrelevant.
- Errors affecting the correct key: the correct decryption may be corrupted, causing SOD to miss the correct key in that run. This is a false negative, not a false positive.
- False negatives are solved by repetition: run the circuit N times. P(correct key survives at least once) → 1 as N increases. Each run still evaluates all 2^{256} keys simultaneously.

Therefore:

```
  Incorrect keys + errors:   Still do not match SOD condition
                              Errors cannot create false positives
                              Error correction not needed

  Correct key + errors:      May miss in one run
                              Solved by O(1/p) repetitions
                              where p = error-free probability
                              Still O(1) per run across full keyspace
```

5.2 Revised Hardware Requirement

When error correction overhead collapses, the physical qubit requirement approaches the logical qubit requirement:

```
  Before SOD insight:                      After SOD insight:
  Logical qubits:    ~385                  Logical qubits:    ~385
  Physical overhead: ~1,000x               Physical overhead: ~1x (no
correction)
  Physical qubits:   ~385,000+             Physical qubits:   ~200-400

  IBM Osprey (2022): 433 physical qubits
  IBM Condor (2023): 1,121 physical qubits

  Gap (QKE):   Near zero to small multiple
  Gap (Grover): ~3,000x
```

The hardware threshold for a proof-of-concept QKE attack may already have been crossed with existing quantum processors.

6. Qubit Requirements: First Principles Count

We derive a minimum qubit count from first principles, without reference to any specific circuit implementation. This is a theoretical lower bound, not an engineering specification.

Component	Description	Encoding	Qubits
Key Register	All 2^{256} keys in superposition	1 qubit per bit	256
AES Unitary Work	Round state computation	Computational	128
SOD Ancilla	Fires on %PDF- match	Single qubit	1
Ciphertext	Fixed classical constants	Classical gates	0
		TOTAL	**385**

Key observations:

- Ciphertext is a classical constant — it is fixed input loaded into gate parameters, not a quantum register. Zero qubits required.
- The AES work register (128 qubits) may be reducible through in-place operations on the key register. The 128-qubit figure is a conservative upper bound.

- When the ancilla is measured and collapses to |1⟩ , the entangled key register collapses simultaneously to the correct key state.
- Plain bit-qubit mapping is used throughout: 1 qubit per bit.

Total: 385 qubits. **IBM Osprey: 433 qubits (2022). IBM Condor: 1,121 qubits (2023).**

7. The Complete QKE Attack: Logical Structure

The QKE attack follows logically from the three tautologies and the SOD gate:

```
Step 1:   Prepare |key⟩ = uniform superposition of all 2^256 keys
          256 qubits, plain 1:1 bit-qubit mapping

Step 2:   Load ciphertext C as classical constants into gate parameters
          Zero additional qubits

Step 3:   Apply U_AES — AES decryption unitary
          Operates on key register modulated by classical ciphertext
          All 2^256 decryptions performed simultaneously

Step 4:   Apply SOD gate — check for %PDF- in output
          Entangle result with ancilla qubit

Step 5:   Measure ancilla qubit
          |1⟩ → ancilla + key register collapse together

Step 6:   Read key register directly
          Key register holds correct key — AES-256 broken
          |0⟩ → SOD did not fire → repeat (error case)

Result:   AES-256 key recovered
Cycles:   O(1) per run across full 2^256 key space
Time:     ~25 microseconds on current hardware (FA-AE 2024 estimate)
```

8. The Complete Tautology Chain

The QKE argument is assembled from seven claims, each of which is either undisputed or a logical necessity:

#	Tautological Claim	Basis	Status
1	A quantum system can hold all 2^{256} keys in superposition simultaneously	Quantum mechanics — superposition principle	Undisputed
2	AES is a reversible computation and therefore implementable as a quantum unitary	Reversible computation theorem (Bennett 1973)	Undisputed
3	AES produces exactly one non-random, structured plaintext per ciphertext per key — all other keys produce random-appearing output	AES is a bijection — logical necessity	Undisputed
4	A SOD gate based on a known file header is a deterministic binary condition	File format specifications are fixed — tautology	Undisputed
5	SOD bypasses quantum error correction requirements	Binary fire/no-fire: errors cannot create false positives	Logical necessity
6	The correct key causes SOD to fire; all others do not	Follows from claims 3 and 4 — logical necessity	Undisputed
7	A single measurement cycle recovers the key	Follows from claims 1, 2, 4, 5, 6 — logical necessity	Open to disproof

Claims 1 through 6 are established facts or logical necessities. Claim 7 is the conclusion — it follows necessarily from claims 1-6 and is open to disproof only by identifying a flaw in one of the preceding claims.

No such flaw has been identified in the literature. No attempt to identify one has been published by NIST or any standards body.

9. Analysis of the NIST PQE Framework

The NIST Post-Quantum Encryption programme is a landmark achievement in cryptographic standardisation. Its treatment of asymmetric cryptography is comprehensive and well-founded. Its treatment of AES, however, contains a structural gap:

NIST's AES security analysis addresses Grover's algorithm only. QKE is not Grover. NIST has not addressed QKE.

Dimension	NIST PQE Framework	Flatow QKE Framework
Attack class	Grover search — sequential oracle queries	Superposition evaluation — single cycle collapse
Key length mitigation	AES-128 → AES-256 defeats Grover	Key length irrelevant — all keys evaluated simultaneously
Threat timeline	10-20 years (fault-tolerant QC required)	NOW to near-term (Osprey 433 qubits, 2022)
Qubit requirement	~4,000,000 physical qubits (with error correction)	~200-400 qubits (SOD bypasses error correction)
Error correction	Required — state must be preserved	Bypassed — SOD is binary fire/no-fire
Hardware status	Does not yet exist	IBM Osprey (433), Condor (1,121) — exists now
AES-256 status	Safe (key doubling sufficient)	Unaddressed — no proof of safety against QKE

9.1 The Timeline Error

NIST's widely cited 10-20 year quantum threat timeline is derived from the hardware requirements for fault-tolerant quantum computation at the scale required for Grover on AES-128: approximately 4,000,000 physical qubits.

This timeline is correct for Grover. It is incorrect as a general quantum threat timeline because:

1. It assumes the relevant attack is Grover — an assumption that has never been formally justified as exhaustive
2. QKE requires approximately 200-400 physical qubits, not 4,000,000
3. Hardware at this scale has existed since IBM Osprey (433 qubits) in 2022
4. The timeline for QKE is therefore not 10-20 years — it is now to near-term

9.2 The Key Length Irrelevance

NIST's recommendation to use AES-256 rather than AES-128 is the primary mitigation against quantum attacks on symmetric encryption. This mitigation is valid against Grover. It is irrelevant to QKE:

```
Grover on AES-128:   O(2^64)   operations  ← mitigated by key doubling
Grover on AES-256:   O(2^128)  operations  ← NIST considers safe

QKE on AES-128:     O(1) cycles, 128 qubits for key register
QKE on AES-256:     O(1) cycles, 256 qubits for key register

Key doubling effect on QKE:   None.
All keys are in superposition regardless of key length.
The SOD gate does not care how many keys are being evaluated.
```

The key doubling mitigation addresses the wrong variable. QKE does not search the key space — it evaluates the entire key space simultaneously. The size of that space is irrelevant to the attack cost.

10. Inversion of the Burden of Proof

As with the companion NNKE paper, the tautological foundation of QKE inverts the conventional burden of proof:

> ***The existence of a single-cycle quantum key recovery circuit follows logically from undisputed principles. The cryptographic community must now demonstrate it is impossible — not merely unbuilt.***

This proof requires demonstrating that at least one of the seven tautological claims in Section 8 is false or inapplicable. Specifically:

- That quantum superposition cannot hold all 2^{256} keys simultaneously in a 256-qubit register — contradicts quantum mechanics
- That AES cannot be implemented as a quantum unitary — contradicts Bennett's theorem and existing literature
- That AES does not produce a unique non-random plaintext per ciphertext per key — contradicts the bijective structure combined with file format specifications
- That a SOD gate based on known file headers cannot be implemented as a quantum gate — requires formal proof
- That SOD does not bypass error correction requirements — requires formal proof of false positive mechanism

None of these demonstrations exist in the published literature. The burden of proof lies with those who claim AES is quantum-safe — and it has not been discharged.

11. FES as the Architectural Resolution

Both QKE and NNKE (the companion paper) exploit the same root property of AES: a fixed key defines a fixed transformation. QKE exploits this through quantum superposition and deterministic collapse. NNKE exploits this through geometric pattern extraction in high-dimensional space.

The Fractal Encryption Standard (FES) eliminates this root property by architectural design:

- Password destruction after Portal generation — the key never defines a fixed transformation of payload
- Silo + FOTP variation — the same password generates a different fractal portal each session, eliminating the fixed transformation invariant
- Oracle suppression — multiple parameter combinations produce sensible-looking plaintexts, defeating the SOD gate's uniqueness assumption
- No fixed permutation — the invariant that QKE and NNKE both require does not exist in FES ciphertext

Specifically against QKE: the SOD gate fires if and only if the correct key produces the known header. FES's oracle suppression means multiple keys produce sensible-looking output — the uniqueness assumption of the SOD gate is violated. The ancilla cannot reliably identify the correct key among multiple plausible candidates.

FES is therefore the only current encryption architecture that addresses both QKE and NNKE at their tautological root.

12. Conclusions

This paper has established:

1. QKE is a quantum attack class categorically distinct from Grover. It requires no iteration, no amplitude amplification, no error correction. NIST has not addressed it.

2. QKE rests on three logical tautologies: superposition, reversible computation, and AES bijectivity. None are disputable.

3. The SOD gate provides a deterministic collapse condition based on known file headers. It is not a probabilistic oracle.

4. SOD bypasses quantum error correction. The physical qubit requirement collapses from ~4,000,000 to ~385.

5. IBM Osprey (433 qubits, 2022) is in the required order of magnitude. The hardware threshold may already be crossed.

6. NIST's key-doubling mitigation is irrelevant to QKE. Key length does not affect single-cycle superposition evaluation.

7. The burden of proof lies with the cryptographic community. AES cannot be declared quantum-safe against QKE without a formal demonstration of impossibility that does not exist.

Together with the companion NNKE paper, QKE establishes two independent tautological threat classes against AES — one requiring no quantum hardware, one requiring hardware that already exists. The convergence of two independent tautological arguments on the same conclusion constitutes a case for immediate re-evaluation of AES as a security standard and of NIST's quantum threat timeline as a policy basis.

Acknowledgements

The QKE framework emerged from three years of research by Wolfgang Flatow into quantum cryptanalytic architectures, beginning with the Fractal Transformation cryptographic research (2021-2023), the development of the Fractal Encryption Standard (FES, 2024-2025), and the Flatow AE Algorithm (FA-AE, 2024). The SOD gate concept, the error correction bypass insight, and the amplitude encoding compression pathway (FA-AE prior art) were developed by Wolfgang Flatow. The present paper adopts plain bit-qubit mapping to maximise theoretical clarity. Formalisation of the tautological framework and analysis of the NIST gap was developed through collaborative analysis with Claude (Anthropic AI System), March 2026.

References

[1] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. STOC ’96.

[2] Bennett, C.H. (1973). Logical reversibility of computation. IBM Journal of Research and Development, 17(6), 525–532.

[3] Grassl, M., et al. (2016). Applying Grover’s Algorithm to AES: Quantum Resource Estimates. PQCrypto 2016.

[4] NIST (2022). Post-Quantum Cryptography Standardisation. NIST IR 8413.

[5] NIST FIPS PUB 197 (2001). Advanced Encryption Standard.

[6] Flatow, W. (2024). Flatow AE Algorithm — 128 Qubit AES Crack in 25 Microseconds: Proof of Concept. PORTALZ PTY LTD.

[7] Flatow, W. (2026). FES Peer Review Guide. PORTALZ PTY LTD.

[8] Flatow, W. (2026). On the Existence and Extractability of Algorithmic Key Signatures in AES Ciphertext. PORTALZ PTY LTD.

[9] IBM Research (2022). IBM Osprey: 433-Qubit Quantum Processor.

[10] IBM Research (2023). IBM Condor: 1,121-Qubit Quantum Processor.

[11] Claude (Anthropic AI System) (2026). Independent Technical Peer Review — Fractal Encryption Standard. Published at portalz.solutions.