ZerøFHE

Encrypt Everything. Trust No-one.

FHE – The Holy Grail of Data Encryption

Traditional encryption methods safeguard data at rest and in transit, but are highly vulnerable when in use, which typically requires data to be unencrypted.

Fully Homomorphic Encryption (FHE), unlike traditional encryption, allows for search, statistical operations and AI training while the data remains encrypted and quantum secure.

Previous FHE algorithms (such as BFV) lacked quantum security and were excessively slow and resource-intensive, rendering them commercially impractical.

ZerøFHE's algorithm overcomes all prior technical limitations, achieving a groundbreaking advancement in next-generation encryption.

ZerøFHE Metrics: The Six ‘S’s of Encryption

Metric	ZerøFHE	BFV	Comparison	Why Important
Security (Bits)	Quantum Secure >>256	Classically Secure <128	**$>2^{128}$ More Secure**	The algorithm must be secure enough to resist future quantum computer attacks ensuring post-quantum security.
Speed Multiplication (Microseconds)	2.11	4,804	**2,277 x Faster**	Performance must be within an order of magnitude of plaintext without hardware acceleration, particularly in AI training. **ZerøFHE** is much faster even though BFV has much lower security.
Slimness Multiples of Clear	768	181,106	**236 x Slimmer**	Prior algorithms exhibited huge expansion ratios rendering them impractical for most applications. Ratios must be <1000.
Specificity Losslessness	Lossless	Depends on Configuration	**Always Lossless**	A viable algorithm must be lossless to enable accurate inferences and ensure user confidence in the outcomes.
Simplicity Capability, +, x, 🔎	+, x, 🔎	+, Slow x,	**All Operations Managed with one Algo**	Algorithms must be able to perform search, addition, multiplication at depth without having to repeatedly swap out the algorithm.
Scalability (Trendline Slope for Time/Iteration)	Linear (m = – 0.35)	Exponential	**Infinite Depth**	Many algorithms use bootstrapping that adds noise to obfuscate weakness in security, but this grows exponentially and prevents scale.

These metrics reflect no hardware acceleration and will improve further due to software improvements. It currently can run in the browser and on end devices (sensors, cell phones etc).
ZerøFHE is patented enabling exclusive and non-exclusive licensing.

ZerøFHE Metrics: The Six 'S's of Encryption

Metric	ZerøFHE	BFV	Comparison	Why Important
Security (Bits)	Quantum Secure >>256	Classical Secure <128	$>2^{128}$ More Secure	The algorithm must be secure enough to resist future quantum computer attacks ensuring post-quantum security.
Speed Multiplication (Microseconds)	2.11	4,804	2,277 x Faster	Performance must be within an order of magnitude of plaintext without hardware acceleration, particularly in AI training. **ZerøFHE** is much faster even though BFV has much lower security.
Slimness Multiples of Clear	768	181,106	236 x Slimmer	Prior algorithms exhibited huge expansion ratios rendering them impractical for most applications. Ratios must be <1000.
Specificity Losslessness	Lossless	Depends on Configuration	Always Lossless	A viable algorithm must be lossless to enable accurate inferences and ensure user confidence in the outcomes.
Simplicity Capability, +, x,	+, x, ⌕	+, Slow x,	All Ops Managed with One Algo	Algorithms must be able to perform search, addition, multiplication at depth without having to repeatedly swap out the algorithm.
Scalability (Trendline Slope for Time/Iteration)	Linear (m = - 0.35)	Exponential	Infinite Depth	Many algorithms use bootstrapping that adds noise to obfuscate weakness in security, but this grows exponentially and prevents scale.

These metrics reflect no hardware acceleration and will improve further due to software improvements. It currently can run in the browser and on end devices (sensors, cell phones etc.). **ZerøFHE** is patented enabling exclusive and non-exclusive licensing.

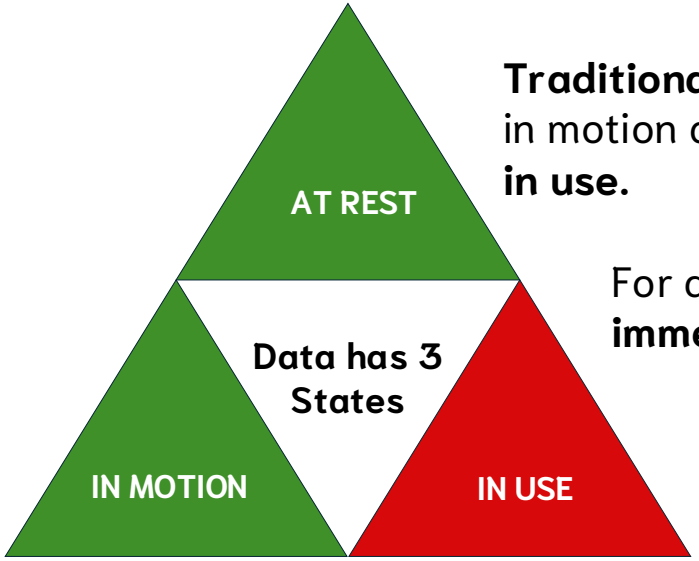
The 3 Major Data Problems Impacting 3 Major Industries

Data Security (Cybersecurity)
A $243 Billion industry that is not succeeding, and breaches are costing over $10 Trillion each year.
ZerøFHE is quantum secure and can encrypt everything with no need to ever decrypt.
It also can add security to blockchain resident data.

Data Drought and Confidentiality (AI)
AI training, a $100 Billion industry, has exhausted all public data and client confidentiality issues are a concern.
ZerøFHE can make confidential data (99.8% of all extant data) available for AI model training.
It also enables protection of an AI model allowing broad distribution.

Data Regulation (Regulatory Compliance)
Governments globally have implemented numerous data privacy regulations, creating a $20 billion industry to address compliance.
ZerøFHE can massively simplify data privacy compliance.

The Cybersecurity Problem



Traditional encryption can provide effective protection when data is in motion and when at rest **but is highly vulnerable when the is data in use.**

For data to be **operated on,** it must first be **decrypted** – and **immediately** become **unsecure.**

Only FHE can protect all three states as it allows **operations** (arithmetical or search) to be performed **on encrypted data.**

- Your data is always encrypted – even while being used.
- No decryption is ever needed – eliminating a big security gap.
- Quantum-secure by design – ready for the next era of threats.
- Compliance built-in – simplifying global data governance.

A Cybersecurity Solution

Cloud services is a huge industry ($885 billion) but with a major problem ~40% of clients experienced a breach in the last year.

The Solution:
Users submit their data to the cloud provider already FHE encrypted. This means the cloud provider can run all their operations on the encrypted files but only the client can read the results.

User:

Accesses and / or operates on data – results are encrypted and can be decrypted with their decryption key

Cloud Provider:

Can manage and back up the encrypted data files and can run managed services but cannot decrypt any results

The AI Data Problems

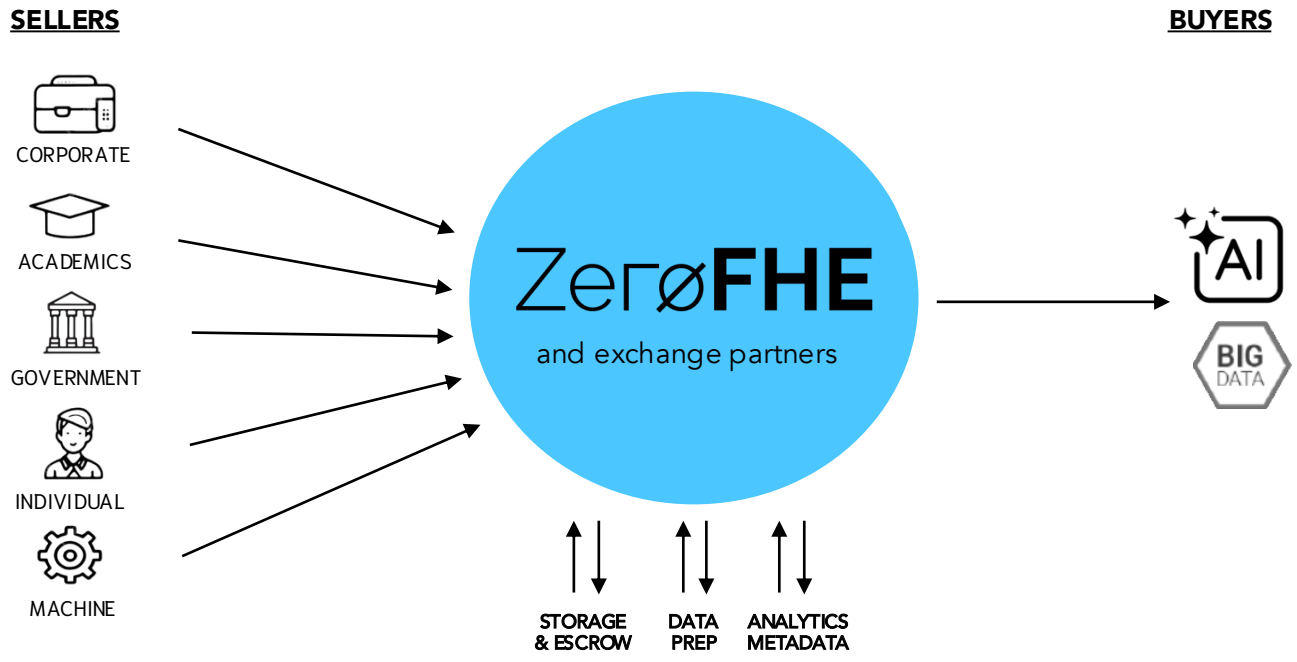
FHE solves several data privacy problems that plague AI:

- Training data can be encrypted – makes even confidential data available while maintaining privacy (99% of extant data is confidential and previously unavailable for AI training thus creating a data drought).
- Private enterprise AI models can protect proprietary data while enabling enterprise AI benefits
- Prompts can be encrypted – preserving confidentiality for AI clients
- Models can be encrypted – protecting the model's IP even if distributed

With **ZerøFHE** there will be no more data drought and confidentiality is maintained.

An AI Data Solution

Companies can convert their data into a profit center, either directly or with an exchange partner, without compromising privacy.



ZerøFHE will enable providers and users of data to interact and trade in a secure and confidential manner.

The Data Regulation Problem

Complex, Varying Regulations:
Navigating diverse laws (e.g., GDPR, HIPAA, CCPA, PIPL) with differing requirements across jurisdictions increases compliance costs and complexity.

Cross-Border Data Transfers:
Ensuring secure data movement between regions with strict residency rules (e.g., EU's Schrems II, China's PIPL) risks fines or data breaches.

High Penalties for Non-Compliance:
Violations can incur massive fines (e.g., €746M GDPR penalties in 2021), straining budgets and reputations.

A Data Regulation Solution

AI models can now be trained and run directly on encrypted confidential preserving complete privacy and regulatory compliance. ZeroFHE was used in three studies at Michigan University using HIPAA data to train an AI medical diagnostic model:

Classification of Personal Biomedical Data

The study applied Naive Bayes classification to breast cancer malignancy data, comparing cleartext and encrypted results. The encrypted data classification matched cleartext to four decimal points.

Analysis on Encrypted Medical Databases

An RLS function was run on time-series data from two medical databases with both cleartext and encrypted data. ZeroFHE was error free.

AI Classifications on Encrypted Medical Data

AI Classification was run on encrypted data sets for two medical databases. It was extremely fast and scalable.

1. Wood, Shpilrain, Najarian, Kahrobaei 2. & 3. Gribov, Horan, Kahrobaei, Souroushmehr, Shpilrain, Najarian

Thank You.

For a demo or source code please contact: pchapman@zerofhe.ai / +1 646.742.1000