H33.ai Removes the Constraints of Quantum Encrypted Computation

Encrypted computation now behaves like plaintext. This was not supposed to be possible in production systems.

H33 Logo

RIVERVIEW, FL, UNITED STATES, May 11, 2026 /EINPresswire.com/ -- H33.ai today announced the production deployment of its TFHE Programmable Bootstrapping engine.

No depth limits.
No noise budgeting.
No branch leakage.

> Encrypted computation didn't fail because it was impossible. It failed because it was constrained. Those constraints are gone. The system computes, proves, and never sees the data”
>
> — *Eric Beans, CEO, H33.ai*

Encrypted computation now behaves like plaintext — except the system never sees the data.

-The server cannot see the data.
-The server cannot know the outcome.
-The server still makes the decision.

This was not supposed to be possible in production systems. It is possible now.

THE CONSTRAINTS ARE GONE

Traditional FHE forces developers to design around cryptographic limits. Depth limits. Noise budgets. Algorithm restructuring.

Those constraints are gone.

Every operation resets noise. Computation does not degrade. It just continues.

THE SERVER LEARNS NOTHING

The system evaluates every possible branch. It cannot determine which path applies.

Not by policy. Not by restriction. By mathematics. The computation reveals nothing about the underlying data.

Only the keyholder can determine which result is real. Branching patterns, timing side-channels, and selective computation attacks are eliminated - structurally, not by configuration.

COMPUTATION, PRIVACY, AND PROOF — UNIFIED

Every decision is sealed with H33-74 — a 74-byte post-quantum attestation backed by three independent mathematical hardness assumptions. Not just encrypted. Verifiable. Anywhere.

H33.ai - The World's First Complete Quantum-Proof Security Platform

Smart contracts can verify these attestations directly on-chain. The computation happens off-chain on encrypted data. The proof lands on-chain in 74 bytes. The verifier never needs to see the data, trust the server, or contact H33.

Computation. Privacy. Proof. One system.

WHAT THIS CHANGES

The matching engine cannot see the orders it is matching. There is nothing to front-run. Prices, size, and counterparties are never exposed. There is no information to exploit.

The processor never sees compensation data. The system computes the result. The auditor verifies the proof. No audit requires access to raw data.

The system makes binding decisions on data it cannot read. The decision output is the policy action. The decision itself becomes the system output. No human ever needs access to the underlying data.

PERFORMANCE

These are not simulations. These are production measurements.

768 TPS — 8-bit encrypted comparisons
372 TPS — 16-bit encrypted comparisons
182 TPS — 32-bit encrypted comparisons
769 TPS — 16-bit encrypted equality

Linear scaling. Predictable cost.

AWS Graviton4 (ARM). Sustained over 30 seconds. No GPU.

THE STACK

No single cryptographic scheme can handle all computation. This is why most systems fail. That is why we built five.

BFV — Batched integer arithmetic (2,293,766 auth/sec sustained)
BFV-256 — Extended security parameters
CKKS — Approximate arithmetic for ML inference on encrypted data
TFHE — Gate-level encrypted Boolean logic
TFHE Bootstrap — Programmable bootstrapping, unlimited depth

All five written from scratch in Rust. Zero external FHE or cryptographic library dependencies.

ABOUT H33.AI

H33.ai builds post-quantum cryptographic infrastructure. Five proprietary FHE engines, STARK-based zero-knowledge proofs, post-quantum
digital signatures across six independent hardness assumptions, and the H33-74 attestation standard. 7 patents pending, 250+ claims.

Everything accessible through an API.

CONTACT

support@h33.ai
https://h33.ai
https://h33.ai/schedule-demo

Eric D Beans
H33.ai, Inc.
+1 813-464-0945
email us here
Visit us on social media:
LinkedIn
YouTube
X
