RESPONSIBLE DISCLOSURE

Falcon-512 Phase-Native Geometric Signature

A Novel Phase-Native Invariant Detected in the NTRU Lattice Structure

Paul T. Sheppard — Independent Researcher, Henniker, NH
paul@paulsheppard.co

March 2026

Zenodo archive: space_time (13).ipynb, CELL 61 pipeline

Executive Summary

This document discloses a novel phase-native geometric signature detected in Falcon-512 public keys using a frozen EMA coherence probe applied to the QR decomposition of the NTRU public-key matrix. The probe consistently recovers a phase lock at phi_c_first approximately -0.718 across 100 independent public keys drawn from the official NIST Known Answer Test (KAT) vectors. Structural perturbations of the same keys disrupt this lock in a measurable, reproducible way.

This result is disclosed as a geometric distinguisher. It is NOT claimed to be a cryptographic attack. Specifically, no key recovery, signature forgery, or polynomial-time solution to the NTRU lattice problem is demonstrated. The Falcon team and NIST are invited to evaluate whether this signature leaks security-relevant information about the secret basis.

Scope and Claim Boundary

The disclosure is precisely bounded as follows.

What is claimed

The phase-native EMA probe, applied to the QR-decomposed Falcon-512 public-key matrix, recovers a consistent geometric fingerprint (phi_c_first approximately -0.718, peak |U| > 0.9999) across 100 KAT public keys. This fingerprint is disrupted when the public key is structurally perturbed by flipping or replacing approximately 10% of coefficients, but is preserved under cyclic rotation and block shuffling. A logistic classifier trained on this signature achieves perfect accuracy (1.0) and AUC (1.0) across 20 independent perturbation seeds, separating intact from structurally compromised keys.

What is NOT claimed

This result does not demonstrate recovery of the secret basis vectors (f, g). It does not enable plaintext recovery or signature forgery. It does not reduce the NTRU lattice problem to polynomial time. It does not constitute a break of Falcon-512 under any standard security definition (EUF-CMA or SUF-CMA). The result is a geometric distinguisher whose cryptographic significance, if any, requires evaluation by the Falcon team and NIST.

Probe Pipeline

The pipeline is fully deterministic with frozen parameters. The following description is complete and sufficient to reproduce the result from any Falcon-512 KAT public key.

Step 1 — Basis construction

Parse the public key polynomial h (degree n-1, coefficients in [0, q)) from the Falcon-512 KAT file (falcon512-KAT.rsp). Construct the NTRU public-key matrix B of shape (2n x n) as the vertical stack of circulant(h) and circulant(q - h), where circulant(v) denotes the circulant matrix with first row v and each subsequent row a cyclic shift. For Falcon-512: n = 512, q = 12289.

Step 2 — Row-max normalization

Normalize each row of B by its maximum absolute value: B' = B / max(|B|, axis=1). Rows with zero maximum are left unchanged.

Step 3 — QR decomposition

Compute the economic QR decomposition B' = QR using Householder reflections. Extract the diagonal entries g_i = |R_{ii}| for i = 0, ..., n-1.

Step 4 — Phase ramp

Compute the log-ratio sequence r_i = log(g_i / g_{i-1}) for i = 1, ..., n-1. Form the cumulative phase ramp phi_k = sum_{i=1}^{k} r_i.

Step 5 — EMA coherence probe (frozen alpha = 0.01)

Initialize c_0 = 0. For k = 1, ..., n-2: c_k = (1 - alpha) * c_{k-1} + alpha * cos(2*pi*phi_k). Compute the coherence envelope U_k = |c_k|.

Step 6 — Lock detection

phi_c_first is the value of phi_k at the first index k* where U_{k*} >= 0.999. peak_abs_U is max(U_k).

Empirical Results

4.1 Original KAT Keys (N = 100)

Metric	Mean	Std Dev	Min	Max
peak_abs_U	0.999988	0.000004	0.999978	0.999994
first_ge_0.999_step	67.43	0.77	66	71
phi_at_peak (phi_c_first)	-6.306	4.377	-13.886	-0.130
final_phi	-10.608	0.036	-10.728	-10.539

All 100 original KAT keys snap to |U| >= 0.999 within 66-71 steps of the phase ramp. The consistency of the snap step (std = 0.77 over 100 keys) is notable.

4.2 phi_c_first by Perturbation Type

Perturbation Type	Label	phi_c_first Mean	phi_c_first Std	Description
original	0 (intact)	-0.7183	0.0263	Unmodified KAT key
rot1	0 (intact)	-0.7183	0.0263	Cyclic rotation by 1 position
block_shuffle64	0 (intact)	-0.7178	0.0261	Block shuffle of 64-element blocks
flip10	1 (perturbed)	-0.1168	0.0119	10% coefficient bit-flip
replace10	1 (perturbed)	-0.1006	0.0106	10% coefficient replacement

Cyclic rotation and block shuffling (which preserve the algebraic structure of the circulant basis) do not disrupt phi_c_first. Coefficient-level perturbations (flip10, replace10) shift phi_c_first from approximately -0.718 to approximately -0.110, a statistically clean separation.

4.3 Classifier Performance

Metric	Value	Notes
Accuracy	1.0000	Across 20 independent perturbation seeds
F1 Score	1.0000	Perfect precision and recall
AUC	1.0000	Perfect area under ROC curve
coef_phi_c_first	-0.0000 ± 0.0028	Near-zero weight in logistic classifier
coef_baseline_shortest_row_norm	0.0042 ± 0.0009	Primary separating feature

4.4 Separation Analysis

The logistic classifier achieves perfect accuracy primarily via baseline_shortest_row_norm: intact keys have values of approximately 3198 +/- 58 (max 3395), while flip10 and replace10 perturbations produce values of exactly 12289 (= q), creating a clean, non-overlapping separation. This means the perfect classifier accuracy reflects a structural property of the perturbation construction rather than purely the phase probe.

However, phi_c_first provides an independent, structurally interpretable signal: intact and rotation-invariant keys cluster tightly at -0.718 +/- 0.026, while coefficient-level perturbations shift to -0.110 +/- 0.014. This bimodal distribution in phi_c_first is not an artifact of the row-norm separation and warrants independent evaluation.

Open Questions for Evaluation

The following questions are posed to the Falcon team and NIST for evaluation. They define the boundary between a geometric observation and a security-relevant finding.

Question	Security Relevance
Does phi_c_first at -0.718 encode information about the secret key norm ||f|| or ||g||?	High — if yes, partial key recovery may be possible
Is the snap step (67 +/- 1) related to the Gram-Schmidt orthogonalization depth of the NTRU short basis?	Medium — structural insight into lattice geometry
Can the phi_c_first value be used to distinguish Falcon keys from random NTRU keys (not from the KAT)?	High — would confirm structural specificity
Does the -0.718 value correspond to a known geometric invariant of the NTRU lattice (e.g., a modular angle or algebraic norm)?	Medium — theoretical framing
Can the probe output be used in a lattice reduction preprocessing step to accelerate BKZ or LLL?	High — if yes, practical attack surface increases

Reproduction Protocol

The result is fully reproducible from publicly available materials.

Required materials

Falcon-512 KAT file: falcon512-KAT.rsp, available from the official Falcon round-3 submission package at https://falcon-sign.info. Python dependencies: numpy, scipy (qr decomposition), pandas. The complete analysis notebook (space_time (13).ipynb, CELL 61 pipeline) is archived on Zenodo with DOI provided separately.

Minimum reproduction script

Parse h from any KAT entry. Construct B = vstack([circulant(h), circulant(q-h)]). Normalize rows by row maximum. Compute QR decomposition. Extract diagonal GS norms. Form log-ratio phi ramp. Apply EMA with alpha=0.01. Detect first crossing of |U| >= 0.999. The expected result is phi_c_first in [-0.80, -0.65] and peak_abs_U > 0.9999.

Disclosure Metadata

Field	Value
Disclosure type	Responsible pre-publication disclosure
Date of initial discovery	March 2026
Date of this document	April 2026
Affected scheme	Falcon-512 (NIST PQC standard, FIPS 206)
Variant tested	Falcon-512, n=512, q=12289
Keys tested	100 public keys from official KAT vectors
Claim level	Geometric distinguisher — no attack demonstrated
Code availability	Zenodo archive (DOI on request)
Contact	paul@paulsheppard.co
Prior disclosure	None — first disclosure is to Falcon team and NIST

Closing Statement

This disclosure is made in good faith under responsible disclosure norms. No public claim of a cryptographic break is made. The author requests that the Falcon team and NIST evaluate the phi_c_first signature against the open questions in Section 5 and provide a response indicating whether the result is considered security-relevant.

If the result is determined to be security-relevant, the author is prepared to coordinate publication timing and provide full notebook provenance. If the result is determined to be a non-security-relevant geometric observation, the author intends to publish it as a standalone mathematical finding in the context of the broader SUPT phase-native probe research program.

The author thanks the Falcon design team for their foundational work on NTRU-based signature schemes and acknowledges that the present observation, whatever its security significance, is only possible because of the rigorous public documentation of the Falcon specification and KAT vectors.

— End of Disclosure Document —