



Quantum Key Extraction (QKE) Ontology and Three Core Tautologies

Wolfgang Flatow

2026

Abstract

This paper defines the Flatow Quantum Key Extraction (QKE) ontology from two foundational assumptions of useful quantum computation and three core tautologies. The QKE computational primitive is the AES Decrypt Unitary (ADU), expressed as a unitary function of ciphertext, Oracletext, and the complete Hadamard-assembled key-space. Pattern matching is intrinsic to the ADU computation: the matching plaintext condition is evaluated within the same coherent operation across the complete key-space. When the Oracletext condition matches, the corresponding key K is the ADU result. No separate marking phase or FOUND flag is required. Access to the computed result is treated as a foundational property of useful quantum computation and the physical read mechanism is therefore outside the scope of this ontology. Qubit errors that do not satisfy the Oracletext condition remain within the non-matching population and do not constitute an ADU result.

1 Foundational Quantum-Computing Assumptions

QKE begins with two foundational assumptions concerning useful quantum computation.

A1: Unitary Computation

The coherent operations of a quantum computer are implemented as unitary functions:

A_1 : Quantum computation is effected through unitary operations.

A2: Accessible Computational Results

The result of a quantum computation can be accessed or read:

A_2 : The result of a quantum computation can be accessed/read.

These assumptions establish the operational boundary of the ontology. If controlled quantum computation cannot be performed, or if its result cannot be accessed, the device ceases to function as a useful computer and reduces operationally toward a random-state generator.

Accordingly, this paper does not specify a physical read mechanism. It establishes what QKE computes. Under A2, the computed result is accessible.

2 QKE Ontology

For AES-256, QKE is constructed around three objects:

$$C = \text{ciphertext}, \quad O = \text{Oracletext}, \quad \mathcal{K} = \text{AES-256 key-space}.$$

The QKE computational function is the AES Decrypt Unitary:

$$\boxed{\text{ADU}(C, O, \mathcal{K})}$$

The Oracletext O is a deterministic known plaintext pattern or condition whose existence can be tested against an AES decryption result.

The ontology contains exactly three core tautologies. Their combination defines the ADU result.

3 Core Tautology I: The Complete Key-Space Exists in Superposition

Let

$$\mathcal{K} = \{0, 1\}^{256}, \quad |\mathcal{K}| = 2^{256}.$$

Beginning with a 256-qubit key register,

$$|0\rangle^{\otimes 256},$$

Hadamard assembly produces

$$|\Psi_{\mathcal{K}}\rangle = H^{\otimes 256}|0\rangle^{\otimes 256} = \frac{1}{\sqrt{2^{256}}} \sum_{K \in \mathcal{K}} |K\rangle.$$

Thus the complete 2^{256} AES-256 computational-basis key-space exists in the assembled quantum state:

256-qubit Hadamard assembly $\Downarrow$ complete 2^{256} AES-256 key-space exists in superposition

This is not a statement that the register merely *can* represent the key-space. It is the state produced by the Hadamard construction.

4 Core Tautology II: AES Decryption Is a Unitary Computation

AES decryption is deterministic reversible computation and can be represented within a reversible quantum circuit. QKE names this operation the **AES Decrypt Unitary (ADU)**.

For a candidate key K and ciphertext C , define

$$P_K = \text{AES}_K^{-1}(C).$$

The ADU acts coherently across the complete Hadamard-assembled key-space. Schematically,

$$U_{\text{ADU}} \left(\frac{1}{\sqrt{2^{256}}} \sum_{K \in \mathcal{K}} |K\rangle |C\rangle |O\rangle \right).$$

The important QKE consequence is that AES decryption is not invoked against one classically iterated key at a time. The unitary computation acts upon the complete assembled key-space.

Complete $\mathcal{K} \xrightarrow{U_{\text{ADU}}} \text{AES decrypt computation across all } K \text{ in superposition}$

5 Core Tautology III: AES Has One Sensible Result

For the ciphertext under consideration, exactly one AES key produces the sensible structured plaintext. All other keys produce random output within the AES wrong-key model.

There therefore exists a unique key $K^* \in \mathcal{K}$ such that

$$D_{K^*}(C) = P_{\text{sensible}},$$

while for every other key,

$$K \neq K^* \implies D_K(C) = P_{\text{random}}.$$

The third tautology is therefore

$\exists! K^* \in \mathcal{K} : D_{K^*}(C) = P_{\text{sensible}}$

with the remaining $2^{256} - 1$ candidate keys producing wrong-key random results.

6 Oracletext Pattern Matching Is Intrinsic to ADU

QKE does not place a separate filtering or marking operation after AES decryption. The Oracletext comparison is part of the ADU computational function itself.

Define the ADU match condition

$$M(K; C, O) = \begin{cases} 1, & D_K(C) \models O, \\ 0, & D_K(C) \not\models O. \end{cases}$$

The coherent ADU computation therefore includes both the AES decrypt relation and the Oracletext match relation for every K represented in the complete key-space superposition.

Conceptually,

$(C, O, |\Psi_{\mathcal{K}}\rangle) \xrightarrow{\text{ADU}} [D_K(C) \text{ matched against } O]_{K \in \mathcal{K}}$

There is no separate temporal sequence of

$$\text{decrypt} \rightarrow \text{mark} \rightarrow \text{find}.$$

Pattern matching or non-matching exists within the ADU computation itself.

7 ADU Match Is the Found Condition

Within this ontology, FOUND is not a separate flag, ancillary search mechanism, or subsequent computational phase.

The found condition is simply the existence of an ADU match:

$$\boxed{\text{FOUND} \equiv \exists K \in \mathcal{K} : M(K; C, O) = 1}$$

Under Core Tautology III, where the Oracletext belongs to the unique sensible plaintext,

$$M(K^*; C, O) = 1$$

and

$$\forall K \neq K^*, \quad M(K; C, O) = 0.$$

Thus

$$\boxed{\text{ADU MATCH} = \text{FOUND}}$$

is a condition of ADU rather than an additional mechanism.

If the Oracletext does not occur in any AES decrypt result, then

$$\forall K \in \mathcal{K}, \quad M(K; C, O) = 0,$$

and no found condition exists.

8 K Is the ADU Result

The central reduction of the QKE ontology is that the matching key is not subsequently searched for after the ADU computation. The matching key is the ADU computational result.

Define

$$\boxed{\text{ADU}(C, O, \mathcal{K}) = \begin{cases} K^*, & \exists! K^* : M(K^*; C, O) = 1, \\ \emptyset, & \nexists K : M(K; C, O) = 1. \end{cases}}$$

Consequently,

$$\boxed{K = \text{ADU output.}}$$

The ADU does not first produce a marker that points toward K . It does not require a later operation to search for a marked key. The Oracletext match condition is intrinsic to ADU and the matching K is its filtered computational result.

The ontology can therefore be reduced to

$$\boxed{(C, O, \mathcal{K}) \xrightarrow{\text{ADU}} K^*}$$

when the unique Oracletext match exists.

9 The ADU Result Exists Within Superposition

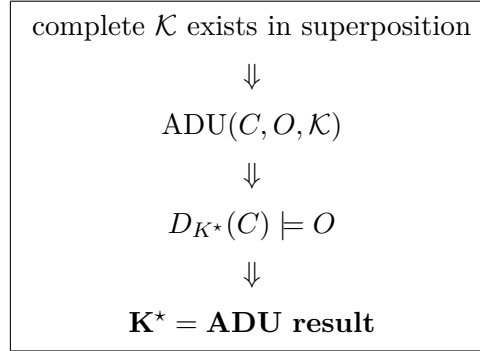
The ADU operates coherently upon the complete key-space. Accordingly, matching and non-matching decrypt relations are established within the same superposed computation.

The important distinction is that QKE does not require an externally created mark to identify K^* . The relation

$$D_{K^*}(C) \models O$$

exists as part of the ADU-computed state itself.

Under the three core tautologies, only the unique sensible key satisfies the Oracletext condition. The ADU therefore presents a filtered result in which the matching K^* is the computational output associated with the match condition.



No separate pre-computation or post-computation marking phase is introduced into the ontology.

10 Result Access Is Assumed, Not Reimplemented

A2 states that the result of a quantum computation can be accessed/read. QKE therefore does not require the ontology to invent a separate physical read architecture.

Once

$$\text{ADU}(C, O, \mathcal{K}) = K^*,$$

K^* is the quantum computational result. Under A2, that result is accessible.

The ontology therefore deliberately stops at

$\text{ADU}(C, O, \mathcal{K}) = K^*$

rather than introducing an additional key-marking, key-search, buffer, or speculative read mechanism.

This separation is methodological: the purpose of the ontology is to establish the computation and its result, not to redefine the general result-access capability assumed for useful quantum computers.

11 Qubit Error Model

Qubit errors are considered within the same ADU/Oracletext relation.

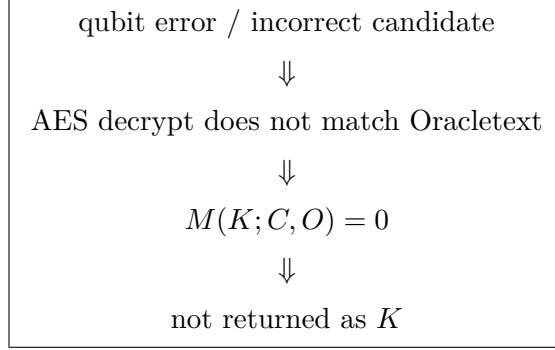
The ADU result is conditioned upon

$$M(K; C, O) = 1.$$

An erroneous key state or erroneous decrypt result that does not satisfy the Oracletext condition therefore remains non-matching:

$$M(K_{\text{error}}; C, O) = 0.$$

Such a state is not an ADU result.
Conceptually,



QKE therefore does not require correction of every erroneous candidate merely because an error occurred. Within the ontology, errors that produce non-matching states fall into the non-result population and are rejected by the ADU match condition.

The relevant condition is not whether every branch is error-free. It is whether a branch satisfies the ADU/Oracletext match relation:

$M(K; C, O) = 1 \quad \Longleftrightarrow \quad K \text{ qualifies as the ADU result.}$

Thus ordinary qubit noise that produces an incorrect key or incorrect plaintext does not itself create a QKE result. It remains outside the matching ADU output.

12 Deduction from the Three Core Tautologies

The ontology now reduces to a short deductive chain.

- D1.** By Core Tautology I, the complete AES-256 key-space exists in the 256-qubit Hadamard superposition.
- D2.** By Core Tautology II, the ADU can compute AES decryption coherently across that complete key-space.
- D3.** By Core Tautology III, exactly one key produces the sensible plaintext while all other keys produce wrong-key random results.
- D4.** Oracletext pattern matching is intrinsic to the ADU function, so each decrypt result either satisfies or does not satisfy O within the same coherent computation.
- D5.** When the Oracletext belongs to the sensible plaintext, exactly one relation satisfies

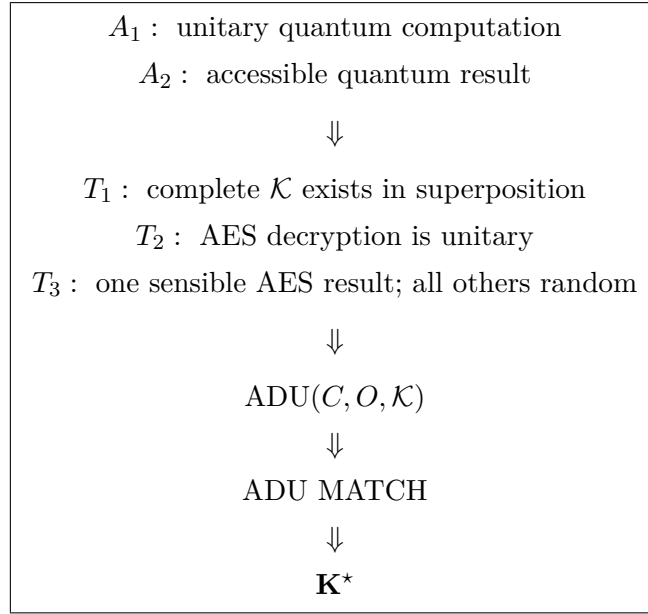
$$M(K; C, O) = 1.$$

- D6.** That matching K is the ADU result:

$$\text{ADU}(C, O, \mathcal{K}) = K^*.$$

- D7.** By A2, the ADU computational result is accessible/readable. No additional read mechanism is required by the ontology.

The complete QKE statement is therefore



13 Ontology Summary

Term	Meaning in the QKE Ontology
A1	Coherent quantum computation is effected through unitary operations.
A2	Quantum computational results are accessible/readable.
$\mathcal{K}$	Complete AES-256 key-space existing in the Hadamard-assembled 256-qubit superposition.
C	AES ciphertext supplied to ADU.
O	Oracletext: deterministic known plaintext pattern or condition.
ADU	AES Decrypt Unitary incorporating AES decryption and Oracletext pattern matching across the complete key-space.
$M(K; C, O)$	ADU match condition: true exactly when the plaintext produced by K satisfies the Oracletext.
FOUND	Not a separate flag or mechanism; simply the existence of an ADU match.
K^*	Unique matching key and therefore the ADU computational result.
Qubit error	Non-matching erroneous states remain outside the ADU result unless they satisfy the Oracletext condition.
READ	General access to the computed quantum result, assumed under A2 and outside the implementation scope of this ontology.

14 Conclusion

The QKE ontology is founded upon two assumptions of useful quantum computation and three core tautologies.

The complete AES-256 key-space exists following Hadamard assembly. AES decryption can be implemented as a unitary computation across that complete superposition. AES has one sensible decryption result while wrong keys produce random results. Oracle text pattern matching is incorporated within the ADU itself.

Accordingly, QKE requires no separate marking phase. The match is a condition of the ADU computation, and the matching key is the ADU result:

$$\boxed{\text{ADU}(\text{Ciphertext}, \text{Oracletext}, \text{key-space}) \rightarrow K}$$

When no Oracle text match exists, ADU produces no matching K . When the unique sensible plaintext matches the Oracle text, the corresponding K is the computational result.

Qubit errors that produce incorrect decryptions remain non-matching and therefore do not constitute the ADU result. Result access itself is not reimplemented by QKE: under A2, the computed result is accessible.

The defining QKE reduction is therefore

$$\boxed{\text{Complete key-space} \implies \text{ADU decrypt} + \text{match} \implies K}$$

References

1. C. H. Bennett, “Logical Reversibility of Computation,” *IBM Journal of Research and Development*, vol. 17, no. 6, pp. 525–532, 1973.
2. National Institute of Standards and Technology, *FIPS PUB 197: Advanced Encryption Standard (AES)*.
3. W. Flatow, *Quantum Key Extraction (QKE): A Tautological Argument for AES Quantum Vulnerability*, 2026.