Analog Guard®

Encryption Implemented as a Physical-Layer Mixed-Signal Environment

Foundational IP White Paper

Core thesis

Analog Guard® frames secure communication as a dynamically evolving physical signal environment rather than as a purely mathematical data-layer operation.

Prepared for	Technical, investor, aerospace/cybersecurity, secure communications, and spectrum-operations audiences
Prepared by	Analog Guard, Inc.
Source document	Analog Guard Foundational IP Article V4
Date	December 2025

Document Profile

Item	Description
Subject	Physical-layer mixed-signal encryption using dynamically evolving analog signal behavior.
Technology focus	Analog Guard® architecture, including dynamic carriers, PLTNM, resonant analog behavior, parallel signal paths, and matched analog reconstruction.
Primary problem addressed	Conventional encrypted communications may hide message contents while leaving carrier behavior, timing, spectral structure, and transmission patterns observable.
Architectural premise	Protection may be distributed through the physical behavior of the communication signal itself rather than being limited to software algorithms and static digital keys.
Reader orientation	This document is a white-paper presentation of the attached article; it is not a patent claim chart, product datasheet, or security certification report.

Executive Summary

Modern cybersecurity is primarily organized around mathematical protection of digital information. Encryption algorithms, keys, protocols, and authentication mechanisms remain essential, but they generally operate after information has been separated from the physical signal environment that carries it.

Analog Guard® proposes a different architectural model. The communication signal itself participates in the protection mechanism through dynamic carrier behavior, analog waveform evolution, phase relationships, timing distortion, resonant behavior, and multidimensional mixed-signal modulation.

This white paper explains the foundational IP concept in which security is implemented as a physical-layer mixed-signal environment. The protected object is not merely the data payload. It is the evolving waveform environment in which carrier behavior, temporal relationships, and analog-state conditions influence whether information can be recovered.

The practical implication is a shift from purely key-centric encryption toward reconstruction-dependent security. Successful recovery depends not only on access to the appropriate keying relationship, but also on reproduction of the correct analog conditions, timing behavior, carrier dynamics, phase relationships, and signal-processing environment.

Key Takeaways

- Analog Guard® treats the waveform and carrier environment as active parts of the encryption architecture.
- The architecture is designed to reduce stable reference points used by interception, classification, and model-assisted signal analysis systems.
- Parallel paths may preserve independent analog-encrypted channels until after decryption and binary reconstruction.
- PLTNM and related analog processes introduce timing, phase, resonance, and waveform-shaping behavior into the protection environment.
- Matched analog conditions support recovery; mismatched analog conditions can produce distortion, noise, and reconstruction failure.
- The approach complements, rather than replaces, conventional cryptographic and secure-communications techniques.

Contents

1. Introduction and Core Thesis

Modern cybersecurity was built on a relatively simple assumption: information can be protected mathematically. For decades, encryption systems have relied on algorithms that transform readable data into computationally difficult problems using digital keys and software-based cryptographic operations. Whether protecting financial systems, military communications, cloud infrastructure, or consumer devices, the dominant philosophy has remained largely unchanged: security exists primarily in mathematics.

Analog Guard® proposes a fundamentally different approach.

The technology described in U.S. Patent Nos. 12,126,720 and 12,615,149 suggests that information security can also emerge from the controlled complexity of physical signal behavior itself. Instead of relying exclusively on computational algorithms, the architecture embeds protection into continuously changing analog waveforms, dynamic carrier environments, resonant behavior, phase relationships, temporal distortion, and multidimensional analog modulation processes.

In practical terms, Analog Guard® treats the communication signal itself as part of the encryption mechanism.

This distinction is important because traditional communications systems separate the message from the transport mechanism carrying it. A digital encryption algorithm scrambles the information, but the carrier transporting the encrypted data often remains relatively stable and observable. Frequencies may hop, modulation schemes may vary, and spread-spectrum techniques may be used, but the underlying transmission structure still tends to exhibit identifiable behavior.

Advanced signal-intelligence platforms classify emissions by analyzing carrier stability, timing periodicity, spectral signatures, synchronization structures, pulse intervals, modulation characteristics, and statistical repetition. AI-assisted systems can accelerate this process by identifying subtle recurring behaviors across large signal datasets. Even when encrypted data cannot be directly decoded, the transmission itself may reveal operational information.

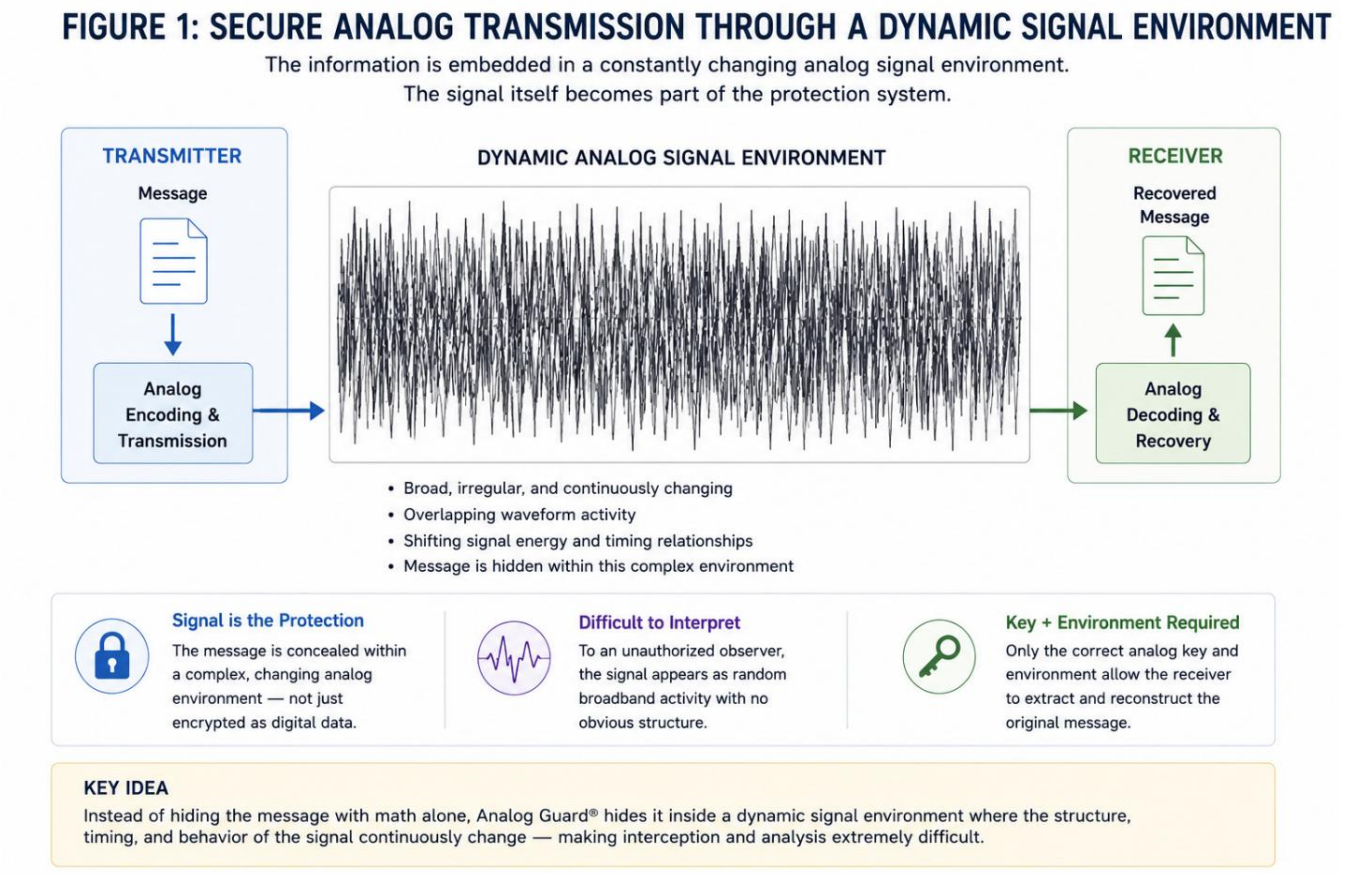

Figure 1. Transmission concealed within a continuously evolving analog signal environment.

Analog Guard® is designed to reduce those stable reference points by moving protection into the broader signal environment. Carrier behavior, timing, resonance, phase structure, waveform evolution, and analog dynamics all become part of the protection architecture.

Unlike conventional encryption systems, where the carrier simply transports encrypted bits, Analog Guard® integrates the carrier directly into the protection process. The waveform carrying the information becomes inseparable from the encryption architecture itself. An unauthorized observer is therefore confronted not merely with encrypted data, but with an unstable physical signal environment whose behavior changes during operation.

This changes the nature of attack. Instead of simply recovering a digital key or breaking an algorithm mathematically, an interceptor may also need to reconstruct the analog conditions governing the transmission in real time. That means reproducing not only the proper data relationships, but also the correct carrier dynamics, phase behavior, temporal structure, resonant conditions, and modulation interactions simultaneously.

2. Dynamic Carrier Environment

The foundational patents repeatedly refer to the concept of a dynamic carrier. In conventional communication systems, carriers are generally stable and predictable. Their frequencies, phases, and modulation behavior follow controlled standards designed for reliable synchronization and efficient transmission.

Analog Guard® intentionally disrupts that stability. The carrier is no longer treated as a passive delivery mechanism; it becomes part of the protection mechanism.

As illustrated in Figure 2, Analog Guard® transforms binary information into analog waveform behavior before encryption occurs.

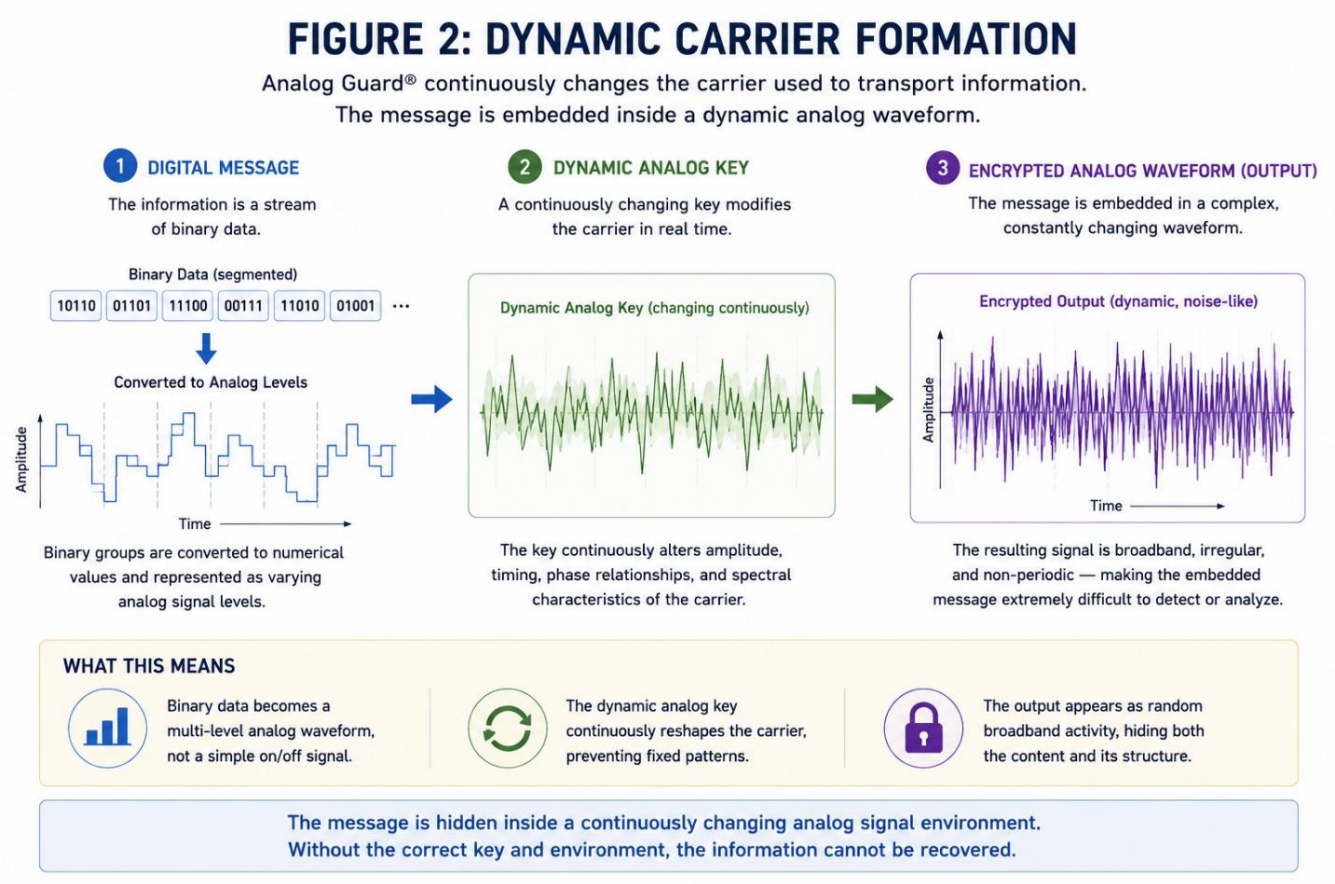

Figure 2. Binary information converted into analog waveform behavior before dynamic carrier-based encryption.

3. Analog Encoding and Carrier Participation

Rather than treating the message as a simple digital bitstream, the system converts grouped binary values into varying analog amplitude levels, creating a complex non-periodic waveform. The analog key then continuously modifies the carrier environment in real time, altering signal relationships as transmission occurs.

This is a major departure from conventional encryption systems. In traditional digital encryption architectures, the encrypted data exists independently of the carrier transporting it. In Analog Guard®, the carrier itself becomes part of the protection mechanism. The signal environment continuously changes while carrying the information.

The result is a transmission whose structure, timing behavior, phase relationships, and spectral distribution evolve during operation. To an unauthorized observer, the transmission may resemble broadband analog noise rather than recognizable communications traffic.

This is strategically important because interception systems depend heavily on stable patterns. Fixed timing intervals, recognizable spectral distributions, and repetitive modulation behavior all provide clues that enable classification and analysis. Analog Guard® is designed to reduce those clues before they can be exploited.

4. Parallel Signal Paths and Analog-State Partitioning

As the architecture evolves, the system expands into multiple parallel signal paths operating simultaneously. Importantly, these parallel paths are not mixed together prior to decryption. Instead, each path functions as an independent encrypted transmission channel carrying its own analog-encrypted signal stream.

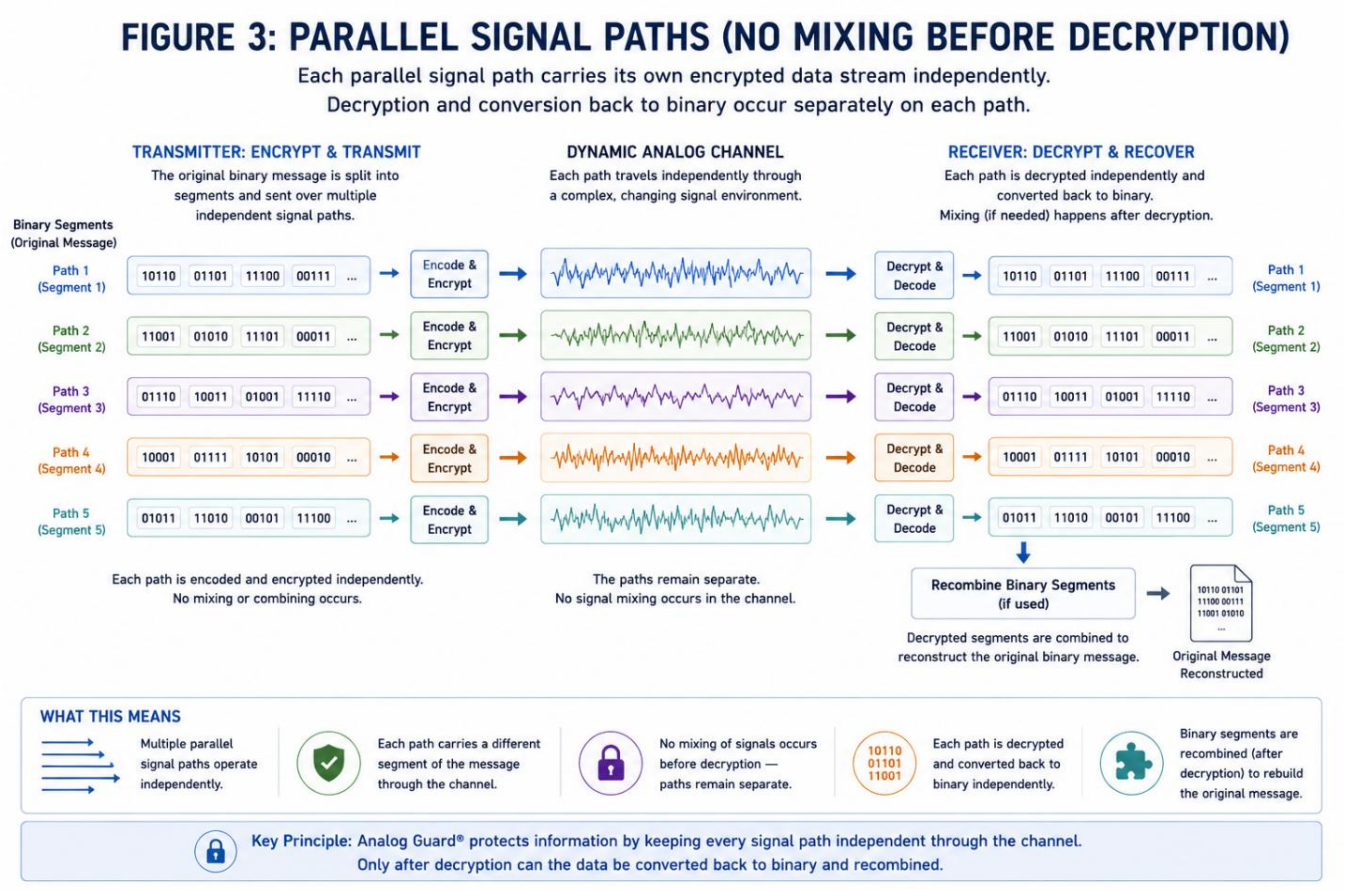

Figure 3. Independent parallel analog-encrypted signal paths maintained separately until recovery.

This distinction is critical to understanding the parallel Analog Guard® implementation. In some secure communications systems, multiple signal streams may be combined into a composite waveform before

transmission. Analog Guard® does not operate this way in its parallel implementation. Each signal path remains physically separate throughout transmission and recovery.

Figure 3 illustrates this concept by showing the original binary message divided into smaller data segments, with different portions of the binary information assigned to separate signal channels. Each channel independently converts its assigned binary segment into an analog-encoded waveform before encryption and transmission.

The analog waveforms are intended to be irregular, multi-level, non-periodic, and continuously varying rather than sinusoidal or repetitive. Each signal path may be visually and operationally distinct, reflecting differences in timing, phase behavior, modulation characteristics, or analog encoding conditions.

The important point is that the parallel analog signals themselves are never recombined during transmission. Each path remains independent while traveling through its own dynamically changing analog signal environment. The encrypted waveforms therefore remain isolated from one another until the recovery stage.

At the receiver, each analog signal path undergoes independent decryption and recovery. The recovered analog information from each path is then converted back into its corresponding binary data segment. Only after successful decryption and binary reconstruction are the separate binary segments recombined to rebuild the original message or data file.

This architecture increases security and complexity because interception would require recovering multiple independent encrypted analog channels simultaneously. An interceptor would not only need to recover the correct analog conditions for one signal path, but potentially several distinct encrypted paths operating independently at the same time.

5. Temporal Encryption and PLTNM

Figure 4 introduces another major concept within the Analog Guard® architecture: temporal encryption and timing manipulation.

Conventional communication systems depend heavily on precise timing relationships. Packet intervals, pulse repetition frequencies, synchronization frames, carrier timing, and symbol alignment all create observable patterns that aid reliable communications but also facilitate interception, classification, and traffic analysis.

Analog Guard® instead treats timing relationships as part of the encryption process itself. Proprietary Phase-Linked Temporal Nonlinear Modulation (PLTNM) circuitry dynamically modulates the analog-encoded data signal using one or more complex analog keys. In doing so, the system continuously alters timing relationships within the waveform through phase-related temporal shifts while also modifying waveform amplitudes and shapes.

Importantly, the waveform is not simply shifted uniformly in time. Continuously changing analog modulation processes alter the overall waveform structure, timing relationships, amplitudes, and signal geometry simultaneously.

The resulting encrypted waveform no longer exhibits stable periodic timing relationships or recognizable signal organization. This matters because timing itself contains information. Even when encrypted data remains unreadable, traffic-analysis systems can infer operational behavior by observing synchronization patterns, periodic transmission behavior, carrier stability, and temporal structure.

Analog Guard® acts to conceal not only message contents, but also recognizable behavioral characteristics of the transmission itself. The resulting signal therefore appears highly irregular, dynamically changing, broadband, and structurally difficult to classify or analyze

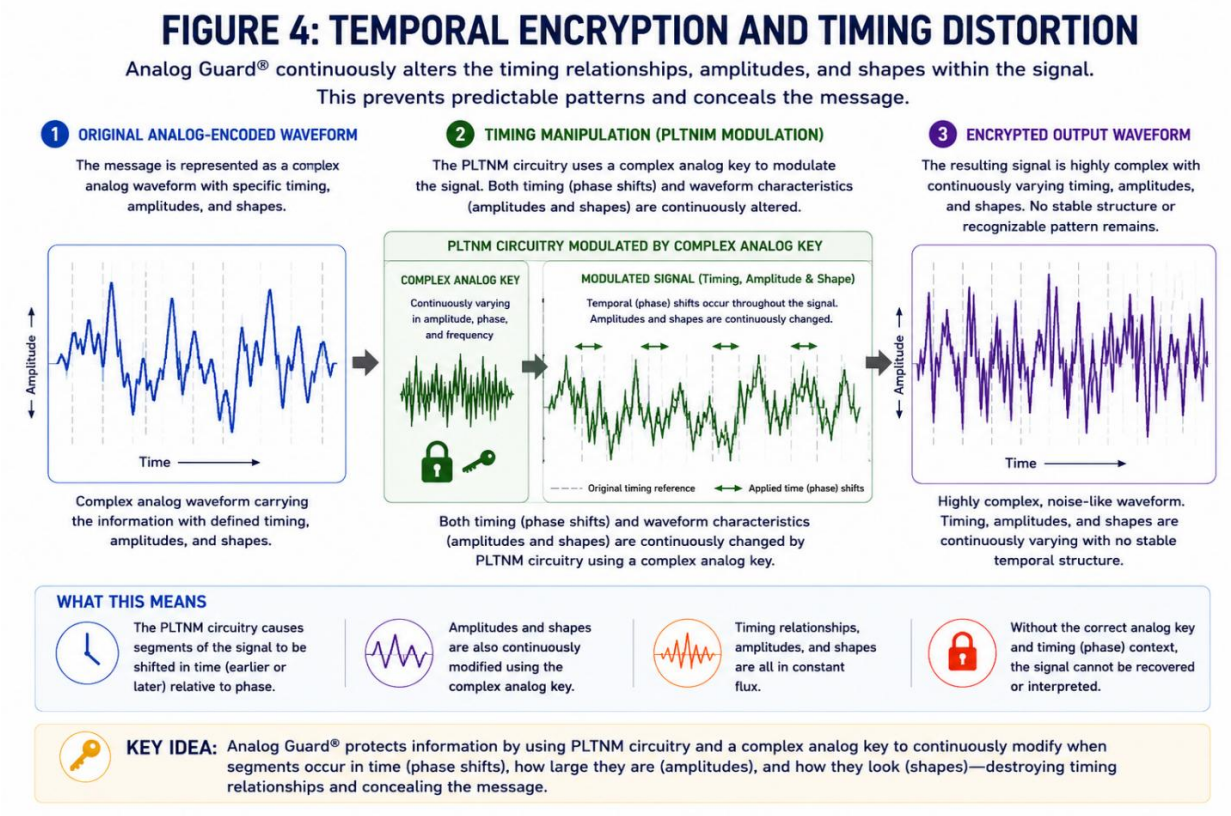

Figure 4. Temporal encryption and timing manipulation within a PLTNM processing environment.

.

6. Resonance, Phase Manipulation, and Negative Group Delay

Figure 5 conceptually illustrates how the signal is continuously transformed inside the Analog Guard® processing system.

The emphasis is not on hardware components alone, but on how signal behavior changes dynamically as it moves through the encryption environment. The system progressively reshapes waveform structure through resonance, phase manipulation, and timing-distortion processes. Each transformation alters the signal in a different way, increasing complexity while reducing recognizable structure.

The patents also introduce resonant analog circuitry and negative group delay architectures intended to further manipulate waveform timing and phase behavior.

Negative group delay is often misunderstood because it appears counterintuitive. It does not imply information traveling backward in time or violating causality. Instead, it refers to carefully engineered phase interactions in which portions of a waveform envelope can appear to emerge earlier than expected due to resonant energy redistribution and phase-slope behavior within the system.

Within Analog Guard®, these effects appear intended to increase waveform unpredictability, distort recognizable synchronization behavior, and complicate unauthorized reconstruction. The final encrypted waveform therefore becomes highly irregular, broadband, and structurally difficult to interpret.

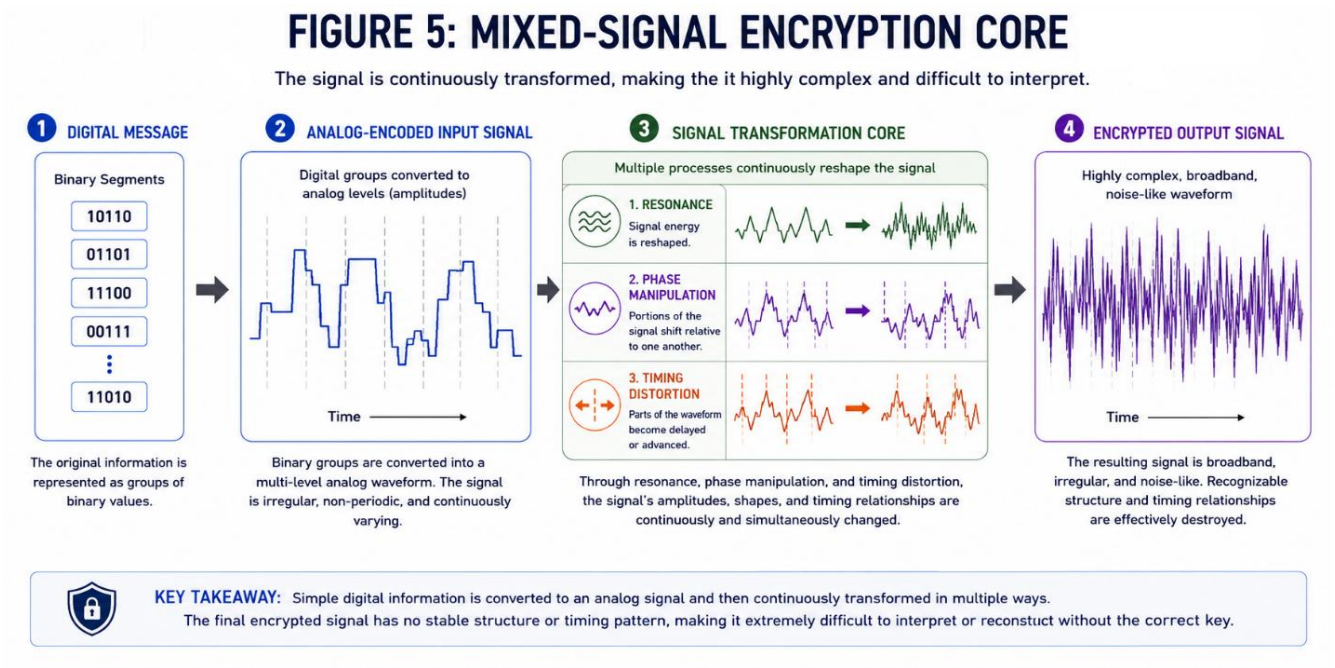

Figure 5. Continuous waveform transformation through resonance, phase behavior, and timing distortion.

7. Multidimensional Analog Transformation Domains

As the architecture scales outward, Analog Guard® can apply multiple simultaneous analog transformation processes throughout the signal environment. Rather than relying on a single modulation effect, the system continuously alters timing relationships, phase behavior, waveform amplitudes, spectral distribution, carrier characteristics, and analog signal geometry simultaneously.

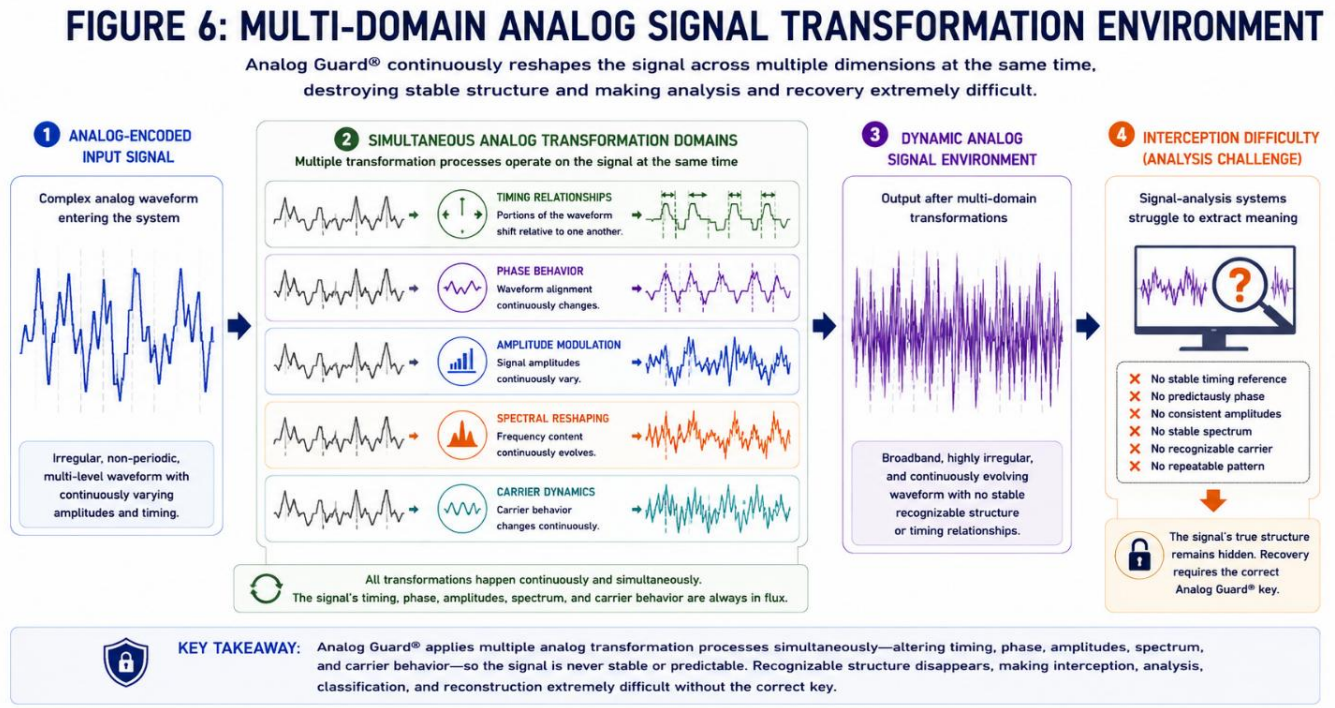

Figure 6. Multiple coordinated physical-layer transformation domains acting on the protected waveform.

Figure 6 conceptually illustrates how several coordinated analog transformation domains may operate together within the broader encryption environment. These transformations are not necessarily separate transmission channels carrying different message segments. Instead, they represent multiple interacting physical-layer modulation and signal-conditioning processes acting on the protected waveform.

The result is a signal whose behavior continuously evolves across several analog dimensions at once. This is important because modern interception and signal-analysis systems depend heavily on stability and repeatability. Predictable carrier structures, stable timing relationships, fixed modulation behavior, and recognizable spectral characteristics all make signals easier to classify and analyze.

Analog Guard® is designed to disrupt stable reference points by allowing several analog transformation mechanisms to operate simultaneously within the signal environment. The protected information therefore no longer exists inside a stable and easily recognizable transmission structure. Instead, the waveform becomes a continuously evolving analog process whose timing, phase relationships, amplitudes, carrier dynamics, and spectral behavior remain in flux.

This creates a different security model from conventional digital encryption systems. Rather than protecting information solely through computational complexity, Analog Guard® distributes protection throughout the physical behavior of the signal itself.

8. Matched Analog Reconstruction and Recovery Failure

Figure 7 illustrates one of the invention's most important characteristics: successful decryption depends not only on possessing the correct key relationship, but also on reproducing the correct physical analog environment.

If the receiver successfully reproduces the proper analog conditions, the encrypted waveform can collapse back into recoverable information. If the analog conditions are incorrect, the recovered signal deteriorates into distortion and noise.

The patent materials describe experimental behavior in which matched analog conditions allow recovery while mismatched conditions fail to reconstruct the original signal accurately. Spectral analysis also shows that the encrypted waveform becomes redistributed and noise-like compared to the original transmission.

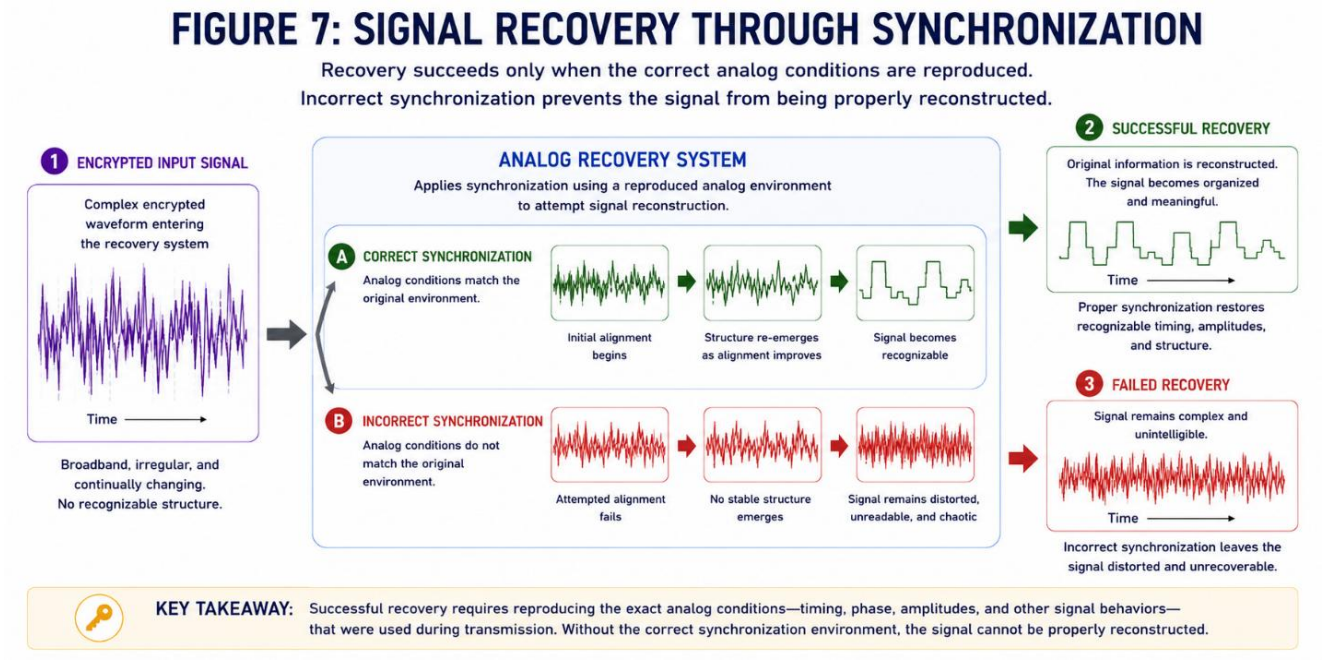

Figure 7. Matched analog conditions support recovery; mismatched conditions produce reconstruction failure.

9. Strategic Implications

This low-observability property may represent one of the technology's strategically significant implications. In many modern encrypted systems, the message contents are hidden while the transmission itself remains visible and classifiable. Analog Guard® is directed to concealing both the information and the recognizable structure of the signal carrying it.

That places the architecture in a technological space spanning cybersecurity, advanced communications engineering, signal intelligence, electromagnetic spectrum operations, and electronic warfare.

The central design implication is that future secure communications may need to protect the signal environment, not merely the message payload. Carrier behavior, timing relationships, resonance, modulation dynamics, phase interactions, and analog signal physics can all become components of the security architecture.

10. Conclusion

Analog Guard® proposes a different philosophy of information protection. Rather than assuming that security exists only within software algorithms, the architecture treats the waveform itself as part of the protected object. Carrier behavior, timing relationships, resonance, modulation dynamics, phase interactions, and analog signal physics become integral components of the encryption process.

In that sense, the technology is not merely another encryption algorithm. It proposes a broader shift in how secure communications may be designed: protection emerges not solely from mathematics, but from the controlled complexity of physical signal behavior itself.

The approach should be understood as complementary to strong cryptography, secure hardware, authentication protocols, and post-quantum migration efforts. Its distinct contribution is the extension of trust and protection into the physical-layer mixed-signal environment where information is carried, transformed, and ultimately reconstructed.

Appendix A. Figure Inventory

Figure	Working Title	Purpose
1	Dynamic Analog Signal Environment	Transmission concealed within a continuously evolving analog environment.
2	Binary-to-Analog Conversion and Dynamic Carrier	Binary information converted into analog waveform behavior before encryption.
3	Parallel Analog-Encrypted Paths	Independent signal paths remain separate until receiver-side recovery and binary reconstruction.
4	Temporal Encryption and PLTNM	Phase-linked temporal modulation alters waveform timing, amplitude, and signal geometry.
5	Resonance and Timing Distortion	Signal behavior changes through resonant, phase, and timing-related transformations.
6	Multidimensional Transformation Domains	Multiple coordinated physical-layer transformations act on the protected waveform.
7	Matched Reconstruction Environment	Recovery depends on reproducing the correct analog reconstruction conditions.

Appendix B. Key Terms

Term	Working Meaning in This White Paper
Analog Guard®	A mixed-signal physical-layer encryption architecture that uses analog waveform behavior as part of the protection mechanism.
Dynamic carrier	A carrier environment whose behavior participates in encryption rather than merely transporting encrypted bits.
PLTNM	Phase-Linked Temporal Nonlinear Modulation; a modulation approach that alters timing, phase, amplitude, and waveform geometry through analog processes.
Analog-state environment	The carrier, timing, phase, resonance, waveform, and modulation conditions that influence recoverability.
Negative group delay	A phase-related signal effect in which waveform envelope behavior can appear advanced without implying causality violation.
Matched analog reconstruction	Recovery condition in which the receiver reproduces the analog environment needed to recover the protected information.
Low observability	Reduced recognizability of the transmission's structure, timing, carrier behavior, spectral features, or modulation patterns.