Analog Guard®

A Physical-Layer Approach to Signal Encryption

From One Foundational Patent to Two Patent Expansions

Core thesis	Analog Guard® began with a single foundational patent — U.S. Patent No. 12,126,720 — covering a dynamic-carrier method for encrypting signals in the analog domain. Two later patents build on that foundation without replacing it: one changes how the signal and key are combined, and the other adds a second key and a more advanced two-stage architecture. This article explains what each patent actually covers and how the three relate to one another.

Prepared for	Investors, engineers, and technical partners evaluating Analog Guard's technology — including readers in aerospace, cybersecurity, and secure-communications fields
Prepared by	Analog Guard, Inc.
Source series	Analog Guard Foundational IP Article Series
Date	September 2026

Document Profile

Item	Description
Subject	What this article covers, and how the patent family expanded from it.
Foundational patent	U.S. Patent No. 12,126,720 — the original invention. It uses an analog key to shape ("modulate") a carrier signal, then mixes the message into that key-shaped carrier.
Direct continuation	U.S. Patent No. 12,689,512 — claims a different order of operations: the reference signal and message are combined first, and the key modifies that combination.
CIP-derived patent	U.S. Patent No. 12,615,149 — claims a two-key, two-stage architecture in which the signal passes through two separate key-controlled processing stages in sequence.
How to read this article	Every section says plainly which patent (or which shared disclosure) a given concept belongs to, so ideas that appear in more than one patent aren't mistaken for something unique to just one of them.

Executive Summary

Most cybersecurity today works by scrambling data mathematically, in software, after it has already been converted to bits. Analog Guard® takes a different approach: it encrypts the signal itself, while it is still an analog waveform, before it is ever transmitted or stored. This is often called physical-layer or mixed-signal security, and it adds a layer of protection that operates underneath conventional digital encryption rather than replacing it.

That idea is protected by a family of three related U.S. patents, developed in stages. Reading the family correctly means keeping two distinctions straight: which patent's claims actually require a given feature, and which material is simply shared background that all three patents draw on.

U.S. Patent No. 12,126,720 is the foundation. In its core claimed method, an analog key first shapes ("modulates") a carrier wave to produce what the patent calls a dynamic carrier. The message signal is then mixed into that dynamic carrier. Both the message and the key begin at the same point in time, and a matching receiver — using the same key, the same carrier relationship, and the same timing — reverses the process to recover the original message.

The original patent's specification describes much more than that core method, though. It also lays out a broader toolkit: circuits for adding controlled nonlinear distortion (PLTNM), ways to represent digital data as analog signals, techniques for splitting a signal across parallel or sequential paths, masking signals, and worked examples comparing correct versus incorrect decryption keys. All of that material is part of the original patent's disclosure, even though the patent's main claim doesn't require every one of these features to be present.

The two later patents each stake out a distinct claim. U.S. Patent No. 12,689,512, a direct continuation of the original application, claims a different sequence: instead of shaping the carrier with the key first, it combines a reference signal with the message first, and the key then modifies that combined signal. U.S. Patent No. 12,615,149, which descends from a continuation-in-part filing, claims a more elaborate architecture: two separate keys, each controlling its own signal-processing stage, connected in sequence and kept in sync by a controller; its supporting disclosure also adds detailed circuitry and worked examples for encrypting and decrypting entire files, not just live signals. Put simply: one invention, three patents, each protecting a different piece of the architecture — the original method, a different way of combining the same ingredients, and a more complex two-key version with the file-processing details needed to apply it to stored data.

Key Takeaways

- Patent 12,126,720 is the original invention: an analog key shapes a carrier wave, and the message is then mixed into that shaped carrier.
- Several supporting techniques — PLTNM circuitry, parallel signal paths, analog encoding of digital data, and the matched-versus-mismatched-key examples — appear in the original patent's disclosure. They are not inventions introduced later by the CIP.
- Patent 12,689,512 claims a different processing order: the reference signal and message combine first, and the key modifies that combination afterward.
- Patent 12,615,149 claims a two-key, two-stage architecture, with each key controlling its own processing stage and a controller keeping both stages synchronized.
- The CIP branch's added disclosure covers detailed circuit control, bit-level encoding, and full file encryption and decryption — going beyond the live-signal focus of the original patent.
- Every figure in this article is labeled with the patent (or patents) it illustrates, so a concept shared across the family isn't mistaken for something exclusive to one claim.

Contents

1 How the Patent Family Fits Together

The Analog Guard® patents share a common technical foundation but stake out three distinct claims. Reading them accurately takes two steps: first, separate the original invention from the two later claim expansions; second, separate material that was already in the original patent's specification from material the CIP branch added for the first time.

U.S. Patent No. 12,126,720 is the original patent. Its core method uses an analog key to shape a carrier wave into what the patent calls a dynamic carrier, then mixes the message signal into that carrier. The message, the key, and the resulting encrypted signal all share a defined starting point in time. A receiver decrypts the signal by reproducing the same carrier, the same key, the same processing steps, and the same timing.

U.S. Patent No. 12,689,512 is a direct continuation — a later application built on the same underlying disclosure as the original patent, but pursuing different claims. Its main claim changes the order of operations: rather than shaping the carrier with the key first, it combines a reference signal with the message first, and the key then modifies that combination. It is a new claim on familiar territory, not a new invention with its own separate drawings.

U.S. Patent No. 12,615,149 comes from the continuation-in-part (CIP) branch. It claims a different internal architecture altogether: two signal-processing stages in sequence, each shaped by its own analog key, kept synchronized by a controller. The CIP branch also added substantial new disclosure — detailed circuit control, file encryption and decryption workflows, and device-level implementations — that goes beyond what the original patent describes.

Patent	What It Actually Claims	What It Doesn't Mean
Original patent, 12,126,720	The key shapes the carrier first; the message is mixed in afterward. Decryption reverses this with a matching key and timing.	Later features described in this article aren't automatically part of this patent's claims just because they build on its disclosure.
Shared foundational disclosure	PLTNM circuitry, analog encoding of digital data, parallel and serial signal paths, masking signals, and matched-versus-mismatched-key examples — all described in the original patent.	Appearing early in the family's disclosure doesn't mean a concept is required by every patent's claims.
Direct continuation, 12,689,512	Combines the reference signal and message first; the key then modifies that combined signal. Includes matching decryption claims.	Shouldn't be illustrated using the original patent's carrier-first diagram — the order of operations is genuinely different.
CIP-derived patent, 12,615,149	Two cascaded signal-processing stages, each controlled by its own key, synchronized by a controller; the stages can be inverses of each other for decryption.	The two-key cascade is new to this patent — it isn't part of the original patent's main claim.
CIP's added disclosure	Detailed dynamic control circuitry, bit-level file encoding, and full file encryption and decryption workflows.	Describing every added embodiment doesn't mean every one of them is required by every claim in this patent.

CONTINUATION PATENTS EXPAND TWO DIFFERENT PARTS OF THE ARCHITECTURE

The direct continuation changes the claimed carrier-combining relationship; the CIP branch adds a two-key cascaded transfer environment.

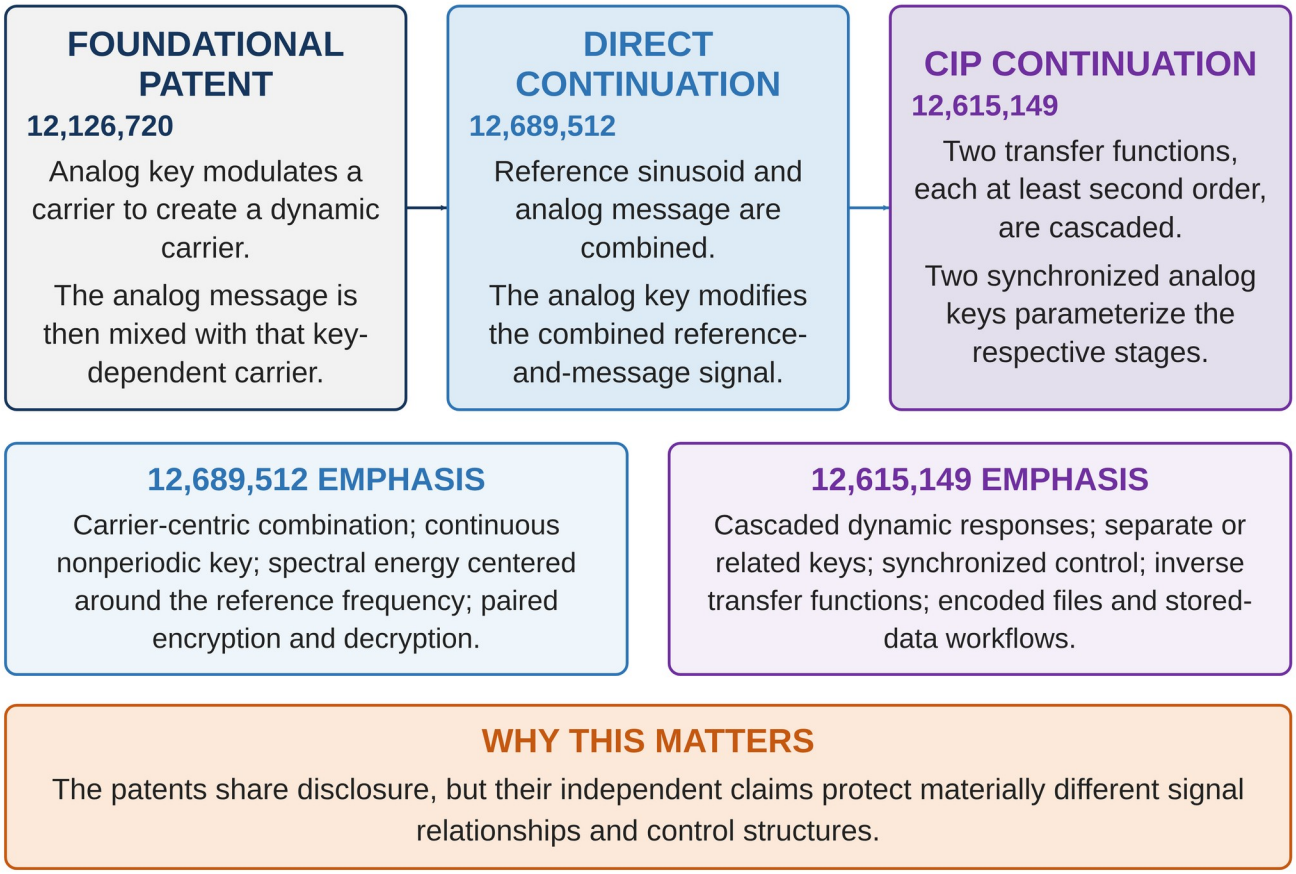


Figure 1. How the three patents relate: the original claim, the direct-continuation claim, and the CIP-derived claim, each shown against the disclosure they draw on.

2 The Original Patent: Building a Dynamic Carrier

Patent 12,126,720 starts with two inputs: a finite analog message and a finite analog key at least as long as the message. Both can be a naturally analog signal, or a digital signal that has been converted into an analog representation. A carrier wave is generated at a fixed center frequency.

The analog key is applied to that carrier first, before the message ever enters the picture. Depending on the specific implementation, the key can vary the carrier's frequency, phase, amplitude, or timing. The result — the patent calls it a dynamic carrier — behaves less like a fixed reference tone and more like a carrier whose exact state, moment to moment, depends on the key.

Only after the dynamic carrier is formed does the message get mixed in. The patent's primary example uses multiplication for this mixing step, though it also describes additive and other nonlinear approaches. The result is an encrypted analog signal that looks noise-like on the surface, but is fully deterministic and — with the correct key — fully reversible.

That order matters for reading the patent family correctly: key shapes carrier first, message mixes in second. That is the sequence the original patent's main claim actually requires, and it is worth keeping visually and verbally distinct from Patent 12,689,512's different sequence, described in Section 5.

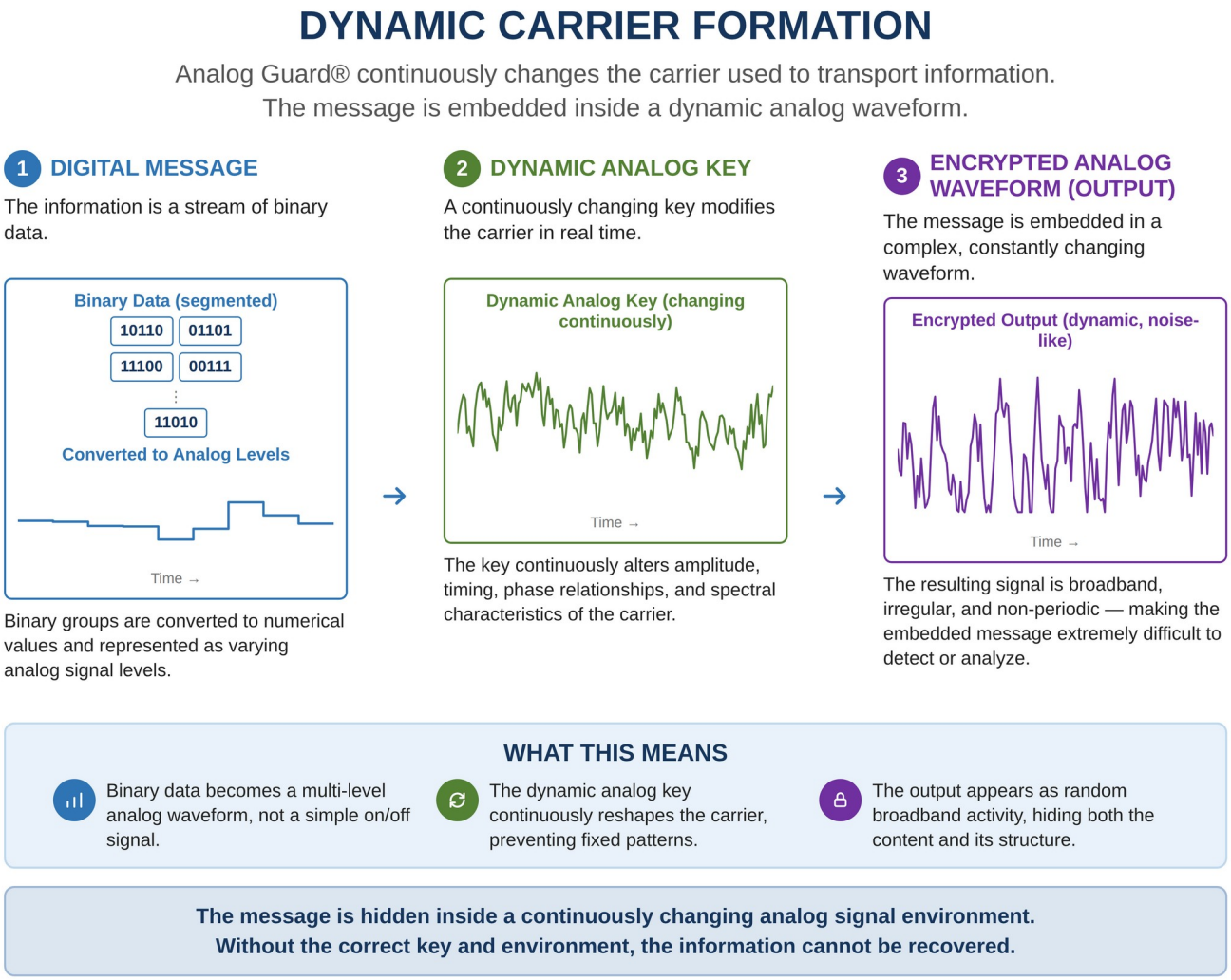


Figure 2. How the original patent builds a dynamic carrier: the key shapes the carrier first, then the message is mixed in. This is a conceptual overview, not every implementation variant in the patent.

3 The Original Patent: Timing, Synchronization, and Recovery

Timing isn't a side detail in this patent — it's part of what the claim actually requires. The message and the key both have a defined starting point, and encryption begins at the moment those two starting points align. The receiver has to reproduce that same alignment to decrypt successfully.

This is what makes an otherwise-correct key unusable if it's applied at the wrong moment: a delay, a drift in clock timing, a phase error, or a resampling mismatch effectively pairs the right key with the wrong part of the signal — which behaves, for practical purposes, like using the wrong key entirely.

On the receiving end, decryption works by generating the same dynamic carrier, applying the same key, and reproducing the same timing relationship, then running the encrypted signal back through the corresponding mixing and filtering steps. Getting the message back cleanly depends on all of these lining up: the key waveform, the carrier parameters, the processing steps, and the synchronization. Real-world components and communication channels add their own tolerances on top of that.

The original patent includes worked examples — in the time domain, the frequency domain, and using metrics like signal coherence, phase, and bit-error rate — comparing what happens with a correctly matched key versus a mismatched one. These examples illustrate the underlying principle; they aren't a performance guarantee for every possible implementation, since real results depend on the specific signal bandwidth, key design, channel conditions, converters, and circuitry involved.

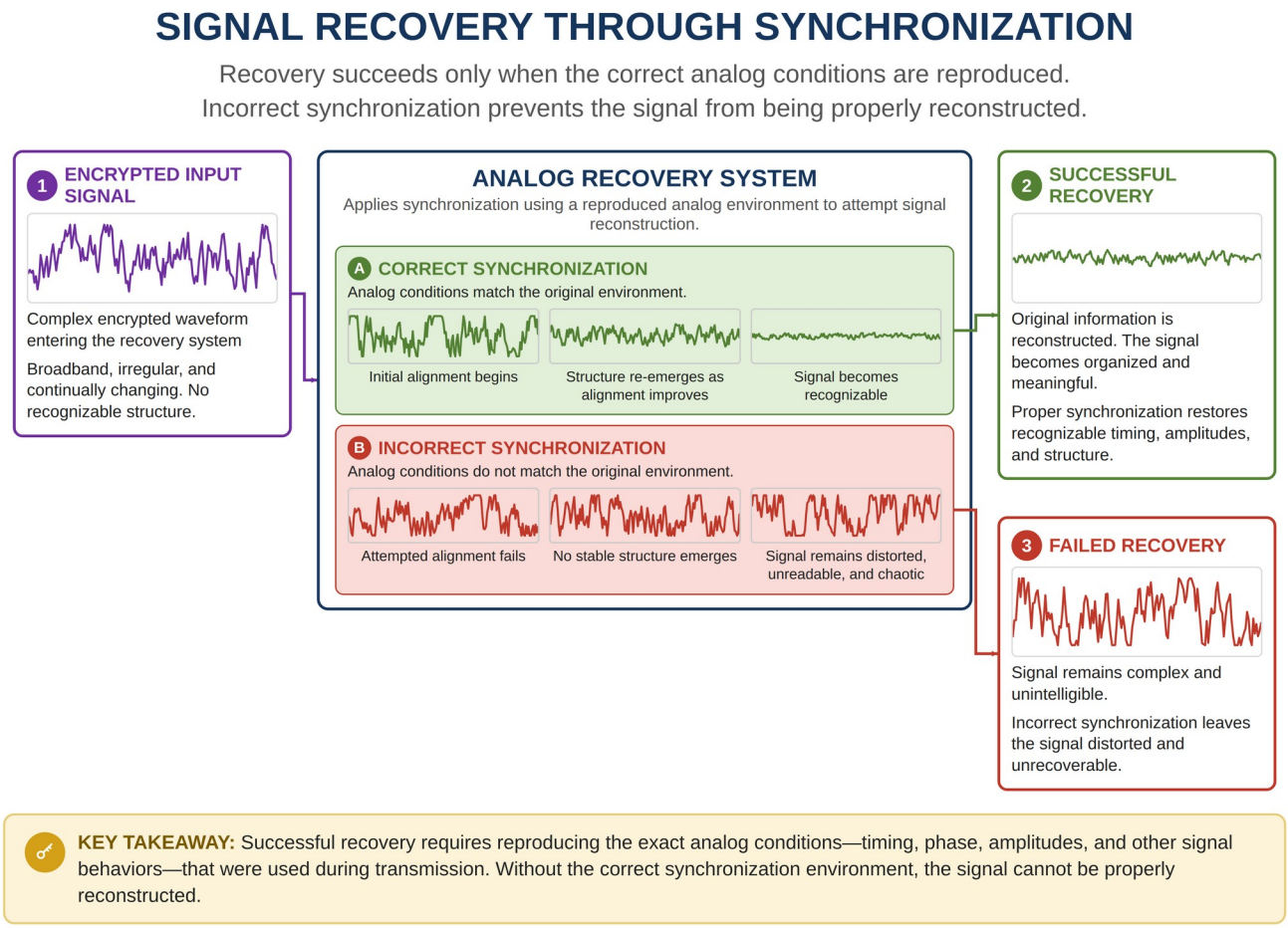


Figure 3. Recovering the message depends on matching the key, the carrier, and the timing at the receiver. This shared principle underlies both the original patent and its later continuations.

4 The Original Patent: A Broader Technical Toolkit

The original patent's specification describes considerably more than its main claimed method. It's worth walking through this broader toolkit directly, both because it's useful engineering context and because later sections of this article need to point back to it: several of these ideas are sometimes mistakenly credited to the CIP branch, when in fact they were already part of the original disclosure.

Digital information can be converted into an analog signal before encryption, using any of several standard encoding schemes — unipolar, polar, bipolar, phase-shift, frequency-shift, or quadrature-amplitude encoding. A signal made of several parallel data streams or frequency bands can be split across separate analog processing paths and recombined after decryption, then converted back to digital form.

The patent also describes PLTNM — phase-linked temporal nonlinear modulation — a family of circuits that add key-controlled, nonlinear behavior to a signal's magnitude, phase, and timing. Some of these circuits exhibit what the patent calls negative group delay. That term sounds like it implies information moving backward in time, but it doesn't: it describes a real, causal circuit response in which the shape of the output and its phase behavior make certain signal features appear to shift in time, without violating causality.

The original specification's Figures 25 through 28 show how PLTNM stages and the ADM (analog dynamic modulation) technique described elsewhere in the patent can be applied in parallel, across multiple bands, or in series. The CIP branch later develops these ideas in more circuit-level detail — but it didn't originate the underlying parallel-path or PLTNM concepts; those were already in the original patent.

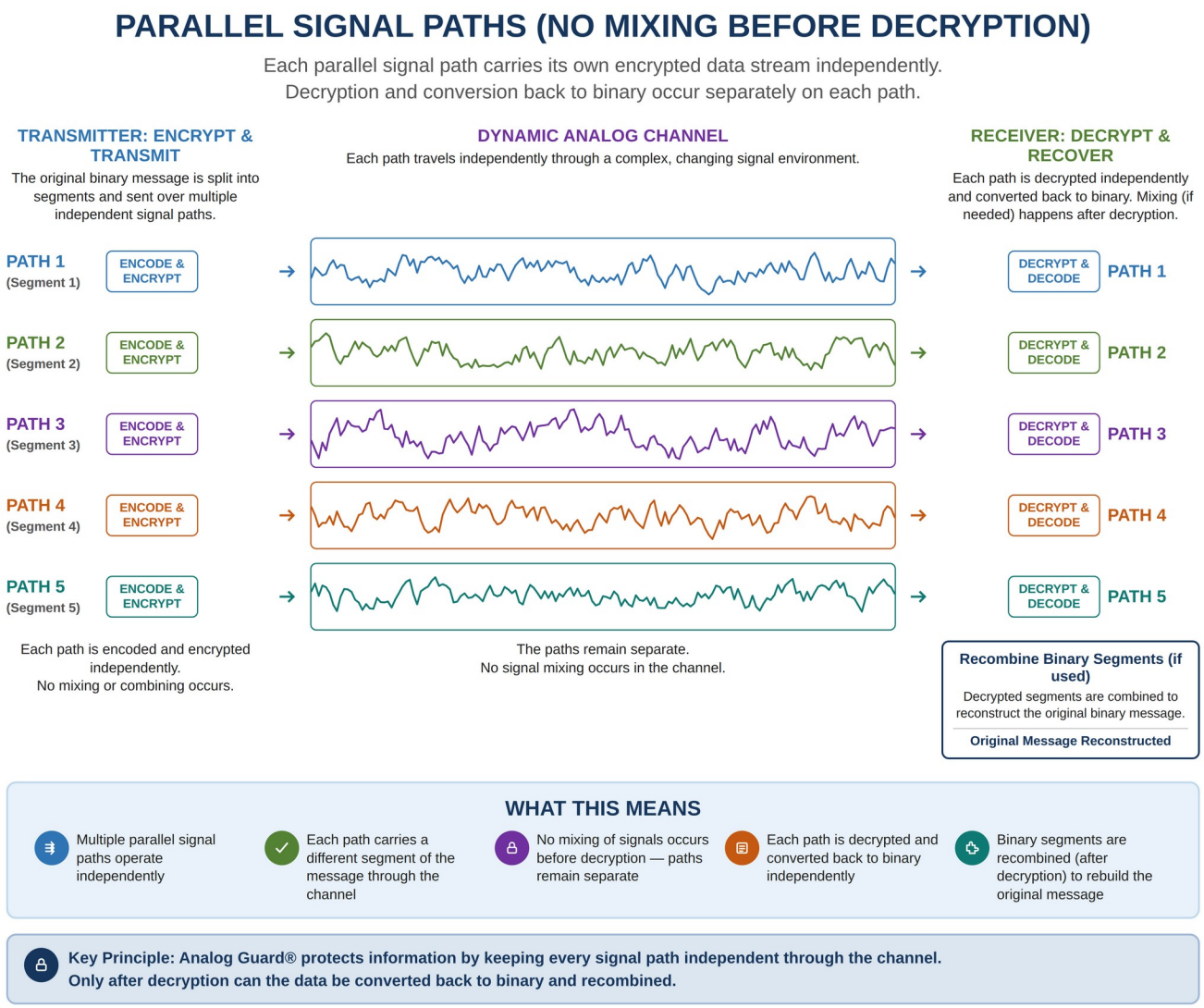


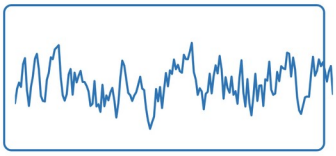
Figure 4. Parallel signal paths, as described in the original patent's shared disclosure. The CIP branch later develops related multi-path and file-processing implementations, but this technique isn't unique to the CIP.

TEMPORAL ENCRYPTION AND TIMING DISTORTION

Analog Guard® continuously alters the timing relationships, amplitudes, and shapes within the signal. This prevents predictable patterns and conceals the message.

1 ORIGINAL ANALOG-ENCODED WAVEFORM

The message is represented as a complex analog waveform with specific timing, amplitudes, and shapes.



Complex analog waveform carrying the information with defined timing, amplitudes, and shapes.

2 TIMING MANIPULATION (PLTNM MODULATION)

The PLTNM circuitry uses a complex analog key to modulate the signal. Both timing (phase shifts) and waveform characteristics (amplitudes and shapes) are continuously altered.

PLTNM CIRCUITRY MODULATED BY COMPLEX ANALOG KEY

COMPLEX ANALOG KEY

Continuously varying in amplitude, phase, and frequency

MODULATED SIGNAL (Timing, Amplitude & Shape)

Temporal (phase) shifts occur throughout the signal. Amplitudes and shapes are continuously changed.

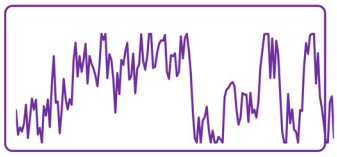
Original timing reference

Applied time (phase) shifts

Both timing (phase shifts) and waveform characteristics (amplitudes and shapes) are continuously changed by PLTNM circuitry using a complex analog key.

3 ENCRYPTED OUTPUT WAVEFORM

The resulting signal is highly complex with continuously varying timing, amplitudes, and shapes. No stable structure or recognizable pattern remains.



Highly complex, noise-like waveform. Timing, amplitudes, and shapes are continuously varying with no stable temporal structure.

WHAT THIS MEANS

- The PLTNM circuitry causes segments of the signal to be shifted in time (earlier or later) relative to phase.
- Amplitudes and shapes are also continuously modified using the complex analog key.
- Timing relationships, amplitudes, and shapes are all in constant flux.
- Without the correct analog key and timing (phase) context, the signal cannot be recovered or interpreted.

KEY IDEA: Analog Guard® protects information by using PLTNM circuitry and a complex analog key to continuously modify when segments occur in time (phase shifts), how large they are (amplitudes), and how they look (shapes)—destroying timing relationships and concealing the message.

Figure 5. PLTNM's effect on timing and waveform shape, as described in the original patent. The CIP branch develops the underlying circuitry in more detail, but the concept itself originates here.

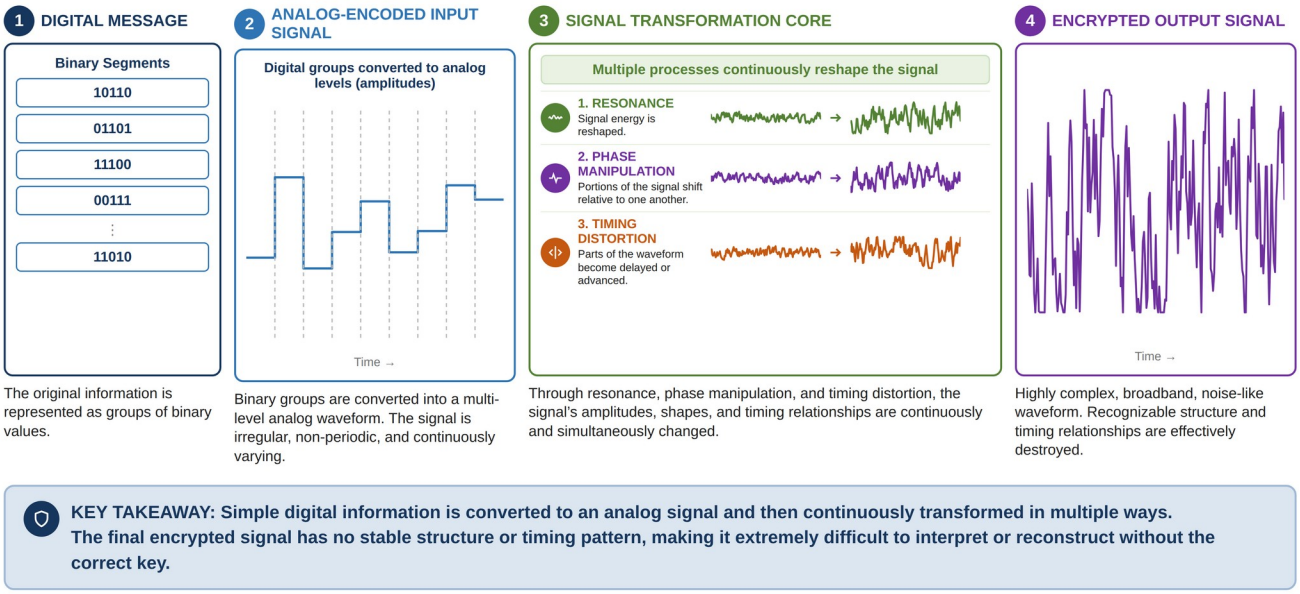


Figure 6. A conceptual view of analog encoding and signal transformation working together, drawn from the family's shared disclosure rather than any one specific claim.

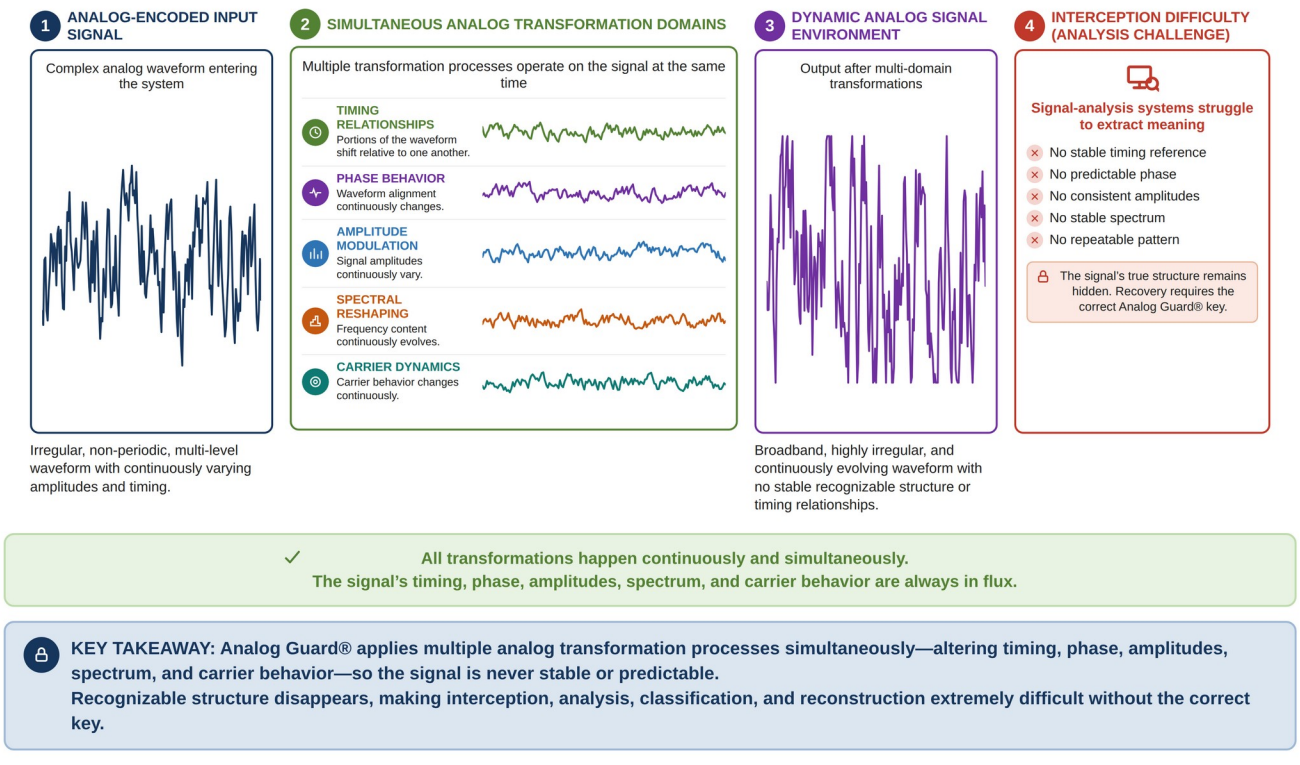


Figure 7. A conceptual view of the family's multi-domain signal transformation approach — again, shared disclosure rather than a requirement of any single claim.

5 The Direct Continuation: Combining the Signal First

Patent 12,689,512 is a direct continuation of the original application: it relies on the same underlying technical disclosure and the same drawings. What's new is the claim itself. Claim 1 works like this: an analog message and an analog key begin at the same moment in time; a reference sinusoidal signal is generated; that reference signal and the message are combined by a "first combiner"; and the analog key then modifies the combined signal, in a way that keeps the signal's energy centered on the reference frequency.

That's a genuinely different sequence from the original patent's. Patent 12,126,720 has the key shape the carrier before the message ever enters the picture. Patent 12,689,512 has the reference and message combine first, with the key applied to that combination afterward. Because the order of operations is different, this patent deserves its own diagram rather than being illustrated with the original carrier-first figure — even though both patents operate in the same general carrier-centric, analog world.

The dependent claims fill in more detail: the combiner can be a mixer or a multiplier; the key's modification can take the form of phase, frequency, or amplitude modulation; the reference frequency runs higher than the key's own frequency range; and the key itself can be non-periodic and continuous.

None of this changes the underlying toolkit. Because this is a direct continuation, it still relies on the same PLTNM circuitry, parallel-path techniques, analog encoding methods, and matched-key recovery principles described in the original patent. It's a new claim on the same technical foundation, not a separate platform.

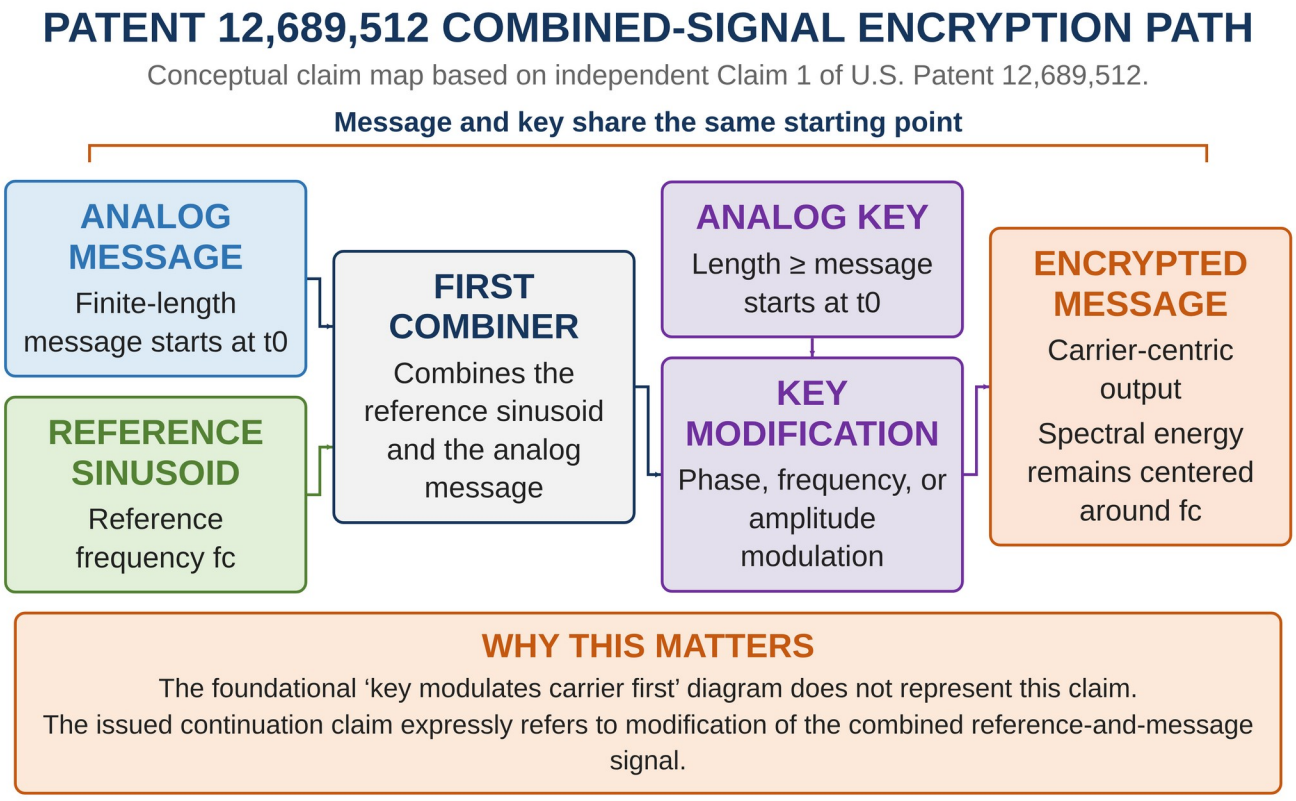


Figure 8. Patent 12,689,512's claimed sequence: the reference signal and message combine first, and the analog key modifies that combined signal afterward.

6 The Direct Continuation: Decryption and Its Boundaries

Patent 12,689,512 also claims a matching decryption method. The receiver takes in the encrypted analog signal along with a key that corresponds to the encryption key, generates its own reference sinusoidal signal, combines that reference with the encrypted signal, applies the same key-based modification, and outputs the decrypted message.

As with the original patent, timing carries real weight here. The key behaves as a continuous, time-varying signal, and recovering the message correctly means using the right segment of that key at the right moment — together with the matching reference-and-combiner processing.

It's worth being precise about what this continuation does and doesn't do: it doesn't replace the original patent. The two patents describe related but genuinely different carrier-centric processing relationships. The original patent remains the foundation for the key-shapes-carrier-first approach; the direct continuation adds a separate, combine-first claim alongside it.

7 The CIP-Derived Patent: A Two-Key Cascade

Patent 12,615,149 comes from the continuation-in-part branch, and it claims a meaningfully different internal architecture. The signal going in can be either an unencrypted message (for encryption) or an encrypted message (for decryption). Alongside it, two separate analog keys are received, each with its own defined starting point and length.

The incoming signal is processed through two transfer functions in sequence — first one, then the other — and each of those two stages has at least a second-order response (meaning it's complex enough to shape both magnitude and phase, not just scale the signal up or down). The first key controls the first stage; the second key controls the second stage. A controller keeps everything synchronized, aligning the start of the incoming signal with the start of both keys.

The dependent claims broaden this considerably. The two keys can be entirely distinct from each other, related in some defined way, or set up as exact inverses of one another. Either key can be converted into a dynamic control signal that governs the stage it drives. And the second transfer function can be built as the mathematical inverse of the first — which is exactly what makes end-to-end decryption possible: run the signal back through the inverse stages, using matching keys, and it comes out the other side as the original message.

This two-key cascade is the heart of what this patent claims, and it isn't something the original patent's main claim covers. At the same time, it isn't built from nothing — it draws on the same underlying toolkit described earlier in this article: PLTNM circuitry, key-controlled analog stages, synchronization, and matched-key recovery.

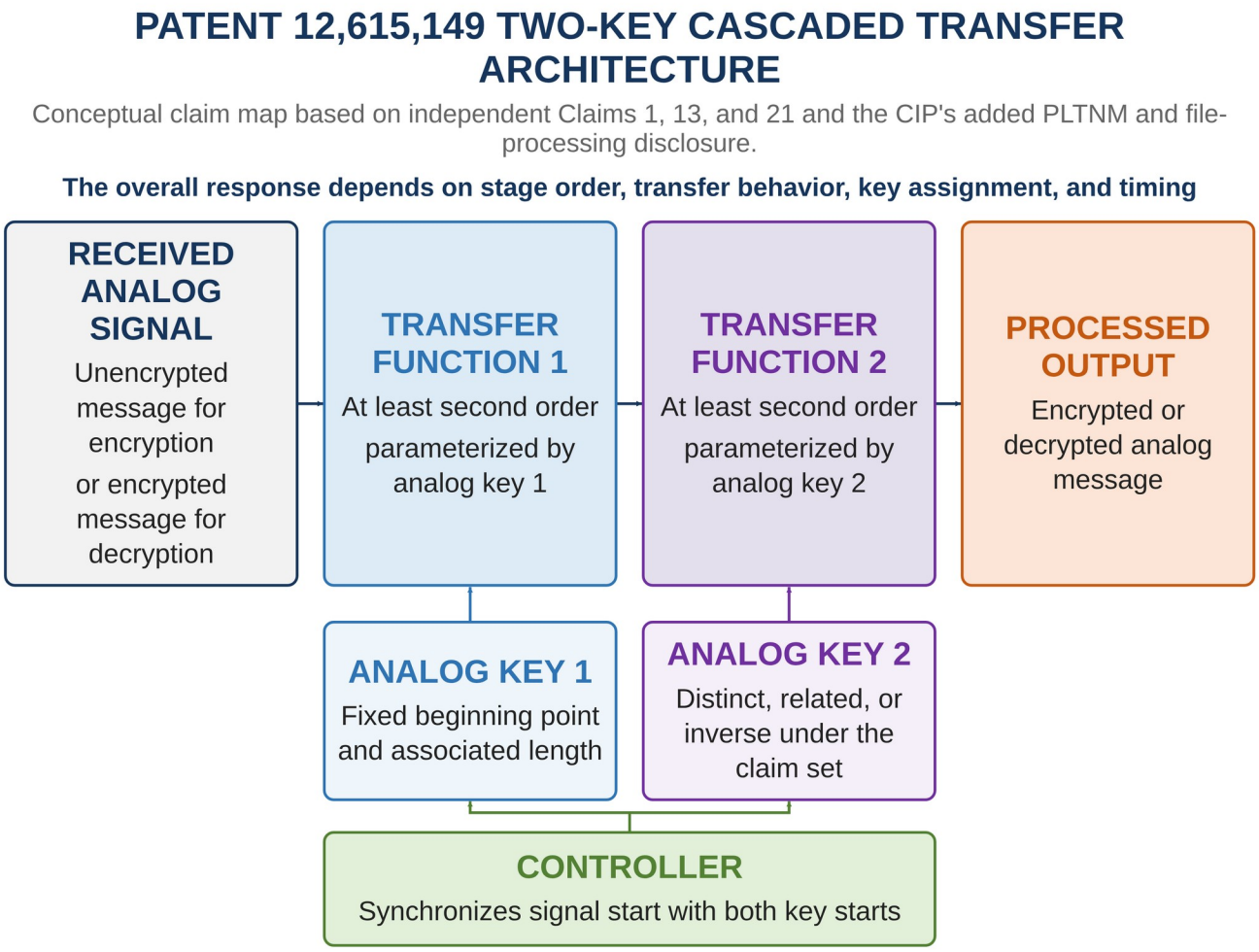


Figure 9. Patent 12,615,149's claimed architecture: two analog keys, each driving its own transfer-function stage, with a controller keeping both stages synchronized to the incoming signal.

8 The CIP-Derived Patent: Control and File Processing

The continuation-in-part disclosure doesn’t stop at the two-key architecture — it adds a substantial amount of new material, corresponding to Figures 58 through 87 in the patent. This includes detailed PLTNM circuit behavior, dynamic baseband control signals, ways to control multiple variable circuit elements independently or together, complete file encryption and decryption workflows, bit-level signal encoding, worked examples comparing matched and mismatched file recovery, and device-level implementations.

A key can drive a transfer function's response directly, or it can first be converted into a dynamic baseband control signal that then drives the response — the added disclosure includes plots showing exactly how that control signal changes magnitude, phase, and group delay over time. With two independent keys available, they can each govern a separate processing stage, or separate individual controllable elements within a stage — which multiplies the number of relationships that have to be reproduced correctly to recover the original signal.

For stored files specifically, the added disclosure describes converting digital source data into an analog waveform, running that waveform through the key-controlled two-stage core, and then digitizing the result for storage or transport as an encrypted file. Decryption reverses each of those steps: the encrypted file is converted back to analog, run through the corresponding inverse stages with synchronized keys, and decoded back into the original digital data.

Bit segmentation — grouping bits together and mapping each group to a specific analog signal level — is part of how digital files get converted to and from analog form in this process. Beyond that, a file or signal can be split across independently processed parallel paths, or run through successive transformations in series. These are implementation options the CIP disclosure describes in detail; they expand what the system can do without changing the more basic point made throughout this article — that a feature being disclosed somewhere in the patent family doesn't automatically mean it's required by any one particular claim.

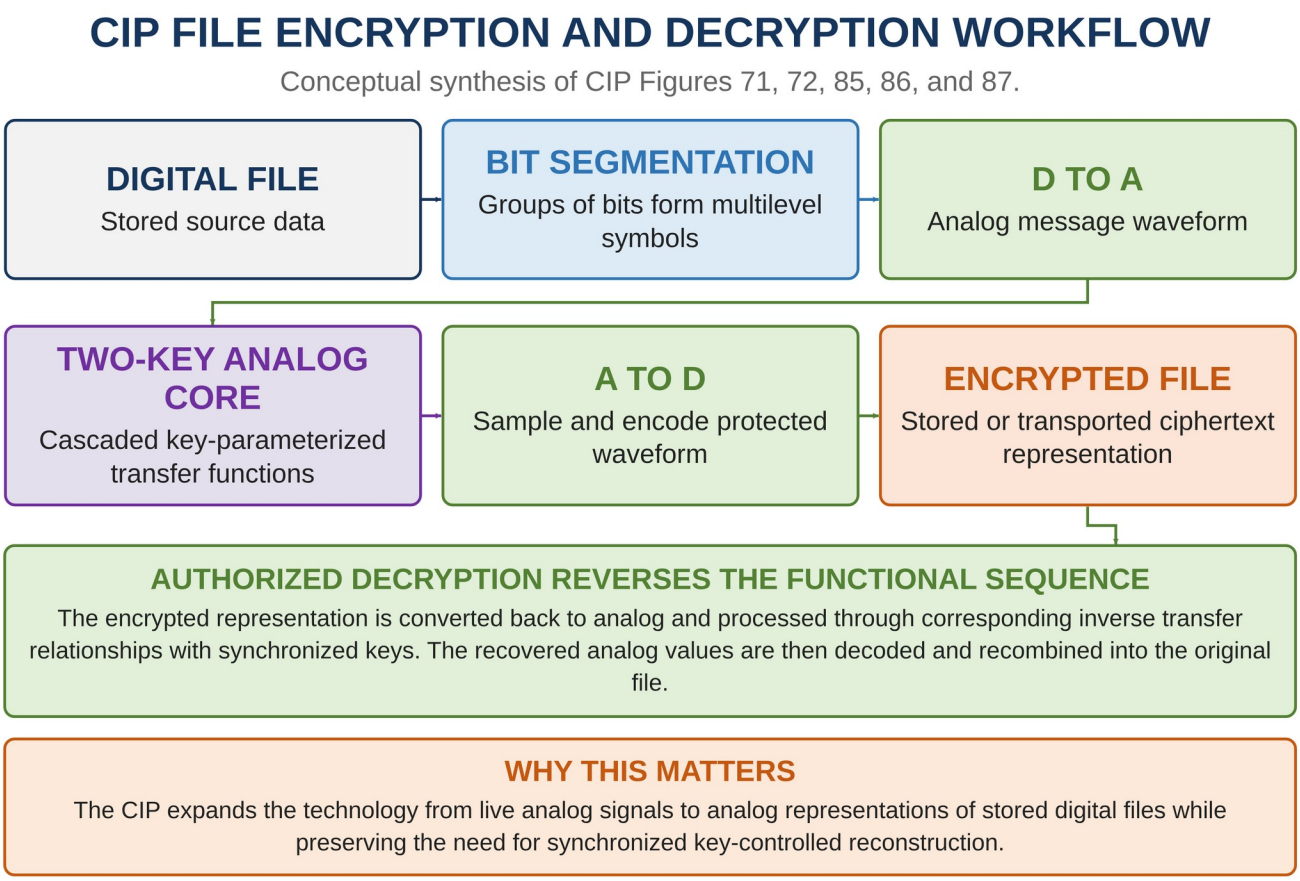


Figure 10. The CIP-derived patent's file encryption and decryption workflow, based on the added Figures 71, 72, 85, 86, and 87.

9 Shared Concepts, Separate Claims

Because all three patents come from the same underlying research, they naturally share a lot of vocabulary: analog keys, synchronization, PLTNM, analog representations of digital data, matched reconstruction, parallel paths, and carrier-centric processing all show up across the family. The distinction that actually matters isn't whether a term shows up in more than one document — it will. What matters is where a concept was first disclosed, and, separately, exactly what each patent's issued claims require.

In short: the original patent claims a key-shaped dynamic carrier with the message mixed in afterward. The direct continuation claims a combine-first sequence, with the key applied to the combined signal. The CIP-derived patent claims a two-key, two-stage cascade. All three draw on shared disclosure, but each patent's claims define a different legal boundary.

Concept	Original Patent (12,126,720)	Direct Continuation (12,689,512)	CIP-Derived Patent (12,615,149)
Order of operations	Key shapes the carrier; message mixes in afterward.	Reference and message combine first; key modifies the result.	Not part of this patent's main claim — it's a two-stage cascade instead.
Number of keys	At least one analog key, required by the main claim.	One analog key, synchronized with the message.	Two analog keys, one per processing stage.
Signal processing	Nonlinear and PLTNM-based approaches are described.	Builds on the same disclosure; supports nonlinear implementations.	Two second-order-or-higher transfer functions are explicitly claimed.

Concept	Original Patent (12,126,720)	Direct Continuation (12,689,512)	CIP-Derived Patent (12,615,149)
Synchronization	Message and key share a coordinated starting point.	Message and key start at the same time.	A controller synchronizes the incoming signal with both keys.
Parallel paths	Described in the original specification.	Part of the shared disclosure, not a defining feature of this claim.	Further developed here for both signal and file processing.
File processing	Basic digital-to-analog encoding concepts are described.	Not a defining feature of this continuation's claim.	Fully developed here: file-level encryption, decryption, segmentation, storage, and device workflows.

10 What This Means Strategically and Technically

The value of this patent portfolio comes from covering several related physical-layer, mixed-signal approaches rather than just one. The original patent protects the foundational dynamic-carrier method. The direct continuation protects a different way of combining the same basic signal, key, and reference. The CIP-derived patent protects a more advanced two-key architecture, along with the file- and device-level work needed to actually use it on stored data.

That range of coverage supports a correspondingly wide range of applications — live communications, embedded hardware, sensor links, and stored-data systems — without the portfolio being reducible to a single mixer circuit or technique. It also comes with real engineering obligations: any practical system built on this technology has to handle key generation and distribution, precise timing, converter performance, available bandwidth, component tolerances, calibration, signal integrity, authentication, and secure operation of the physical device itself.

It's worth being clear-eyed about what patent coverage does and doesn't establish: owning the intellectual property doesn't by itself guarantee a particular level of real-world security. That has to be evaluated separately, and should account for how sensitive the system is to key quality, whether an attacker could identify system parameters from observed traffic, resistance to chosen-plaintext and known-plaintext attacks, whether machine-learning classifiers could fingerprint the signal, timing-related information leakage, the effects of real-world component variation, electromagnetic and power side-channels, and deliberate fault injection. Conventional cryptography and authentication protocols remain useful complements to this technology, not replacements for it.

11 Conclusion

Analog Guard® is best understood as one architecture that grew in three clearly separated stages, each protected by its own patent. U.S. Patent No. 12,126,720 is the foundation: it establishes the core dynamic-carrier method and supplies most of the shared technical disclosure — PLTNM, analog encoding, parallel signal paths, and matched-key recovery — that the rest of the family builds on.

U.S. Patent No. 12,689,512 adds a direct-continuation claim built around a different processing order: combine the reference and message first, then apply the key. U.S. Patent No. 12,615,149 adds a CIP-derived claim for a two-key cascade of second-order-or-higher processing stages, synchronized by a controller, and backed by detailed control circuitry and file-processing implementations.

These three patents are related, but they aren't interchangeable, and collapsing them into one undifferentiated story would understate what the portfolio actually covers. Keeping the original claim, the shared disclosure, the direct-continuation claim, and the CIP-derived claim clearly distinct is what makes it possible to see both where this technology came from and how far it has since expanded.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge University Press, 2011.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, 2014.

[5] J. Hall, M. Barbeau, and E. Kranakis, "Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 1-14.

[6] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-Layer Identification of RFID Devices," USENIX Security Symposium, 2009.

[7] R. Maes, Physically Unclonable Functions: Constructions, Properties and Applications. Berlin, Germany: Springer, 2013.

[8] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview," IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001.

[9] C. M. Hymel, M. H. Skolnick, R. A. Stubbers, and M. E. Brandt, "Temporally Advanced Signal Detection: A Review of the Technology and Potential Applications," IEEE Circuits and Systems Magazine, vol. 11, no. 3, pp. 35-54, 2011.

[10] N. A. Otman, C. M. Hymel, A. Nightingale, and R. Stubbers, Signal Protection and Retrieval by Non-Linear Analog Modulation, U.S. Patent 12,126,720, Oct. 22, 2024.

[11] N. A. Otman, C. M. Hymel, A. Nightingale, and R. Stubbers, Signal Protection and Retrieval by Non-Linear Analog Modulation, U.S. Patent 12,689,512, July 21, 2026.

[12] N. A. Otman, C. M. Hymel, and R. Stubbers, Signal Protection and Retrieval by Non-Linear Analog Modulation, U.S. Patent 12,615,149, Apr. 28, 2026.

[13] Signal Advance, Inc., SIGN60-35946 CON Application and Drawings, filed Oct. 21, 2024.

[14] Signal Advance, Inc., SIGN60-35992 CIP Application and Drawings, including added Figures 58-87.

Appendix A. Figure Inventory

Figure	Working Title	Purpose
1	Patent Family Relationship Map	Shows how the original claim, the direct-continuation claim, and the CIP-derived claim each relate to the disclosure they draw on.
2	Dynamic Carrier Formation	Shows how the original patent builds a dynamic carrier: the key shapes the carrier first, then the message is mixed in.
3	Signal Recovery Through Synchronization	Shows how matching the key, the carrier, and the timing at the receiver recovers the message — a principle shared across the family.
4	Parallel Signal Paths	Shows the original patent's parallel-path technique, later developed further by the CIP branch.
5	PLTNM Timing and Waveform Effects	Shows PLTNM's effect on timing and waveform shape, as described in the original patent.
6	Mixed-Signal Encryption Core	A conceptual view of analog encoding and signal transformation working together, from the family's shared disclosure.
7	Multi-Domain Transformation Environment	A conceptual view of the family's multi-domain signal transformation approach, drawn from shared disclosure rather than a single claim.
8	Direct Continuation Combined-Signal Path	Shows Patent 12,689,512's claimed sequence: the reference and message combine first, then the key modifies the result.
9	CIP-Derived Two-Key Cascade	Shows Patent 12,615,149's claimed two-key, two-stage transfer-function architecture.

Figure	Working Title	Purpose
10	CIP File Workflow	Shows the CIP-derived file encryption and decryption workflow, based on added Figures 71, 72, 85, 86, and 87.

Appendix B. Key Terms

Term	Working Meaning in This White Paper
Foundational patent	U.S. Patent No. 12,126,720 and the original dynamic-carrier method it claims.
Shared disclosure	Technical material described in the original patent that later continuation claims are free to build on.
Direct continuation	A later patent application that relies on the same disclosure as an earlier one, but pursues a different, specific claim.
Continuation-in-part (CIP)	A later patent application that keeps the earlier disclosure and adds genuinely new material on top of it.
Dynamic carrier	A carrier wave whose frequency, phase, amplitude, or timing has been shaped by an analog key — central to the original patent's claim.
Combined reference signal	The reference-and-message combination that Patent 12,689,512's key modifies, rather than shaping the carrier beforehand.
Transfer function	The mathematical relationship describing how a circuit stage changes a signal's frequency content as it passes through.
Parameterization	Using an analog key (or a control signal derived from it) to set how a transfer function behaves.
PLTNM	Phase-linked temporal nonlinear modulation — key-controlled circuitry that affects a signal's magnitude, phase, and timing in a nonlinear way.
Matched reconstruction	Successfully recovering the original message by reproducing the correct key, processing steps, carrier conditions, configuration, and timing at the receiver.