

THE GROVER TUNNEL

The Dangers of Ignoring Other Attacks

A National-Security Briefing

Revised September 2026 — Current-status review



Concept illustration: the Grover Tunnel as a narrow field of view onto a much larger quantum landscape.

**The central question is not when we can run Grover against AES.
It is what quantum computation can do to AES outside the Grover model.**

by Wolfgang Flatow

wolfgang.flatow@portalz.solutions

Contents

Executive Proposition.....	3
1. The Classical Security Proposition	3
2. The Computational Boundary Changes	3
3. The Grover Tunnel	3
4. Outside the Tunnel: Quantum Key Extraction.....	4
5. The Quantum-Safe Symmetric Encryption Problem	4
6. Cryptographic Volume: The Payload Is the Mass	4
7. The NIST PQC Asymmetry.....	6
8. Key Exchange Under the QKE Threat Model	6
9. The Missing Symmetric Off-Ramp	6
10. Historical Data: The First Clock.....	7
11. Global Scope.....	8
12. Current Quantum Evidence: What Has Actually Changed.....	8
13. The Adversary and Disclosure Problem	9
14. The National-Security Question	9
15. Conclusion	9
Reference Trail — Current Status, September 2026	10
Interpretive Status of QKE	10
Quantitative Note on the Supplied Graph.....	11
Why This Briefing Is Coming From Portalz	11

Executive Proposition

The quantum threat to symmetric cryptography has become institutionally organised around Grover's algorithm. That is the Grover Tunnel: one known quantum attack model becomes the practical boundary of the threat discussion.

Grover is important. NIST's public material continues to use Grover-style key search as the principal reference model for the quantum impact on symmetric cryptography. NIST currently states that applications may continue to use AES-128, AES-192 and AES-256, while noting that this position assumes no new cryptographic weaknesses are found. [1][2]

The larger national-security question is different: what else can quantum computation do with the key-space and the encryption process? This briefing calls the threat space outside the Grover model - Quantum Key Extraction (QKE). QKE is a threat model and objective, not a demonstrated public algorithm.

The strategic asymmetry is now clear. NIST has a mature public-key PQC migration programme: ML-KEM for key establishment and ML-DSA/SLH-DSA for signatures. Symmetric payload encryption remains on a different track. AES remains a core NIST standard, and in 2026 NIST is even developing a wider Rijndael-256/AES-family variant as a complement to the existing AES algorithms rather than as their replacement. [3][4][5]

**This briefing therefore treats the issue as a threat-model question:
NIST PQC materially addresses quantum-vulnerable public-key cryptography, but it does not constitute a replacement programme for AES as the bulk symmetric payload-encryption architecture.**

1. The Classical Security Proposition

AES was designed for a classical computational environment in which the practical security proposition is the computational inaccessibility of the key-space. AES-128 has 2^{128} possible keys; AES-192 has 2^{192} ; AES-256 has 2^{256} .

Increasing key size and rounds strengthens the existing keyed-block-cipher architecture. It does not replace that architecture. The classical proposition is straightforward: make the search space too large to search.

The quantum question begins when the computational model changes. The issue is no longer only how expensive a classical search is, but what operations a quantum computer can perform over the corresponding computational state-space and entangled qubit key registers.

2. The Computational Boundary Changes

An n -qubit register has 2^n computational-basis states. Superposition changes how the machine represents and manipulates a state-space. This does not, by itself, establish a practical key-extraction attack against AES; it establishes the reason the classical security model must be analysed within a quantum computational model.

Grover is one response to that changed environment. It gives a quadratic speed-up for unstructured search, but its resource requirements include a long classic iterative quantum computation and a substantial oracle implementation. NIST's current technical work continues to treat these classical costs as central to the assessment of AES under quantum attack. [1][6]

3. The Grover Tunnel

Grover's algorithm became the dominant public model for quantum attacks on symmetric key search. The engineering question consequently becomes: how large and fault-tolerant must a quantum computer be to run Grover against AES?

That is a legitimate question. It is not the whole question.

A quantum resource estimate for one algorithm does not establish quantum resource requirements for other quantum algorithms.

Grover’s algorithm does not exhaust the useful quantum attack surface.

The danger of the Grover Tunnel is model closure: preparedness becomes organised around the resources required by Grover, and the resulting timetable can become the implicit boundary of AES quantum security.

**Grover is a single route through the quantum landscape.
It indicates a distant quantum timeline because it requires enormous fault-tolerant quantum computers.**

4. Outside the Tunnel: Quantum Key Extraction

QKE, as used in this briefing, is the threat class outside the Grover Tunnel. It describes the objective of extracting a cryptographic key from the quantum computational representation associated with the key-space and encryption process without assuming Grover’s classical iterative search architecture.

QKE is not presented here as a publicly demonstrated break of AES. No public evidence located for this revision establishes full-AES QKE. The point is different: the absence of a public QKE demonstration does not establish that Grover defines the entire future quantum attack surface, nor the threat timeline.

Recent research does demonstrate that quantum cryptanalysis is moving beyond purely abstract discussion. In 2026, peer-reviewed work reported successful Grover key recovery against Mini-AES in a quantum-circuit implementation and reviewed continuing efforts to reduce the resources required for quantum cryptanalysis. Separate 2026 work reported real-hardware quantum cryptanalysis of reduced or structured symmetric constructions, while explicitly stating that it did not break full AES. [7][8]

5. The Quantum-Safe Symmetric Encryption Problem

NIST’s post-quantum standards are principally a public-key response. FIPS 203 standardizes ML-KEM, a key-encapsulation mechanism used to establish a shared secret. FIPS 204 and FIPS 205 standardize digital-signature mechanisms. NIST SP 800-227, finalized in September 2025, provides recommendations for KEM use. [3][4][5]

The architectural sequence remains: public-key or KEM mechanism → shared secret → AES symmetric cipher → encrypted payload.

NIST itself describes the role of ML-KEM in these terms: a shared secret established by a KEM is then used with AES symmetric-key cryptographic algorithms for encryption and authentication. [3][4]

Quantum-safe key establishment is not, by itself, quantum-safe payload encryption.

6. Cryptographic Volume: The Payload Is the Mass

The supplied graphic, “Public Key vs AES Encryption,” is useful because it visualises the architectural asymmetry between the key-establishment layer and the payload layer. It must, however, be treated as an illustrative comparison rather than as a statistical census of global cryptographic traffic.

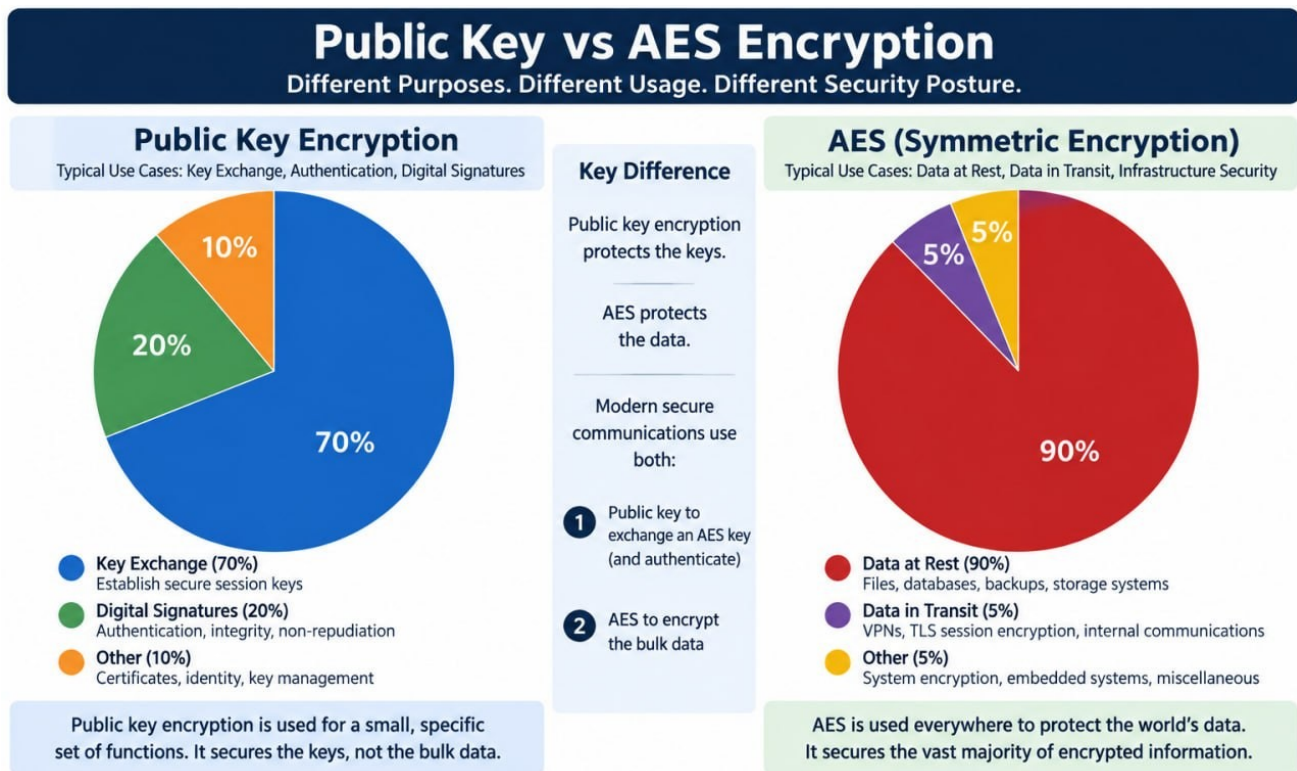


Figure 1. Supplied comparison graphic: Public Key vs AES Encryption.

The percentages are used here as an illustrative architectural model, not as measured global traffic statistics.

The graphic reveals a direct relationship between the two sides. The 70% public-key category is **key exchange**: it establishes the cryptographic keying relationship for secure communications. That relationship then feeds into the 5% AES category representing **data in transit**. The 70% is therefore not itself the payload; it is the mechanism that enables the 5% of AES-protected communications.

This distinction is fundamental to the quantum-security problem. NIST's PQC programme replaces and protects the **public-key** key-exchange layer, while the resulting communication is still protected by **AES** at the symmetric payload layer. The 70% key-exchange function therefore leads directly to the 5% AES data-in-transit function. Securing the 70% does not replace or secure the 5% against a quantum attack on AES itself.

The other 90% of AES shown in the graphic is data at rest. That is not preceded by a public-key exchange in the same operational sense. It is the enormous stored-data estate protected directly by symmetric encryption.

Importantly, any successful AES QKE would bypass and undermine the key exchange!

For scale, IDC's global DataSphere figure reached approximately 181 zettabytes in 2025. That figure covers data created and replicated worldwide; it is not a measurement of AES-encrypted data. [9]

If the supplied graphic's 95% AES bulk-data proportion were applied purely as an illustrative arithmetic model to 181 ZB, the result would be 171.95 ZB. That number must not be presented as the measured quantity of AES-protected data. It is a scale illustration only. The defensible conclusion is that the symmetric payload layer operates at zettabyte-scale across the global digital estate, whereas key establishment operates on comparatively tiny quantities of keying material.

The contrast can be expressed more precisely as architecture rather than false precision: ML-KEM establishes a shared secret; AES then uses symmetric keying material to protect the data stream or stored payload. NIST's own description makes that dependency explicit. [3][4]

7. The NIST PQC Asymmetry

The current NIST position is not that AES is being replaced by a post-quantum symmetric cipher. NIST's PQC programme has produced finalized standards for **public-key** key establishment and signatures, while its current **symmetric** guidance continues to regard AES-128/192/256 as providing significant resistance to known quantum attacks.

NIST IR 8547 identifies ML-KEM as the approved post-quantum public-key key-establishment mechanism and places AES-128, AES-192 and AES-256 within its security-category framework. NIST's FAQ continues to state that current applications can use AES-128/192/256 and that transition guidance for symmetric algorithms will be issued when a transition need can be foreseen. [2][4]

In 2026, NIST is also developing a wider Rijndael-256 variant to address data-volume and block-size considerations. NIST describes this work as complementing, not replacing, the current AES algorithms. [10]

**The resulting gap is precise:
NIST has a formal PQ migration pathway for quantum-vulnerable public-key cryptography,
while there is no finalized NIST post-quantum symmetric replacement for AES.**

8. Key Exchange Under the QKE Threat Model

A post-quantum KEM can protect the establishment of the symmetric session key against the class of attacks for which the KEM was designed. FIPS 203 states that ML-KEM is currently believed secure even against quantum adversaries. [3]

QKE asks a different question. If a quantum capability could recover the symmetric payload key from the ciphertext-side computational representation, then the security of the KEM exchange would no longer be sufficient to protect the payload. The attacker would not need to defeat ML-KEM at the key-establishment layer; the attacker would attack the symmetric key after establishment.

This is therefore a conditional consequence of the QKE threat model, not a claim that ML-KEM has been broken. Under QKE, quantum-safe key establishment and quantum-safe payload encryption are separate requirements.

The key exchange can be quantum-safe while the payload remains exposed.

9. The Missing Symmetric Off-Ramp

As of September 2026, the public NIST PQC programme provides no standardized replacement for AES as a quantum-safe bulk symmetric payload cipher. NIST's migration work is therefore not an AES-replacement competition. It is a public-key migration programme combined with continued confidence in current symmetric primitives under the dominant Grover quantum threat model. [2][4][10]

If a non-Grover key-extraction capability were demonstrated before a replacement architecture had been evaluated, standardized and deployed, there would be no ready-made symmetric migration runway. The issue is not simply selecting a larger AES key. It is whether the underlying architecture remains valid under the newly demonstrated quantum capability.

10. Historical Data: The First Clock

NIST's post-quantum response to public-key cryptography and the AES problem operate on fundamentally different clocks.

Key exchange is a here-and-now service. A post-quantum key-establishment mechanism such as ML-KEM is used when a new secure session is established. Replacing the vulnerable key-exchange mechanism therefore protects **future key establishment**.

AES is different. AES protects data **here and now**, but it also protects the enormous historical archive of data encrypted yesterday, last year, and decades ago. That ciphertext remains AES ciphertext regardless of which key-exchange mechanism was used to establish its key.

This creates the first clock:

The key-exchange clock starts when a new session is established.

The AES clock started when the data was encrypted and continues for as long as that ciphertext has value.

Consequently, replacing key exchange with a post-quantum mechanism does not solve the historical AES problem.

If a future capability can recover an AES key from existing ciphertext, the confidentiality of that ciphertext is already lost. **Changing the key-exchange mechanism after the fact cannot change the cryptographic state of historical AES ciphertext.**

This produces three distinct migration requirements:

- **Key exchange:** migrate the mechanism before future sessions are established.
- **AES-protected data at rest:** re-encrypt the historical data **now**, using a quantum-safe symmetric architecture, if that data is required to remain confidential against a future AES key-extraction capability.
- **AES data in transit:** newly created communications remain exposed to the AES problem even after the key-exchange layer has been made post-quantum, because the negotiated session key is ultimately used to protect the AES payload.

The architectural threat is therefore:

1. **NIST PQE key exchange → protects the establishment of the AES key**
2. **AES → protects the payload**
3. **AES QKE → extracts the AES key**
4. **Result → the post-quantum key exchange has been bypassed**

For historical data, the consequence is even more severe:

**Data encrypted today → remains AES ciphertext tomorrow
→ AES QKE → historical data exposed**

Therefore:

**Quantum-safe key exchange protects the future establishment of keys.
It does not make historical AES ciphertext quantum-safe.**

The migration of data at rest must consequently begin **before** the quantum capability that threatens AES becomes operational or publicly recognised.

The historical clock is already running.

11. Global Scope

AES is not one application. It is embedded throughout the digital estate:

- critical infrastructure — energy, telecommunications, transport, water and industrial control;
- financial systems — banking, payments, markets, clearing and settlement;
- national security — military, intelligence and strategic information;
- cloud and AI infrastructure — computing, credentials, models, datasets and protected workloads;
- government systems — operations, legal records and citizen data;
- corporate systems — intellectual property, industrial secrets and commercial strategy; and
- personal data — identities, communications and long-lived records.

The scale is therefore a global cryptographic infrastructure problem, not an encryption-product problem.

12. Current Quantum Evidence: What Has Actually Changed

The current public record supports a stronger statement than it did several years ago, but not the claim that full AES has been broken by a quantum computer.

- **2024–2026:** NIST continues to treat Grover as the principal known generic quantum key-recovery model for AES and continues to assess its large practical resource requirements. [1][6]
- **2026:** Peer-reviewed work reports successful Grover key recovery on Mini-AES in a quantum-circuit implementation and documents continuing optimisation of quantum resources. [7]
- **2026:** Research has demonstrated quantum cryptanalysis of reduced or structured symmetric constructions on real quantum hardware, while explicitly distinguishing those results from breaking full AES. [8]
- **2026:** Quantum cryptanalysis research is not confined to Grover. Published research has investigated alternative quantum approaches to symmetric cryptanalysis, including Simon-based, Bernstein–Vazirani, quantum related-key, differential and structural attacks. These approaches do not establish a break of full AES, but they demonstrate that Grover is not the complete research space for quantum attacks against symmetric cryptography.
- **2026:** NIST’s own work continues to develop and refine symmetric standards rather than declaring an imminent AES replacement. [10] These observations support the need to examine the attack surface beyond Grover. They do not constitute public proof of QKE against full AES.
- **2026:** NIST has not identified a quantum-safe replacement for AES, nor has it established a formal competition or standardisation process for selecting one. NIST’s current post-quantum programme therefore does not provide an AES replacement off-ramp.

13. The Adversary and Disclosure Problem

A cryptanalytic capability of exceptional intelligence or strategic value would have strong incentives to remain undisclosed. Public experiments therefore establish the boundary of public knowledge, not necessarily the boundary of private capability.

This is an intelligence-assessment issue, not evidence that QKE already exists. The correct national-security posture is to distinguish what is demonstrated, what is theoretically possible, and what cannot be ruled out by public evidence.

14. The National-Security Question

**Are we preparing for the arrival of the quantum threat
— or are we preparing only for the arrival of Grover?**

The question cannot be answered by Grover resource estimates alone. A national-security assessment must examine the functional space outside the Grover Tunnel, including alternative quantum mechanisms, AI-assisted cryptanalytic discovery, and the possibility that a decisive capability could emerge before the assumed Grover timetable.

The practical test is architectural: if AES ceased to be trusted tomorrow, what standardized, evaluated and deployable symmetric payload-encryption architecture would replace it? As of September 2026, there is no NIST-standardized answer to that question.

15. Conclusion

NIST's post-quantum programme is a major and necessary response to the quantum vulnerability of public-key cryptography. Its standards establish a real migration path for key establishment and digital signatures. That achievement should not be confused with a quantum-safe replacement for the symmetric payload-encryption layer.

The supplied comparison graphic makes the architectural asymmetry visible: public-key mechanisms establish trust and keying material; symmetric cryptography protects the bulk data. The 95% AES data-at-rest/data-in-transit share in the graphic is illustrative, but it correctly directs attention to the payload layer. The global data estate is measured in hundreds of zettabytes, while a KEM operates on keying material rather than on that bulk data.

QKE, as defined in this briefing, changes the question again. If a quantum capability can extract the symmetric payload key without relying on Grover's search architecture, then a quantum-safe key exchange does not, by itself, solve the payload problem. The KEM may remain secure while the data it enabled the parties to encrypt becomes recoverable through a different quantum attack.

The Grover Tunnel is therefore a warning about model closure. Grover is a known route through the quantum landscape. It should not be allowed to become the definition of that landscape.

**The danger is not only that there may be no warning.
The danger is also that preparedness is aimed at the wrong boundary.**

Reference Trail — Current Status, September 2026

The following sources were reviewed for this revision. Dates and status statements in the body are based on these current sources.

[1] NIST Post-Quantum Cryptography FAQ — symmetric cryptography and Grover

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs>

Current NIST FAQ: AES-128/192/256 may continue to be used; discussion of Grover and practical limitations.

[2] NIST Post-Quantum Cryptography — project overview and migration

<https://csrc.nist.gov/Projects/post-quantum-cryptography>

Current migration position, including the 2035 deprecation/removal horizon and high-risk migration earlier.

[3] NIST FIPS 203 — ML-KEM

<https://csrc.nist.gov/pubs/fips/203/final>

Finalized August 13, 2024; ML-KEM establishes shared secret keying material for subsequent symmetric cryptography.

[4] NIST SP 800-227 — Recommendations for Key-Encapsulation Mechanisms

<https://csrc.nist.gov/pubs/sp/800/227/final>

Finalized September 2025; KEM definitions, properties and deployment recommendations.

[5] NIST FIPS 204 / FIPS 205 — ML-DSA and SLH-DSA

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

Finalized NIST post-quantum digital-signature standards.

[6] NIST — On the Practical Cost of Grover for AES Key Recovery

<https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf>

NIST technical discussion of AES Grover resource costs and the overheads of quantum implementation.

[7] npj Quantum Information — Quantum cryptanalysis of SPN ciphers with known plaintext

<https://www.nature.com/articles/s41534-026-01218-x>

2026 peer-reviewed study reporting successful Grover key recovery on Mini-AES and discussing quantum resource optimisation.

[8] 2026 research — Quantum cryptanalysis on IBM quantum hardware

<https://arxiv.org/abs/2607.18340>

Real-hardware quantum cryptanalysis of reduced/structured symmetric constructions; explicitly not a full-AES break.

[9] IDC global DataSphere figure as reported in 2026

<https://www.techtarget.com/data-technologies/tip/Is-your-data-infrastructure-ready-for-the-zettabyte-era>

IDC figure reported as approximately 181 zettabytes of global data in 2025. Used only as scale; not treated as AES-encrypted volume.

[10] NIST — Advances in NIST Symmetric-Key Standards: Ascon, Accordion, and Wide-AES

<https://csrc.nist.gov/csrc/media/presentations/2026/mpts2026-3a1/images-media/mpts2026-3a1-slides-nist-symm-meltem.pdf>

2026 NIST presentation: wider Rijndael-256/AES-family work is described as complementing, not replacing, current AES.

Interpretive Status of QKE

QKE is used in this briefing as the Portalz threat-model terminology for a class of quantum key-extraction capability outside Grover's iterative search model. It is not a NIST-defined algorithm or a publicly demonstrated full-AES break. The briefing deliberately distinguishes documented NIST positions and published research from the strategic threat proposition represented by QKE.

Quantitative Note on the Supplied Graph

The graph supplied for this revision shows 90% of AES use as data at rest and 5% as data in transit. Those two categories total 95%. The public-key side shows 70% key exchange, 20% digital signatures and 10% other. These figures are treated as an illustrative architectural model. They are not used as measured global encryption-traffic statistics.

The 181 ZB global DataSphere figure is likewise not treated as AES-encrypted volume. It is used to demonstrate the scale of the digital estate. The arithmetic illustration $181 \times 95\% = 171.95$ ZB shows what a 95% proportion would look like at that scale, but it is explicitly not a claim that 171.95 ZB of AES-protected data exists.

Why This Briefing Is Coming From Portalz

Portalz is an Australian technology company with ongoing R&D in the fields of quantum-safe cryptography and information systems spanning six years.

We have been examining the quantum-security problem from an architectural perspective.

In 2021, we identified that quantum computing breaks the classical assumption of security by computational difficulty for symmetric encryption such as AES.

This led to investment in developing original IP, invented by Wolfgang Flatow in 2020, that approached symmetric security through both computational difficulty and **Shannon OTP compliance — security by logical impossibility**.

That work has now produced a demonstrated encryption technology: **FES (Fractal Encryption Standard)**.

In the course of this project, our team has investigated quantum computing with the particular objective of determining the quantum vulnerability of FES.

This, in turn, has led to deeper insights into the quantum vulnerability of AES and the peculiar circumstances surrounding current preparedness, including the limitations of the present NIST post-quantum approach.

We are therefore bringing this briefing to you because our own research into making symmetric cryptography quantum-safe led us directly to the question of whether the current national-security response is examining the complete quantum threat surface.