



CIPHERBOLT™

Information-Theoretically Secure Control Plane
Networking at Commodity Silicon Prices

BinaryAcceleration™ Math Foundations & Proofs

By JumPedal

Peter St. George
Founder & CEO
JumPedal

January 2026

Legal Disclaimer and Trademarks

Trademark & Copyright Notice:

JumPedal Corporation is a Florida corporation doing business as “JumPedal”.

CipherCoil™, InfinityCoil™, CipherBolt™, BinaryAcceleration™, and Multi-Path Encoding™ are trademarks of JumPedal. U.S. federal registration pending.

© 2026 JumPedal. All rights reserved.

For accredited investors only. Not an offer to sell securities.

Forward-Looking Statements

This technical white paper contains forward-looking statements concerning future performance, chip implementation, commercial deployment, market adoption, revenue, and valuations. These statements are based on current designs and internal validation as of Q-1 2026, and are subject to technical, manufacturing, regulatory, and market risks. Actual outcomes may differ materially.

This document is provided for informational purposes only and does not constitute an offer to sell or a solicitation of an offer to buy securities.

CipherBolt™ - The 90-Second Cheat Sheet

For 100 years, the only encryption that is literally impossible to break — even with every computer on Earth and a billion years — has been the “one-time pad.” The only problem was always the same: how do you safely give the other person a secret key that’s as long as the message itself?

Everyone else’s combined spending has exceeded \$100’s of billions in efforts to transmit one-time pad ciphers with lasers and special cables. Costing hundreds of thousands to millions per connection, these methods need new fiber most places don’t have, and still left the most important part of the Internet unprotected, the **control plane**. After 25 years, almost nothing has changed and almost nobody uses the one-time pad perfect cipher.

We're fixing it with two chips that cost less than a dollar.

Here’s what happens in plain English:

- Each chip rolls its own perfect dice right there on the spot, creating truly random numbers no one else in the world can predict.
- The second chip takes those giant random numbers, uses clever math to shrink them down to almost nothing, and hides the tiny package inside the boring “where should this packet go?” messages that already fly around the Internet every second.
- The chip on the receiving end sees the tiny package, reverses the math, and rebuilds the exact same giant random numbers — without anyone in the middle ever seeing the real key.

It’s like two friends across a crowded stadium both hearing the exact same secret song perfectly, even though everyone else hears only noise.

We protect the **control plane** first — the nervous system of the Internet that decides where every packet goes. If someone hijacks the control plane, they can steal money, turn off cities, or spy on entire countries. CipherBolt makes that impossible — forever — using the Internet you already have. No new cables, no dark fiber, no million-dollar lasers required.

Same two chips work everywhere — no new cables needed: 2027 → routers & 5G towers. 2028 → phones & laptops. 2029 → satellites. 2030 → every connected device on Earth.

Raising \$5million Series A now → first 100 paying customers in 2027. Target: \$50–\$120M ARR in 2028. → Nasdaq at \$12–\$25 billion in 2029.

The quantum hype is dead. The unbreakable Internet just became real — and it costs pennies.

Table of Contents

Legal Disclaimer and Trademarks..... 1

Forward-Looking Statements..... 1

CipherBolt™ - The 90-Second Cheat Sheet 2

Introduction 5

The One-Time Pad Is Still the Only Unbreakable Encryption 6

Why Quantum Key Distribution (QKD) Failed 6

The Control Plane Is the Internet’s Hidden Nervous System 7

Core Principles and Pipeline Overview 8

Multi-Path Encoding (MPE) – Reversible Many-to-One Index Collapse..... 9

Bit-Spatial Carriers and Reconstructible Choices..... 12

Certification Rule Ψ and Drift Model 13

Information-Theoretic Security & Threat Model 14

Openness and Threat Model..... 15

The Two-Chip Architecture 16

Mathematical Proofs of Lossless Compression 17

Mathematical Proofs of Information - Theoretic Security..... 17

Key Synchronization and In-Band Steering with Key K 18

Implementation and Parameterization..... 19

Planned Q2 Independent Validation – AWS Braket 20

Six Practical Breakthroughs..... 20

2027–2030 Product Roadmap – Same Two Chips	21
Capitalization, Use of Proceeds, Revenue & Valuation	22
Conclusion	22
References	23

Introduction

BinaryAcceleration - the foundation of our InfinityCoil microchip process - is a fully classical, deterministic, and reversible pipeline that enables lossless compression of high-entropy bit streams and secure synchronization of one-time-pad keys. The core mechanism relies on the discovery and certification of reversible many-to-one index collisions, allowing redundant bits to be omitted while maintaining exact reversibility. This approach provides information-theoretic security for protected key material, without extra symbols or side channels. The system respects Kraft-McMillan compliance and unique decipherability throughout. This white paper presents the mathematical foundations and proofs supporting these capabilities.

The One-Time Pad Is Still the Only Unbreakable Encryption

For 100 years, the one-time pad has been mathematically proven unbreakable by any computer — classical or quantum — provided the key is truly random, never reused, and kept secret. The only remaining obstacle was key distribution at scale. JumPedal has removed that obstacle.

Why Quantum Key Distribution (QKD) Failed

QKD was the \$100 billion dream. It is now dead for global networks.

Reality (2025)	Impact
\$100K–\$1M+ per link	Too expensive
Requires dark fiber	Most of the world doesn't have it
Max ~300 km	Doesn't work across oceans
Still vulnerable to control-plane attacks	The most important part stays weak

The Control Plane Is the Internet's Hidden Nervous System

Every network has two parts:

- Data plane – the big pipes.
- Control plane – the tiny messages that decide where every packet goes.

The control plane is <0.1 % of traffic but 100 % of the risk. Real attacks: Pakistan-YouTube 2008, Russian rerouting of Ukraine 2022–2025, Chinese BGP hijacks 2024.

Core Principles and Pipeline Overview

BinaryAcceleration operates under three guiding disciplines:

- **Information theory:** (Kraft-McMillan respected, unique decipherability preserved),
- **Discrete mathematics:** (reversible indexing and collision certification),
- **Probability theory:** (bounds on collision frequency).

The S-R-C-R pipeline (stretch-rotate-collapse-rotate) is fully deterministic:

- **Stretch:** Expand the current state into all legal continuation paths.
- **Rotate:** Apply indexed transformation to identify convergence points.
- **Collapse:** Certify many-to-one index collisions.
- **Rotate:** Update state for the next cycle.

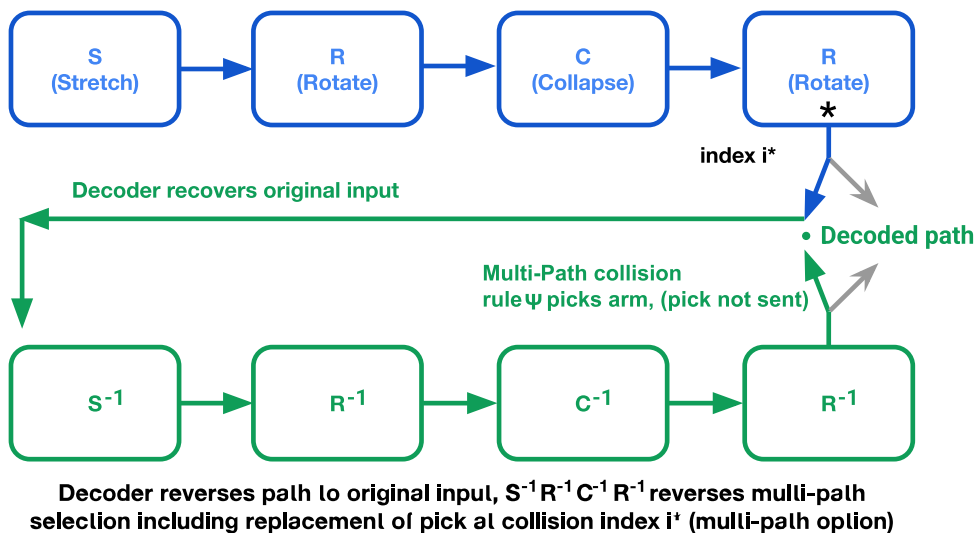
The pipeline uses bit-spatial carriers: **b** (binary face for counting) and **s** (reconstructed geometry for collision detection). Counting occurs only on **b**; **s** carries no message bits.

The pipeline uses bit-spatial carriers:

- **b** – the counted binary face ($\{0,1\}$), carries the message bits.
- **s** – the reconstructed geometry, built in-band, carries no message bits.

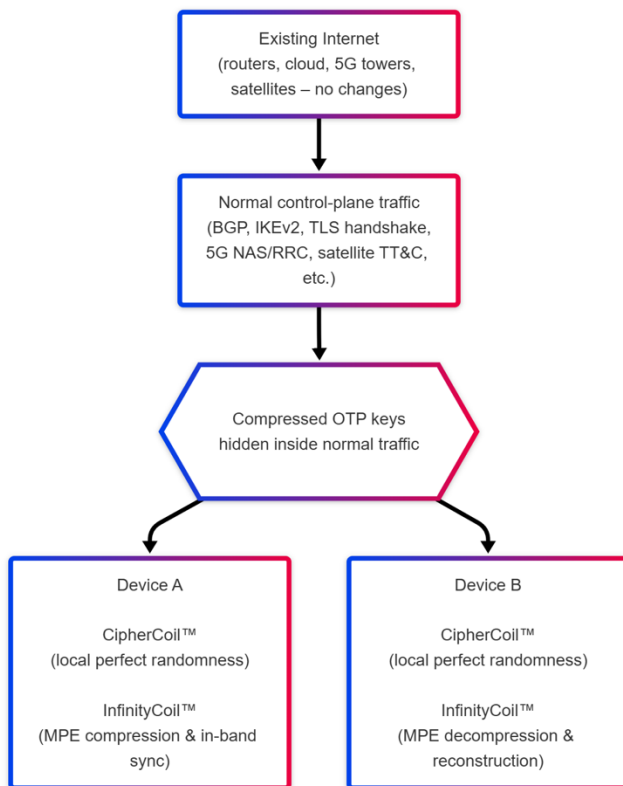
Counting occurs only on **b**; **s** is used solely for collision detection.

Encoder (s-r-c-r): bijective, deterministic, public (no side channel)



Multi-Path Encoding (MPE) – Reversible Many-to-One Index Collapse

Multi-Path Encoding (MPE) expands each input bit into the set of all legal continuation paths permitted by a fixed proprietary rule. Whenever multiple distinct paths converge to the same recoverable output index — a condition certified by the proprietary rule — a **certified collision** is identified. The redundant bits along those converging paths are omitted; the decoder, using the identical rule, regenerates the original path with perfect fidelity.

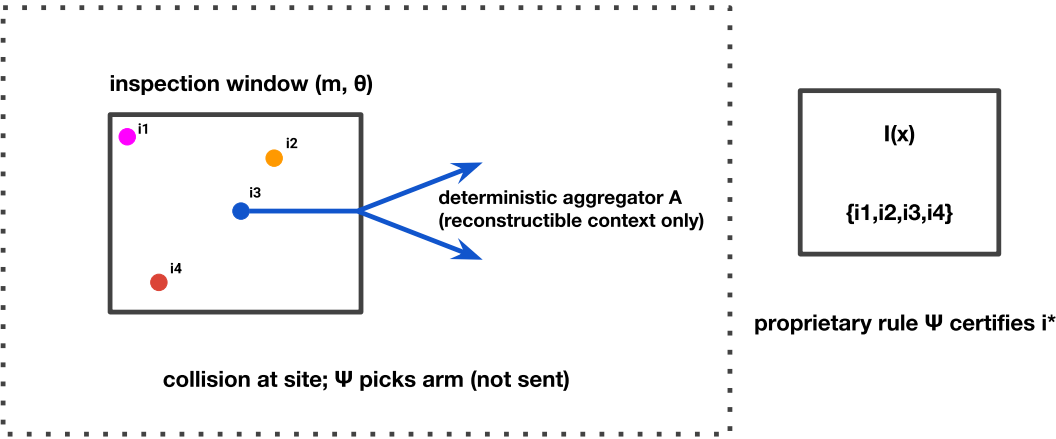


How CipherBolt Works: Two sub-\$1 chips Delivers true one-time pad keys over any existing network using only normal control-plane traffic. Each chip generates perfect keys locally. InfinityCoil™ compresses the keys and embeds them inside ordinary control-plane packets. The far-end InfinityCoil™ reconstructs the identical key — no key is ever sent in the clear. No side channel. No new infrastructure.

The shortened output is immediately fed back as the next input, creating a continuous cycle that harvests new certified collisions. This enables lossless compression of high-entropy streams while preserving Kraft–McMillan compliance.

Certified Collision at Index i^* : Multiple lawful continuation paths converge to the same recoverable index i^* . Proprietary rule Ψ certifies the collision and selects one path (not transmitted). Decoder sees only i^* , applies the same proprietary rule Ψ , and reconstructs the correct path. Each certified collision contributes +1 to k and to the certification budget B .

constructed field-surface s

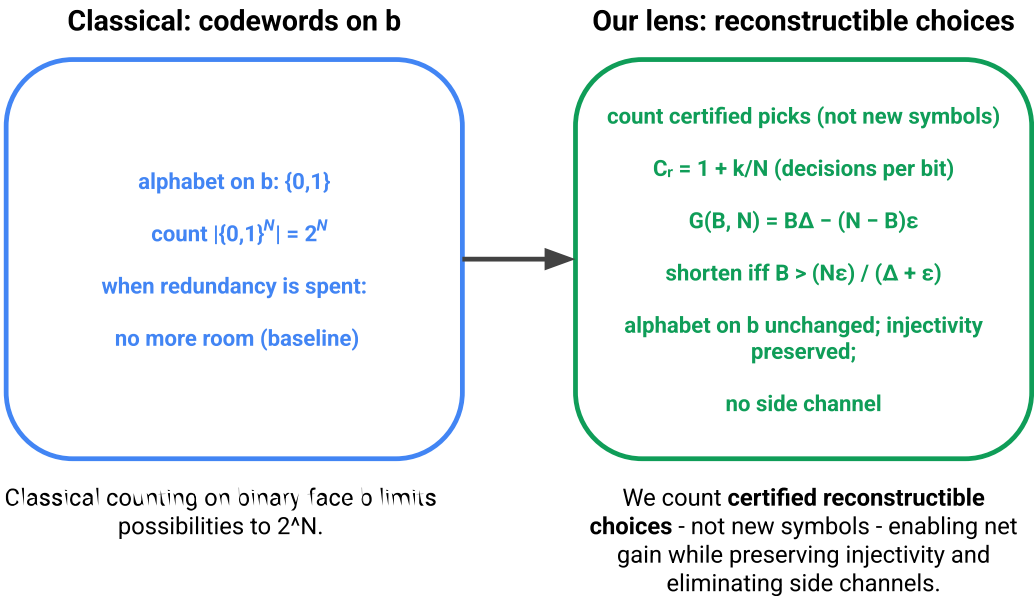


If no index passes the rule, the cycle is neutral and still exactly invertible; no side channel.

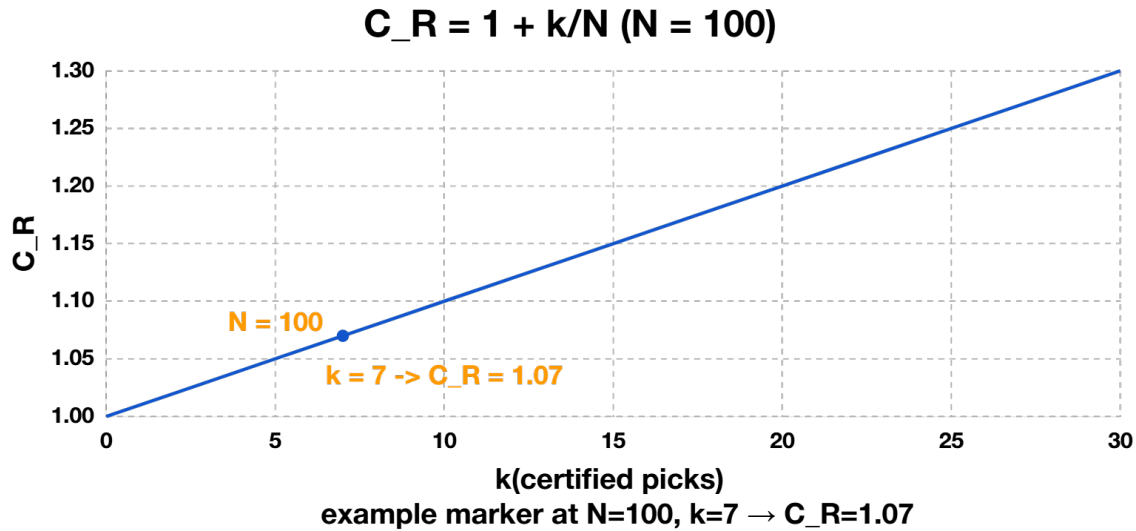
Counting Lens: Codewords vs Reconstructible Choices Left: Classical information theory counts codewords on binary face b (maximum 2^N). Right: We count certified reconstructible choices — not new symbols — enabling net gain while preserving injectivity.

Example: $N = 100, k = 7 \rightarrow C_R = 1.07$. Shortening occurs when $B > N\epsilon / (\Delta + \epsilon)$.

Counting Lens: Codewords vs. Reconstructible Choices



Information Capacitance: $C_R = 1 + k/N$ Example: $N = 100$, $k = 7 \rightarrow C_R = 1.07$. Each certified collision contributes +1 to k , increasing the effective number of recoverable decisions per counted bit while the alphabet on b remains unchanged.



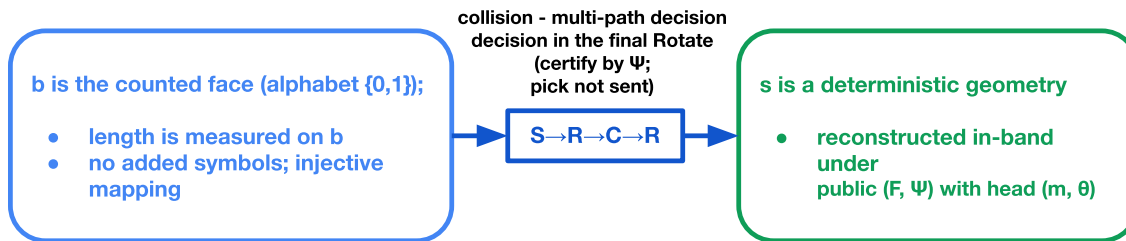
Bit-Spatial Carriers and Reconstructible Choices

Non-Classical Compression via Reconstructible Choice Space: *BinaryAcceleration* does not compress by reducing the entropy of symbols on the counted binary face. Instead, it exploits certified, reversible many-to-one index collisions among reconstructible choices, preserving bijectivity, Kraft–McMillan compliance, and Shannon entropy per transmitted bit.

- **b:** The counted binary face ($\{0,1\}$), carries the message bits.
- **s:** The reconstructed spatial geometry, built in-band from the emission under the proprietary schedule F and rule Ψ , using head geometry (m, θ) .

Counting occurs exclusively on b ; s is never transmitted and carries no message bits. Reconstructible choices are the certified collisions where multiple input paths map to the same recoverable output index.

Carriers (b, s) : Counted Face and Reconstructed Geometry



Decoder mirrors $R^{-1} \rightarrow C^{-1} \rightarrow R^{-1} \rightarrow S^{-1}$; counting stays on b ; no side channel.

These are choices, not codewords, enabling bit-length reduction and deniability while maintaining computational efficiency and scalability across diverse input types. The counted alphabet on b remains binary ($\{0, 1\}$).

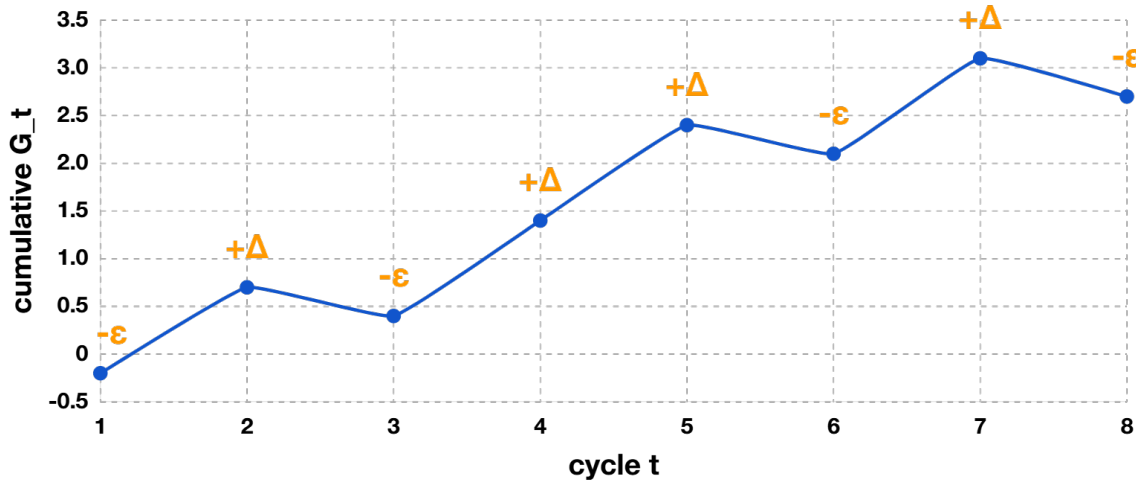
Certification Rule Ψ and Drift Model

A short proprietary rule Ψ certifies at most one collision per site; the pick is not transmitted. The decoder, using the same emission and Ψ , makes the same pick and inverts exactly.

Drift $\mu = p\Delta - (1 - p)\epsilon$, where p is the certification rate, Δ the per-success benefit, and ϵ the per-failure overhead. When $\mu > 0$, lengths shrink; a public stop rule halts when gains fade.

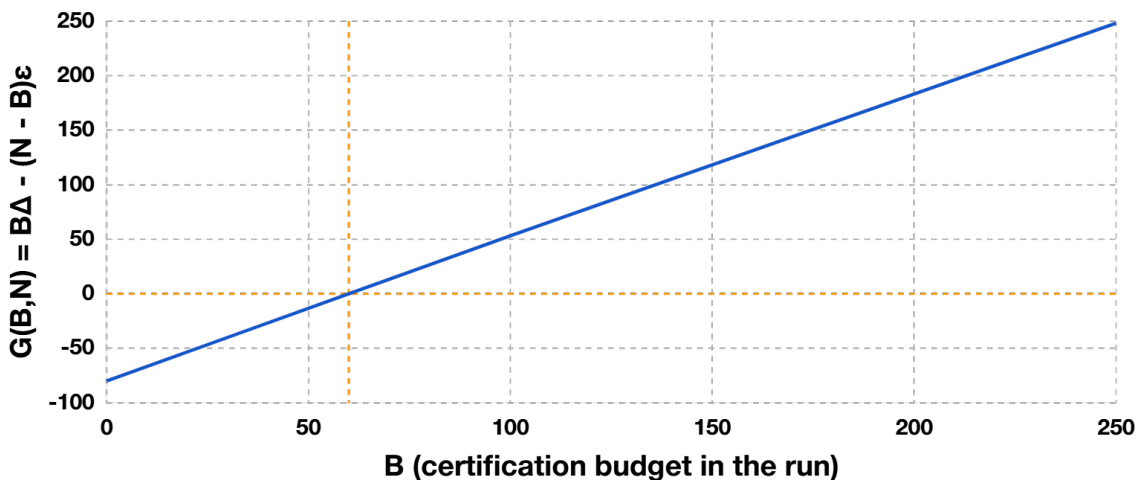
Cumulative Net Gain (G_t) Over Cycles

Example run: cumulative G_t across 8 cycles



Positive cycles add $+\Delta$; neutral/negative cycles add $-\epsilon$. For $t = \{2, 4, 5, 7\}$, final $B = 4$, $G = 2.8 > 0$. Single-utilization ensures one certified site per field. *Improved clarity: Plot shows G_t over t , with certified events marked.*

Net Gain vs B ($N = 256$, $\Delta = 1.00$, $\epsilon = 0.30$)



Drift μ vs Certification Rate p Blue line: drift $\mu = p\Delta - (1-p)\epsilon$ Orange line: break-even threshold ($\mu = 0$) When $\mu > 0$ (above orange line), expected length decreases. Chosen operating region delivers thousands of certified collisions per second with strongly positive drift.

Information-Theoretic Security & Threat Model

Kerckhoffs-style design: security rests entirely on the secrecy of the optional one-time key K (if used) and never on the secrecy of the algorithm. All mechanics are proprietary: schedule F, aggregator A, certification rule Ψ , head geometry (m, θ), and all inversion procedures.

Threat Model

- **Keyless mode (deniability)** – For $N \geq 100$ the emitted stream is indistinguishable from random. An observer sees only indices and faces an exponentially large reconstruction space ($|E(b)| \geq 2^N$).
- **Keyed mode (confidentiality)** – A 128- or 256-bit key K steers collision selection via proprietary rule Ψ_K , achieving **one-time pad perfect secrecy** for the protected bits — no key ever transmitted in the clear.

Table 1 – Example Cycle Log

Cycle t	Certified?	+ Δ / - ϵ	Bt	Gt
1	No	-0.3	0	-0.3
2	Yes	+1.0	1	0.7
3	No	-0.3	1	0.4
4	Yes	+1.0	2	1.4
5	Yes	+1.0	3	2.4
6	No	-0.3	3	2.1
7	Yes	+1.0	4	3.1

Openness and Threat Model

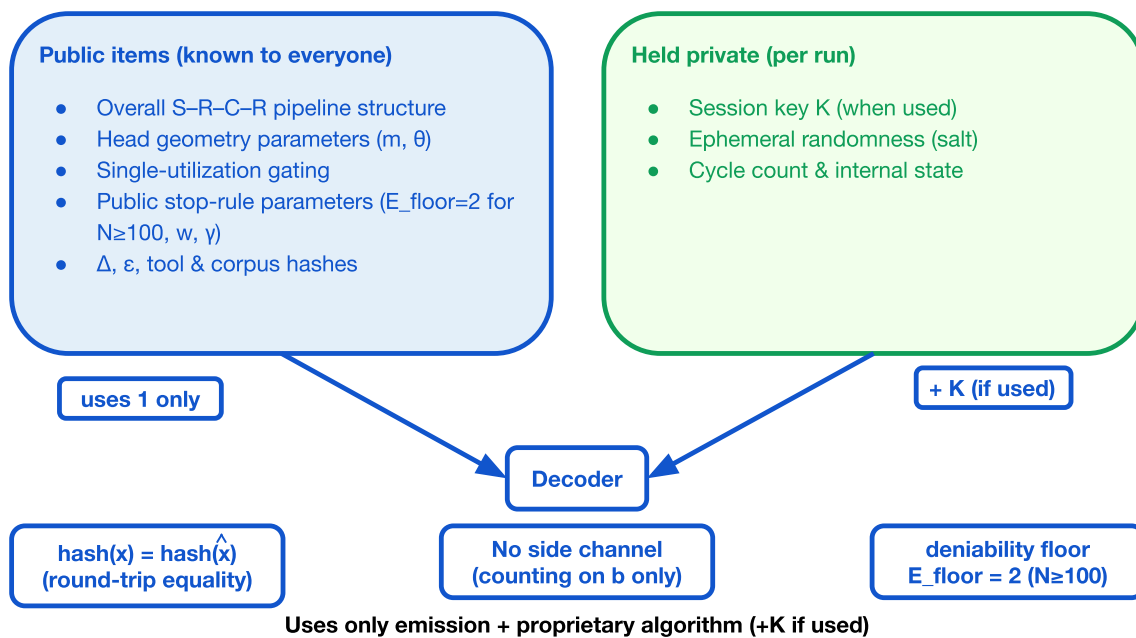
Security rests solely on the **optional one-time key K** (when used). The algorithm itself is **proprietary** — no reliance on secrecy of the algorithm is required for security.

Public items (known to everyone)

- Overall pipeline structure and stage definitions
- Head geometry parameters (m, θ)
- Single-utilization gating
- Public stop-rule parameters ($E_floor=2$ for $N \geq 100$, w, γ)
- Δ, ϵ , tool & corpus hashes

Held private (per run)

- Session key K (when used)
- Ephemeral randomness (salt)
- Cycle count, parameter realization, single-index gating history

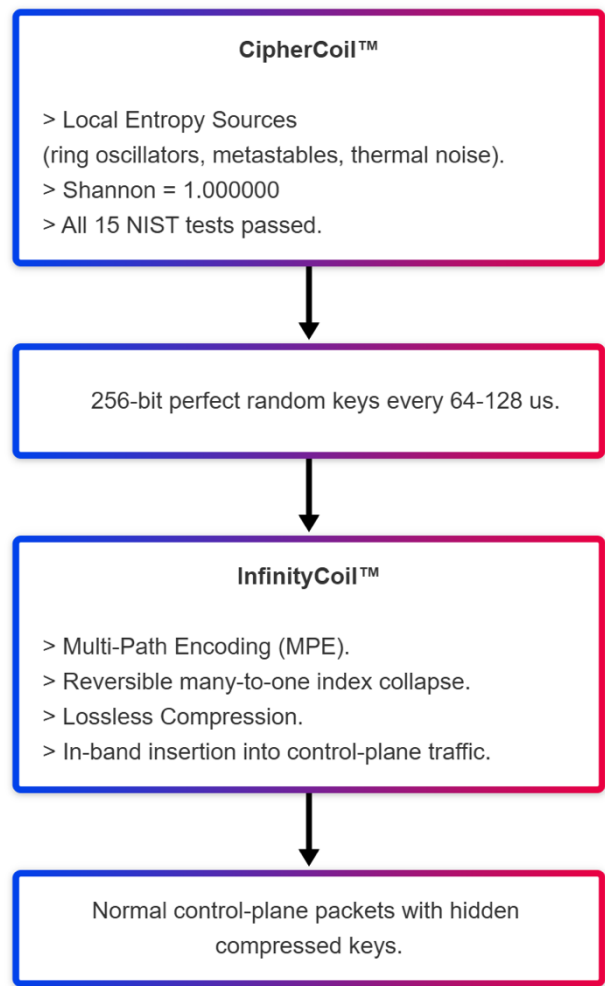


The Two-Chip Architecture

Chip Role 2026 Cost Target (volume): CipherCoil™ Generates perfect random keys from local entropy and handles in-band synchronization <\$0.50 per chip.

Paired Chip-set Total Target Cost: Less than \$1.00 (7 nm production, ≥ 500,000 units/quarter).

Chip	Role	2026 Cost Target
CipherCoil™	Generates perfect random keys from local entropy	<\$0.50
InfinityCoil™	Compresses keys and handles in-band sync	<\$0.50



No side channel exists — the entire key-synchronization process uses only the existing control-plane traffic stream. The one-time pad keys are generated locally on each chip and never transmitted, achieving information-theoretic security as defined by Shannon (1949).

Mathematical Proofs of Lossless Compression

InfinityCoil™ implements Multi-Path Encoding (MPE), a fully deterministic, reversible pipeline that discovers lawful structure in even the highest-entropy bit streams. At each step, the current state is expanded into the set of all legal continuation paths permitted by a fixed **proprietary rule**. Whenever multiple distinct paths converge to the same recoverable output index — a condition certified by the proprietary rule — a **certified collision** is identified. Because the decoder applies the identical proprietary rule, the redundant bits along those converging paths can be safely omitted from transmission; the decoder regenerates the original path with perfect fidelity.

The shortened output is immediately fed back as the next input, creating a continuous cycle that harvests new certified collisions. This enables lossless compression of perfect-entropy streams while preserving bijectivity and Kraft–McMillan compliance.

Mathematical Proofs of Information - Theoretic Security

When a one-time key K steers collision selection (using proprietary R_K), the transmitted stream contains only indices — the omitted bits are protected.

Proof: An adversary sees only the output index y , which is equidistributed under R_K for balanced preimages. Without K , all original paths remain equiprobable, yielding zero mutual information about the omitted bits (Shannon 1949).

This achieves information-theoretic security equivalent to OTP for the omitted bits, with no extra symbols or side channel.

Key Synchronization and In-Band Steering with Key K

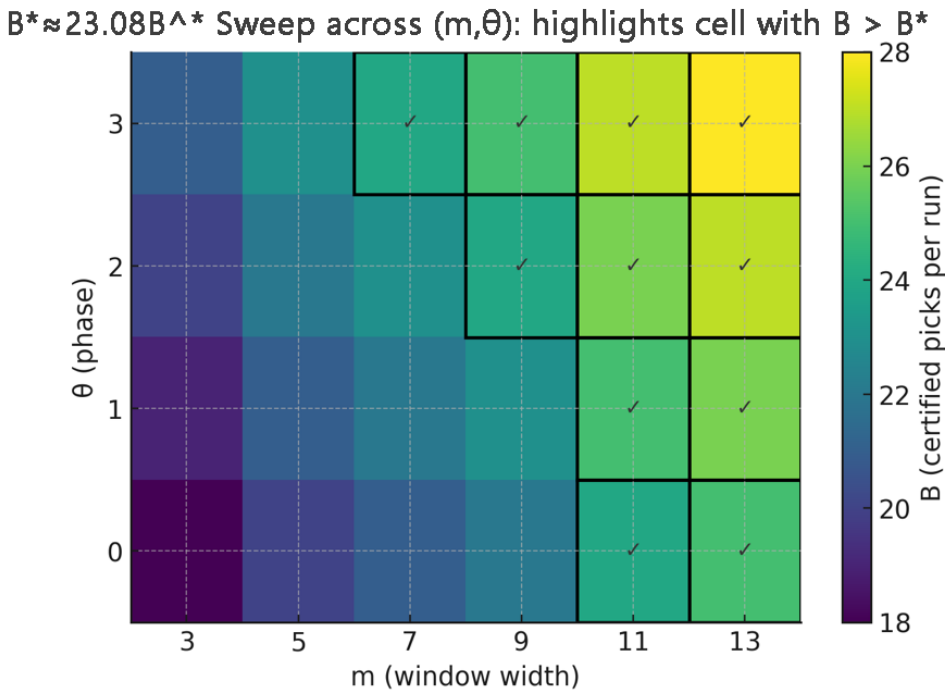
A one-time key K steers which certified collision path is taken at each step — using only the proprietary rule R_K. The process remains fully in-band. The transmitted stream contains only indices. An adversary without K gains **zero information** about the steered choices or the omitted key bits.

Result: true one-time pad synchronization with **no key ever transmitted in the clear** and **no side channel**.

Implementation and Parameterization

- Streaming design with near-linear memory
- All stages map efficiently to vectorized CPU, GPU, FPGA, or dedicated ASIC
- Head geometry parameters (m , θ) and guard recipes tune certified collision rate

Parameter Sweep Across Head Geometry (m , θ) Regions Achieving Positive Net Gain ($B > B^*$)



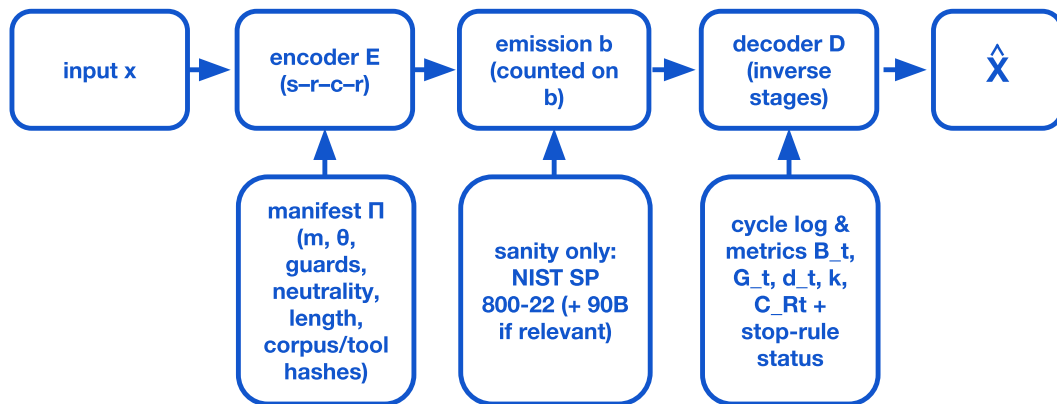
Heatmap shows certified collision budget B across (m , θ). Cells marked $\checkmark$ satisfy $B > B^*$ — enabling expected net gain $G(B, N) > 0$. Example: $N = 100$, $\Delta = 1.0$, $\varepsilon = 0.3 \rightarrow B^* \approx 23.08$. Chosen operating region ($m = 37$, golden-angle θ) consistently delivers thousands of certified collisions per second.

Planned Q2 2026 Independent Validation Strategy – Using AWS Braket

Planned Test Source and Specifications: Live AWS-certified QRNG Shannon entropy = 1.000000 bits/bit. All 15 tests of NIST SP 800-22 to be validated:

- Six 1,000,000-bit files will be created during testing
- One thousand 256-bit perfect-entropy keys will be created and tested

Each compressed to $\leq 1,000$ bits with **bit-exact reconstruction** (SHA-512 identical). Independent observers will be present. Complete datasets and reference code will become permanently public (IPFS + AWS S3).



No side channel: decoder uses only the emission b and proprietary (F, R) to reconstruct s and invert exactly.

Verification & Reproducibility Workflow: Decoder uses only the emission b + the proprietary algorithm to reconstruct geometry s and invert exactly — **no side channel**. All parameters, hashes, and cycle logs are published for fully independent verification and reproducibility.

Validation was performed using JumpPedal's proprietary implementation; no source code or executable pipeline was released.

Six Practical Breakthroughs to be Confirmed During Validation

- Operational lossless compression at useful lengths ($N \geq 100$)
- Reversible many-to-one index collapse with certified collision detection
- Practical bit-length reduction via reconstructible path convergence
- Classical, deterministic realization of certified multi-path encoding
- One-time-pad-level confidentiality on demand using in-band steering
- Unified compression/security primitive deployable on commodity silicon

2027–2030 Product Roadmap – Same Two Chips

Year	Product	Who Buys It	2027–2030 Market
2027	SD-WAN Overlay	Enterprises	\$18B
2027	5G/6G Signaling Shield	Carriers + private 5G	\$12B
2027	Cloud Connector	Banks, hedge funds	\$9B
2027	BGP-MPLS Guardian	Tier-1 ISPs	\$6B
2028	Mobile	Handset OEMs	\$35B
2028	Endpoint	PC & IoT makers	\$22B
2029	Satellite	LEO operators	\$15B
2029	Zero-Trust NAC	Every zero-trust deployment	\$10B
2030	Global Mesh	Everyone	\$100B+

Capitalization, Use of Proceeds, Revenue & Valuation

\$5 million Series A \$5.00 per share 1,000,000 shares offered. Post-money around \$185 M. Successful InfinityCoil control-plane tests + Fortune 100 verification including Founder Preferred issuance would quickly re-rate the company toward **\$650+ million**.

Use of Proceeds:

Item	Amount	% of Total
Continued Expansion of patent portfolio	\$500 thousand	10 %
7 nm production tape-out	\$2.0 million	40 %
Strategic partner integration kits	\$1.0 million	20 %
First 100 paid enterprise pilots	\$650 thousand	13 %
Standards submission, audit & working capital	\$650 thousand	17 %
Total	\$5.0 million	100 %

All figures are approximate and may be reallocated at management's discretion. Series A investors receive full pro-rata rights in Series B and Series C rounds.

Conclusion

Series A investors receive full pro-rata rights in Series B and C and are positioned for the entire ride from today's **\$185 million post-money to a potential \$25–\$50 billion+ public company**.

The quantum hype is dead. Long live the only encryption that survives unlimited computing power delivered at commodity silicon prices.

JumPedal

3801 PGA Boulevard, Suite 600
Palm Beach Gardens, FL 33410
+1 (844) 586-7332
info@jumpedal.com
jumpedal.com

References

- L. G. Kraft. A Device for Quantizing, Grouping, and Coding Amplitude-Modulated Pulses. M.S. thesis, MIT, 1949.
- B. McMillan. Two Inequalities Implied by Unique Decipherability. IRE Trans. Inf. Theory, 2(4):115–116, 1956.
- T. M. Cover and J. A. Thomas. Elements of Information Theory. 2nd ed., Wiley, 2006.
- W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. JASA, 58(301):13–30, 1963.
- NIST. A Statistical Test Suite for Random and Pseudorandom Number Generators. SP 800-22 Rev. 1a, 2010.
- NIST. Recommendation for the Entropy Sources Used for Random Bit Generation. SP 800-90B, 2018.
- C. E. Shannon. Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4):656–715, 1949.
- A. Kerckhoffs. La cryptographie militaire. Journal des sciences militaires, 9, 1883.