César Soto Valero

Fully Homomorphic Encryption

César Soto Valero

Trustworthy AI

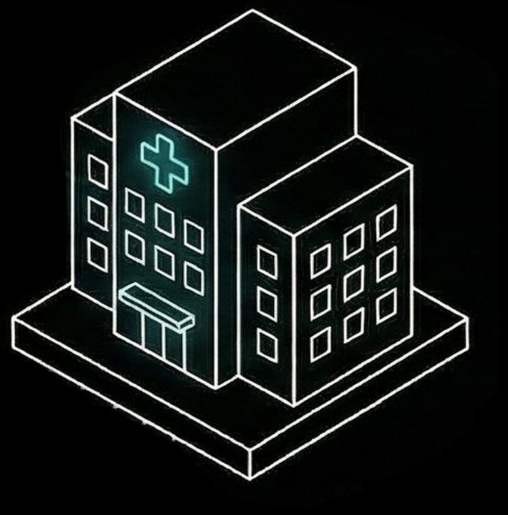
César Soto Valero

Fully Homomorphic Encryption and the Future of Trustworthy AI

César Soto Valero

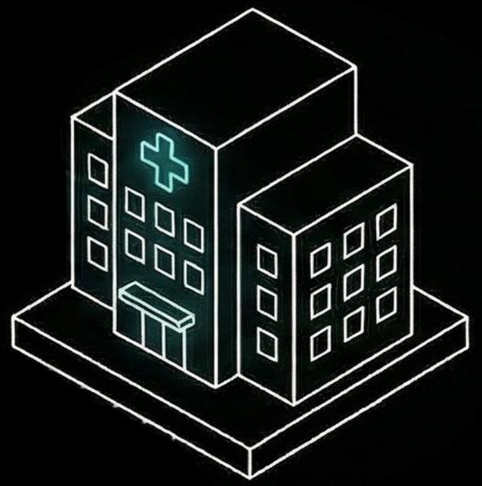
Trust

Trust



Healthcare

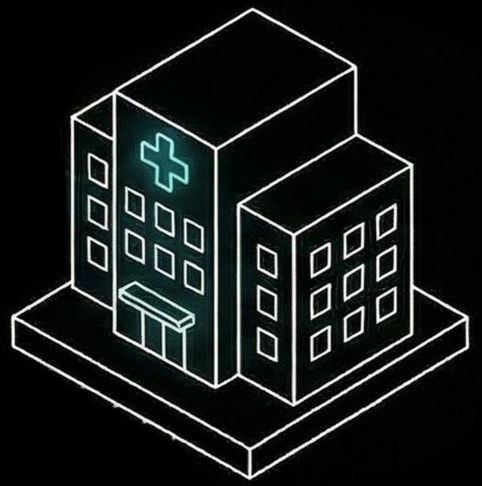
Trust



Healthcare

Education

Trust

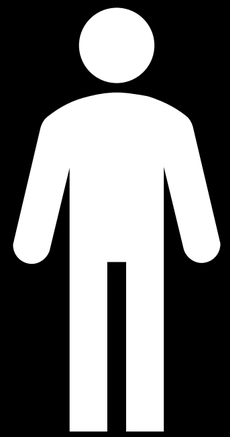


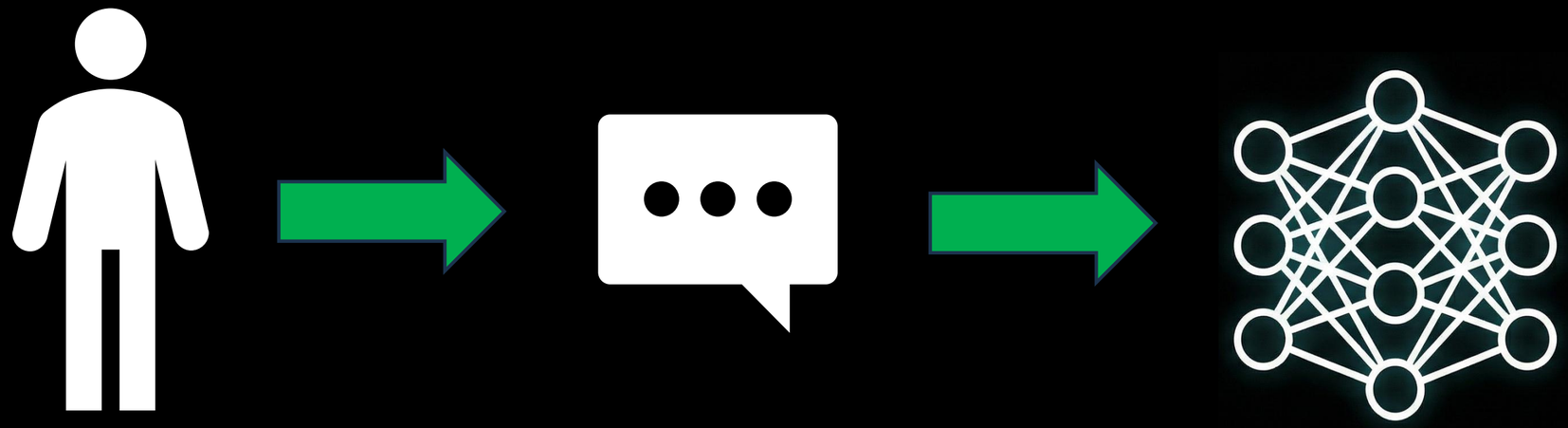
Healthcare

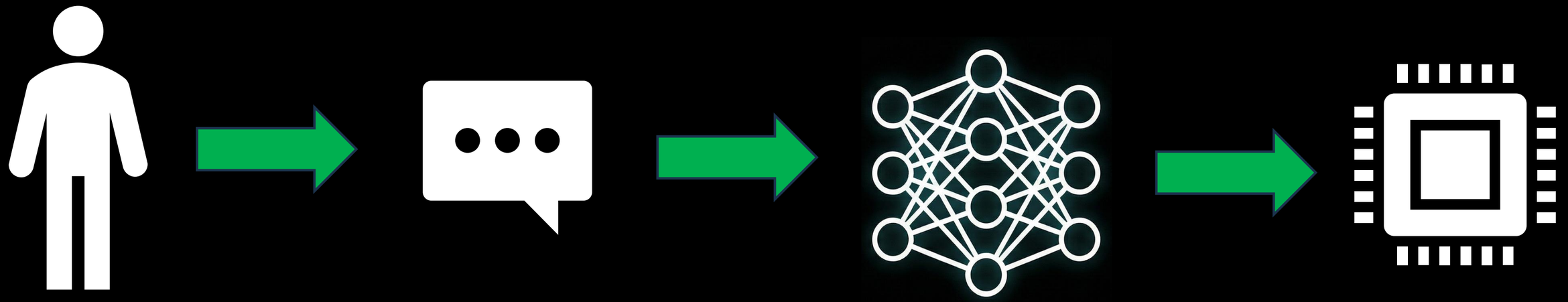
Education

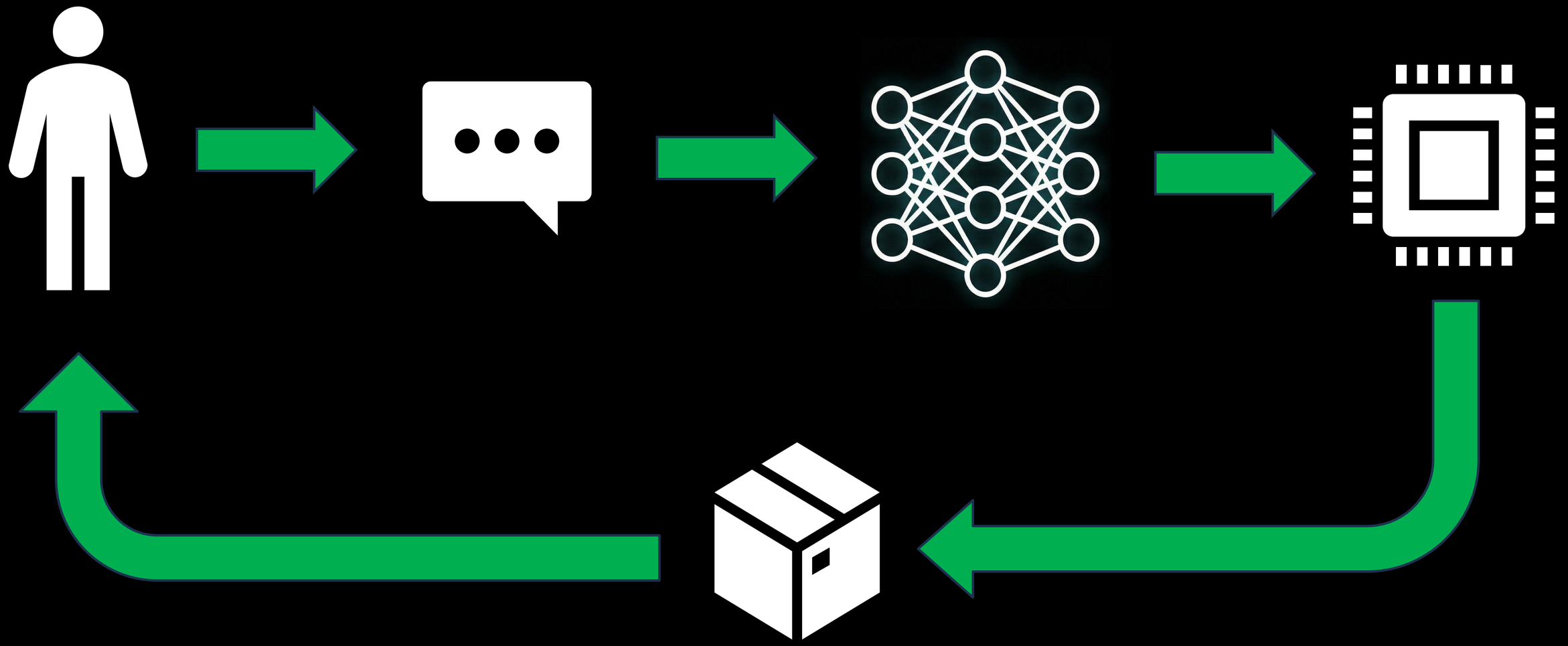
Finance

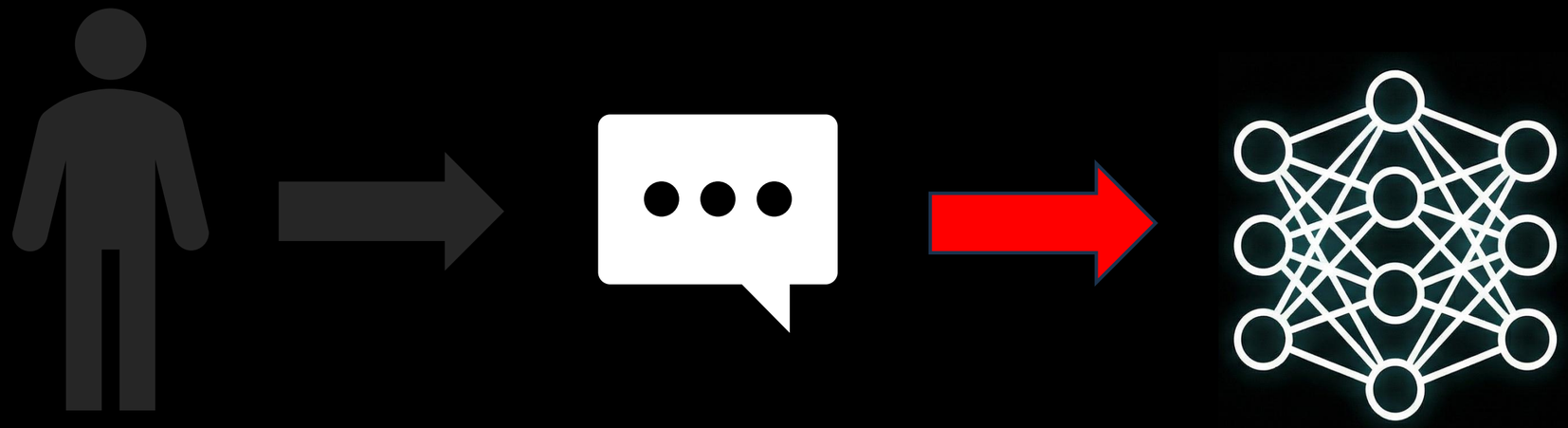
AI





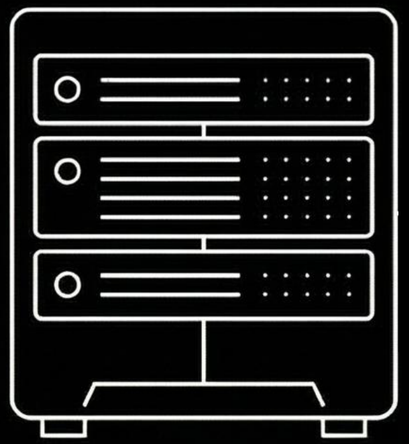






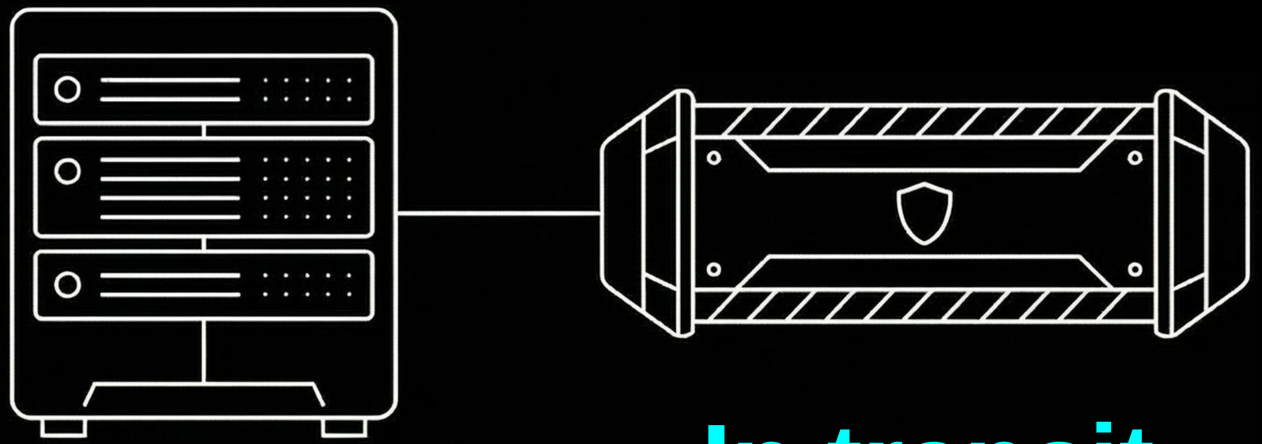
Data States

Data States



At rest

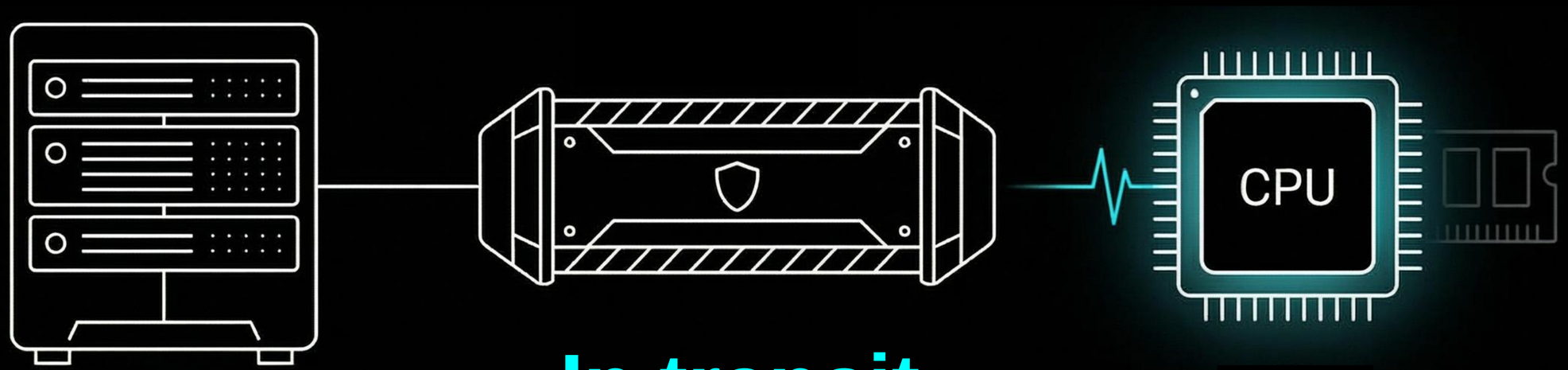
Data States



In transit

At rest

Data States

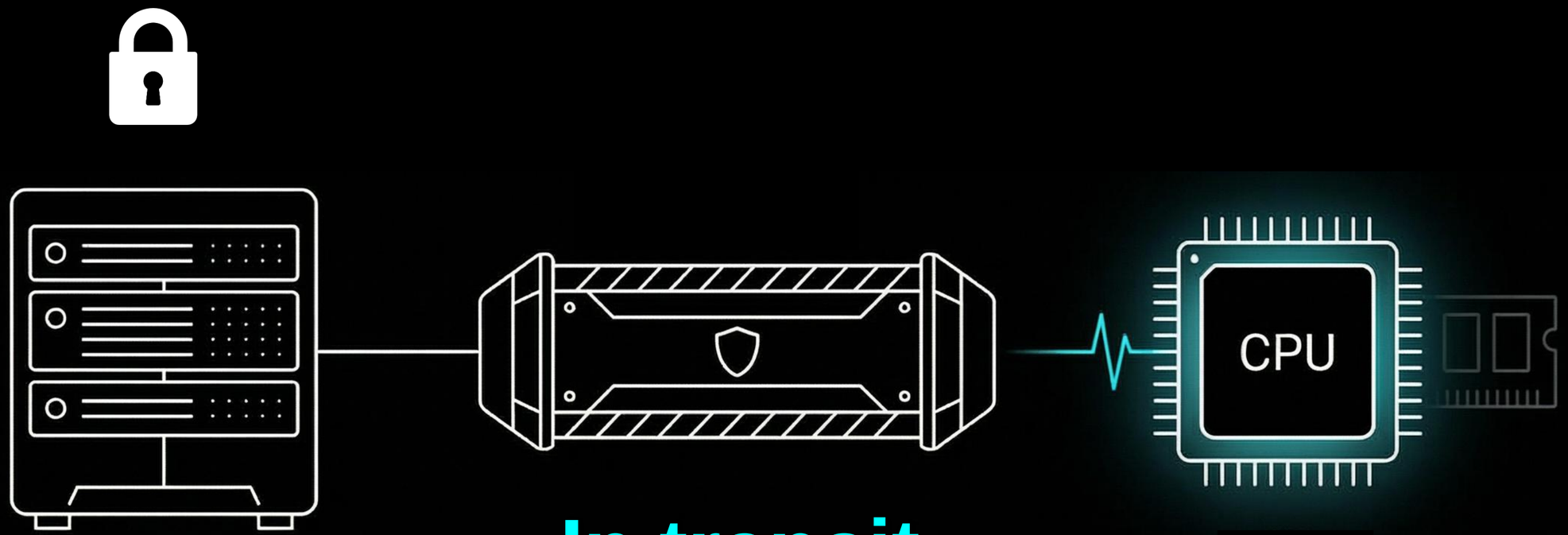


At rest

In transit

In use

Data States

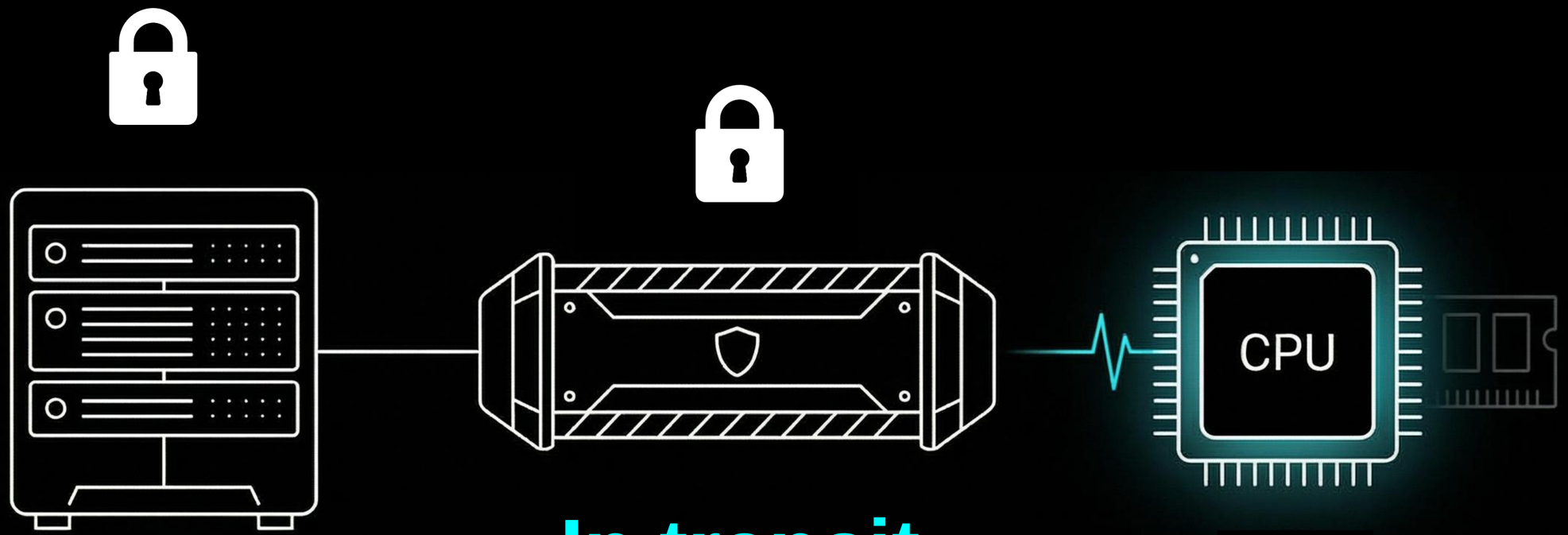


At rest

In transit

In use

Data States

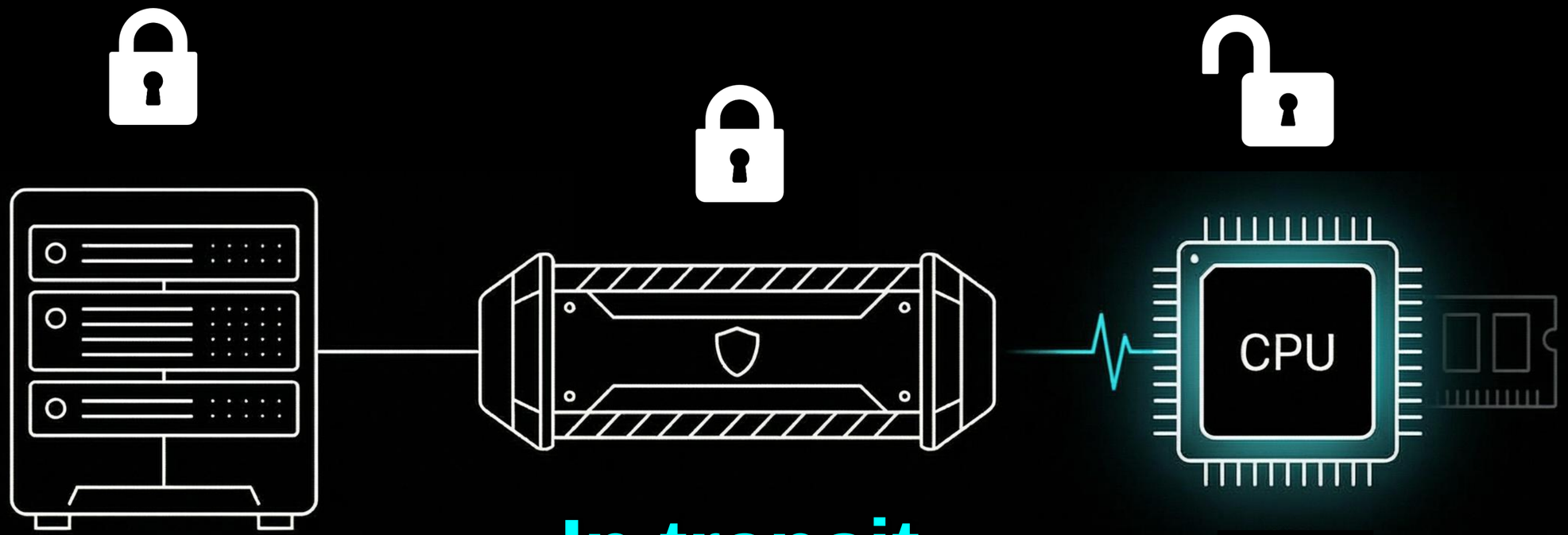


At rest

In transit

In use

Data States



At rest

In transit

In use

Data in Use Is Exposed

JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-069A

March 10, 2021

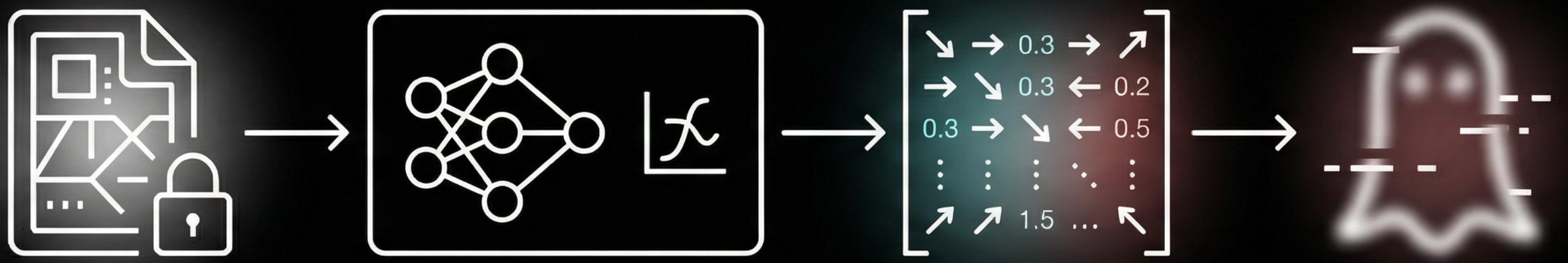
Compromise of Microsoft Exchange Server

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

SUMMARY

This Advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of vulnerabilities in Microsoft Exchange on-premises products. The FBI and CISA assess that nation-state actors and cyber criminals are likely among those exploiting these vulnerabilities. The exploitation of Microsoft Exchange on-premises products poses a serious risk to

Gradients can reveal data

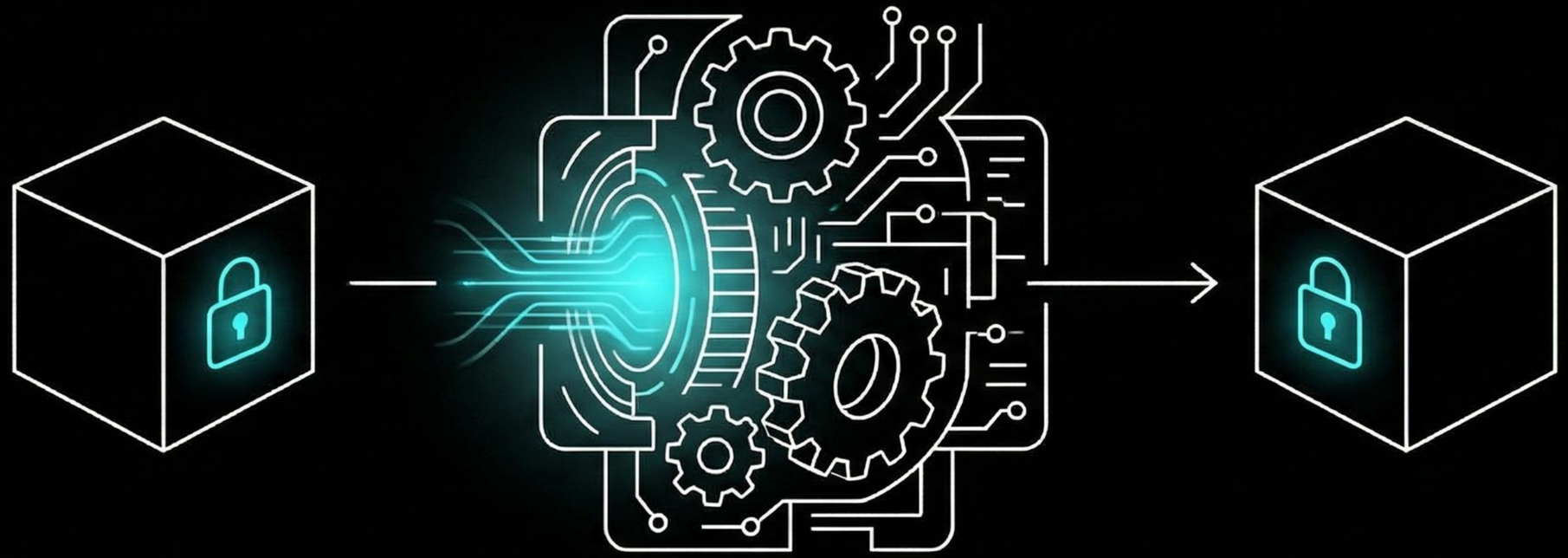


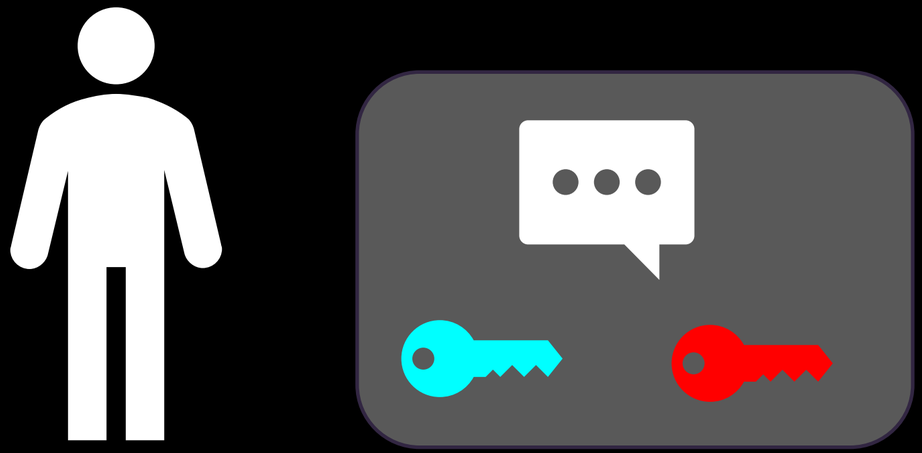
Zhu et al., “Deep Leakage from Gradients,” NeurIPS 2019

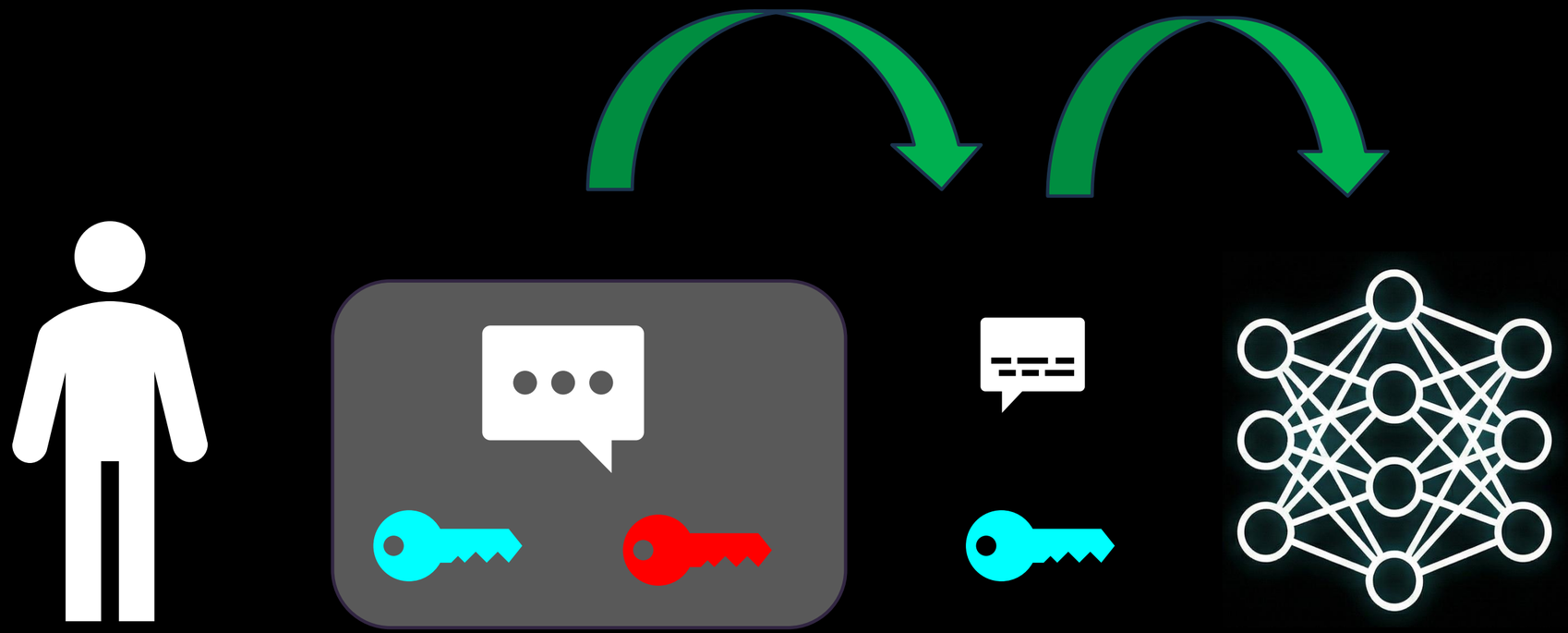
Solution?

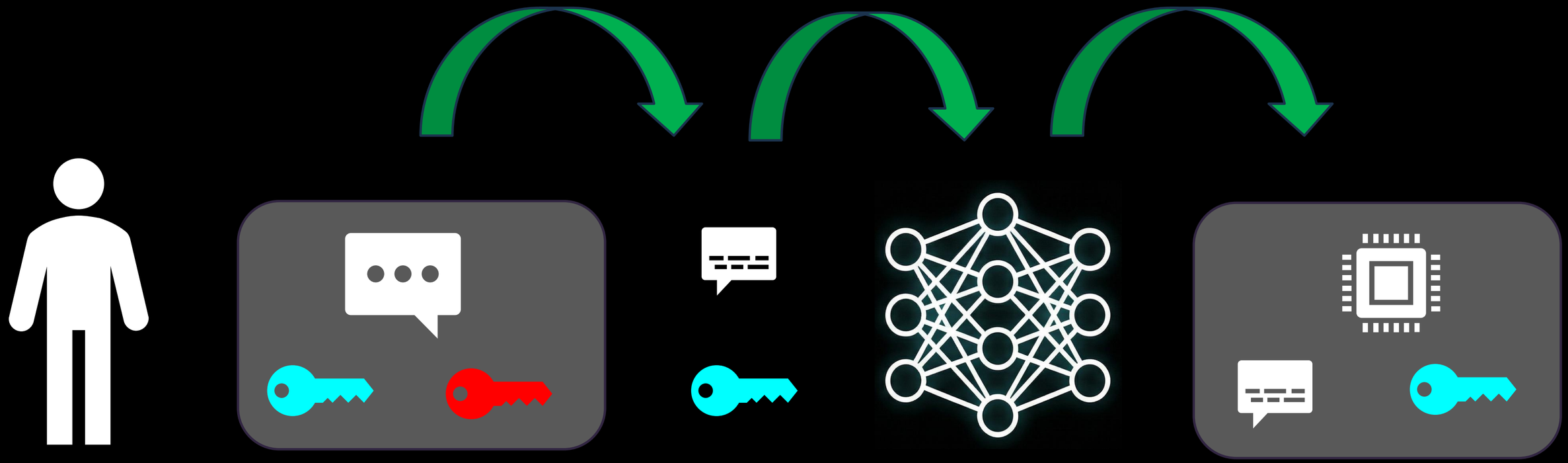
Fully Homomorphic Encryption

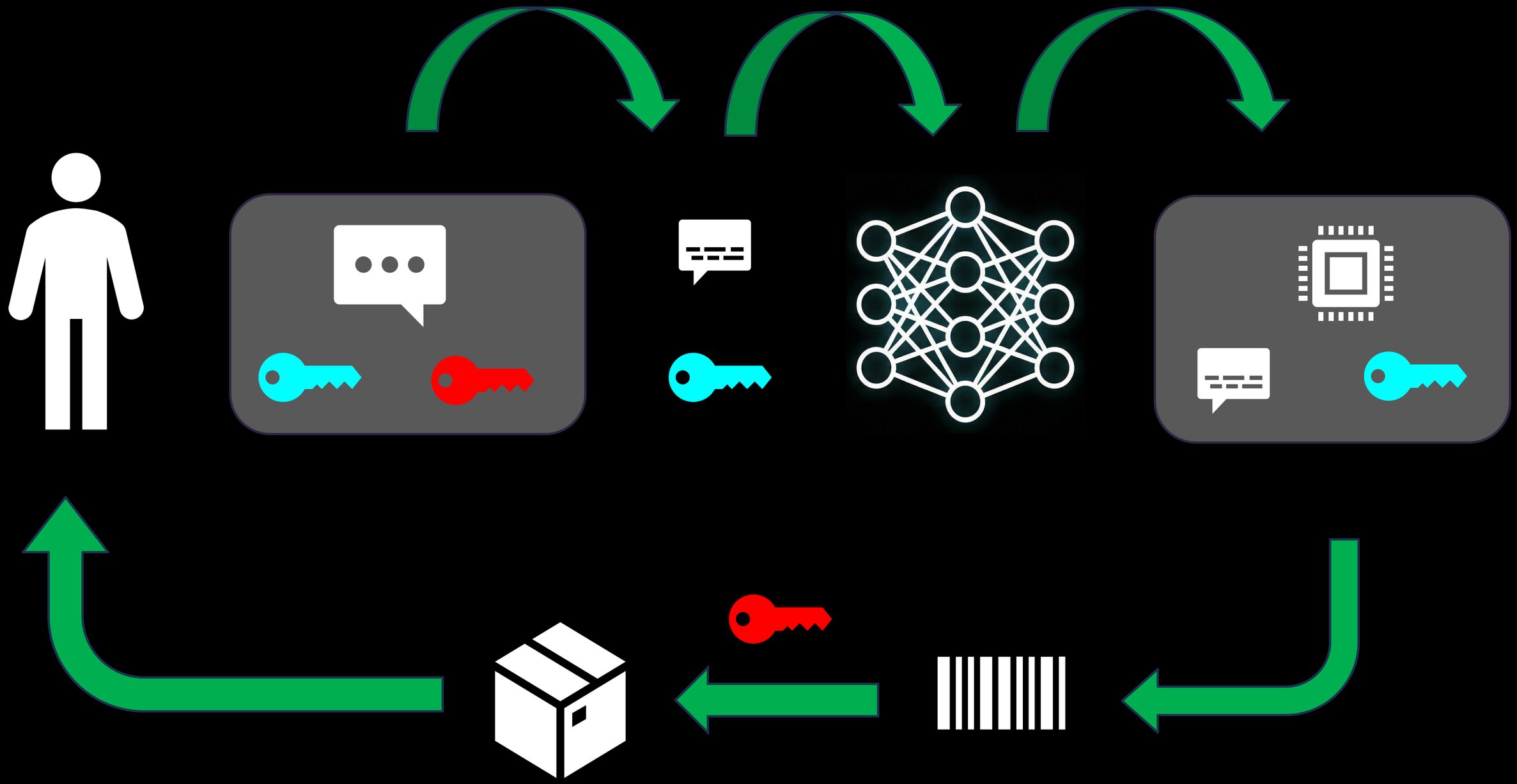
Computing on encrypted data



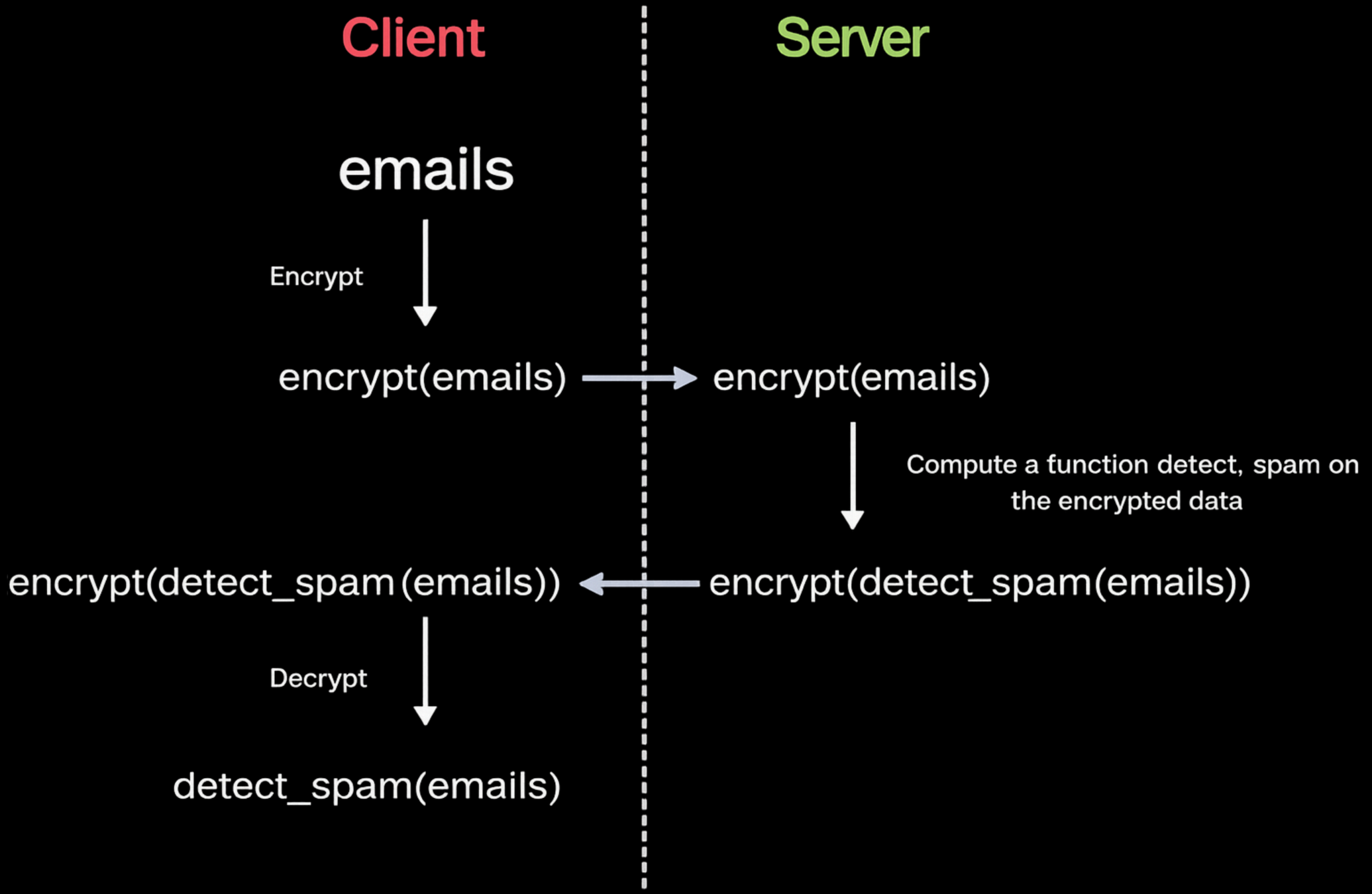




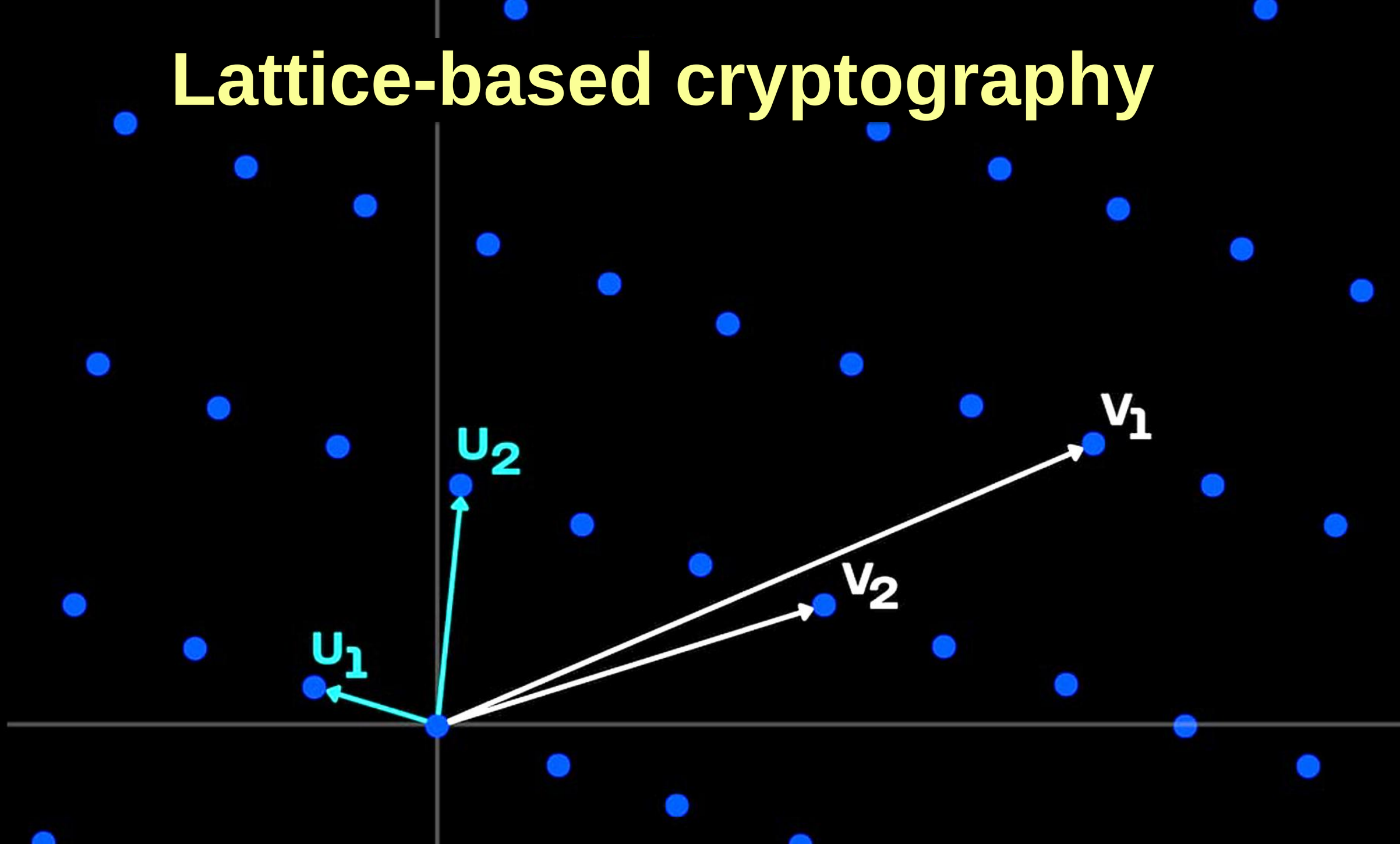




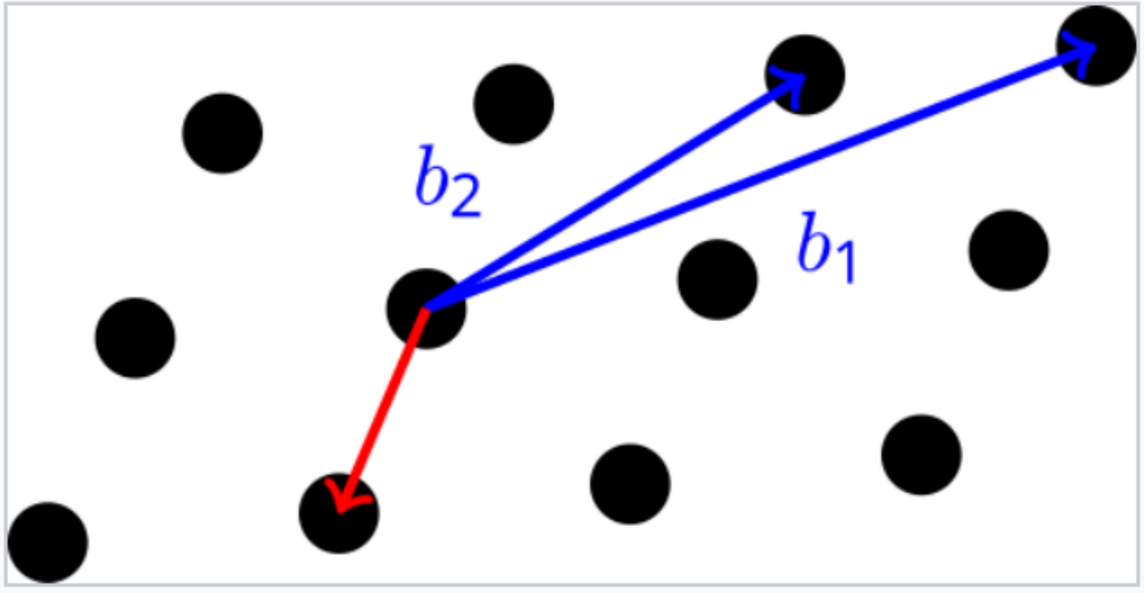
Example


Client
Server
emails
Encrypt
encrypt(emails)
encrypt(emails)
Compute a function detect, spam on the encrypted data
encrypt(detect_spam(emails))
encrypt(detect_spam(emails))
Decrypt
detect_spam(emails)

Lattice-based cryptography



Shortest vector problem (SVP) [edit]



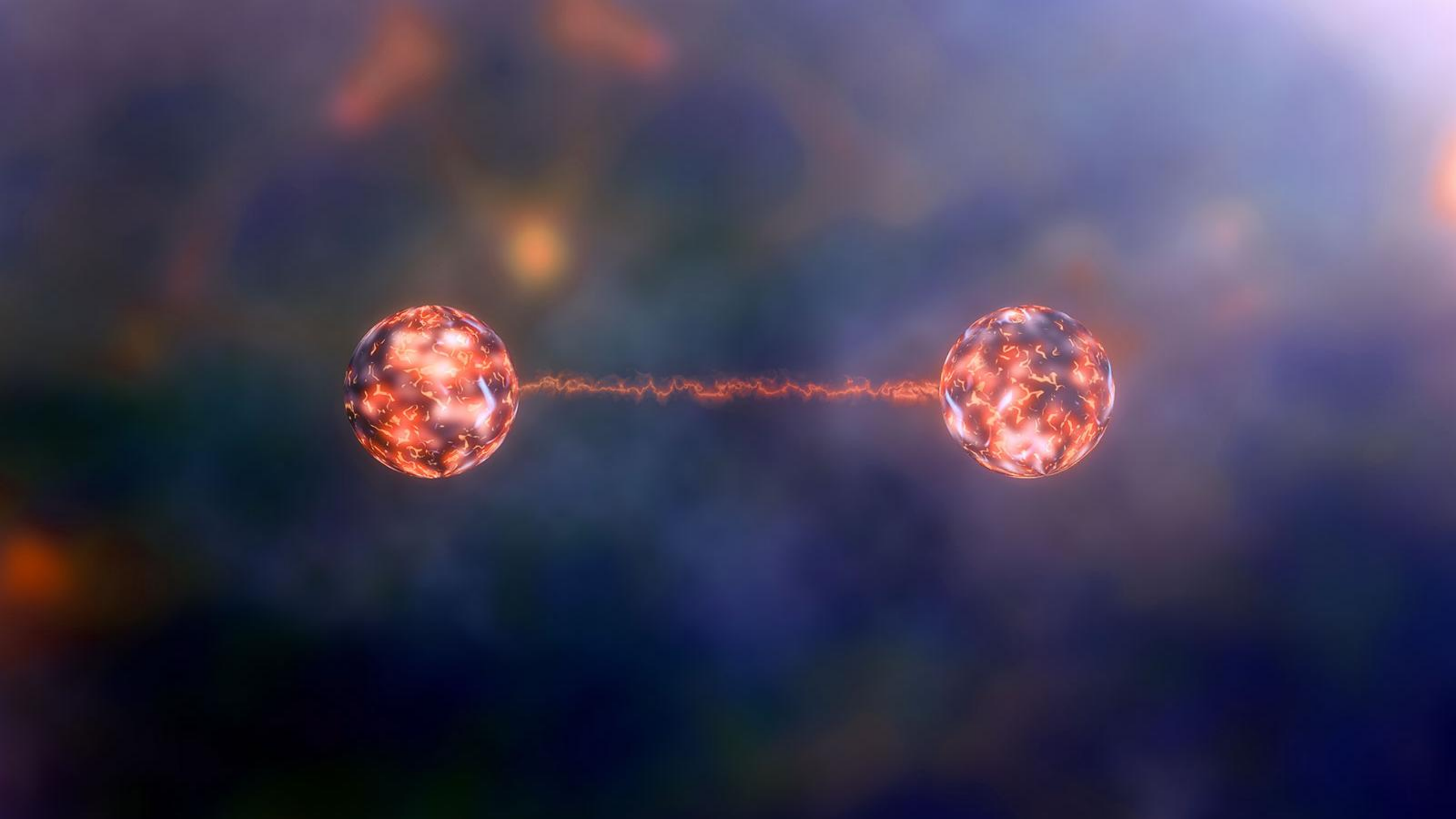
This is an illustration of the shortest vector problem (basis vectors in blue, shortest vector in red).

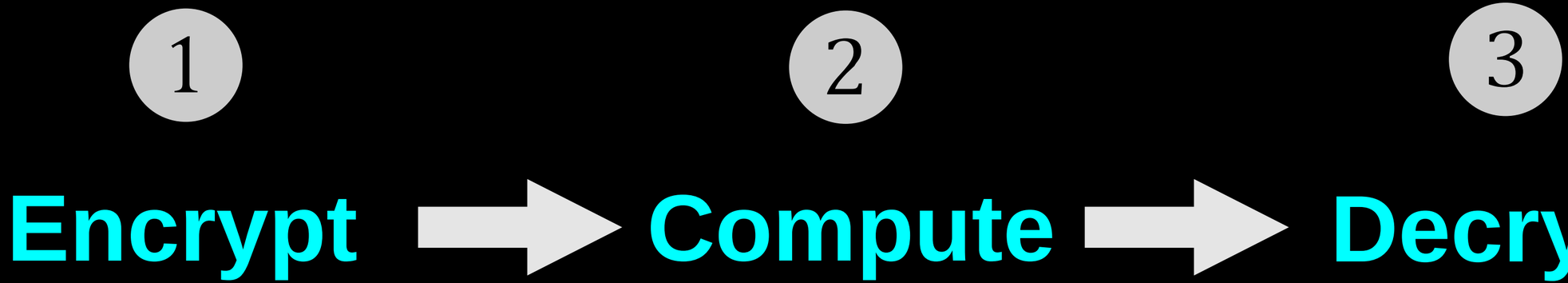
In the SVP, a basis of a vector space V and one must find the shortest non-zer words, the algorithm should output a no

In the γ-approximation version SVP_γ, o most $\gamma \cdot \lambda(L)$ for given $\gamma \geq 1$.

Hardness results [edit]

The exact version of the problem is onl reductions.[2][3] By contrast, the corresponding problem with respect to the unif




1
2
3
Encrypt
Compute
Decrypt

Moore’s Law of Fully Homomorphic Encryption

vitalik.eth
@VitalikButerin

Prediction:

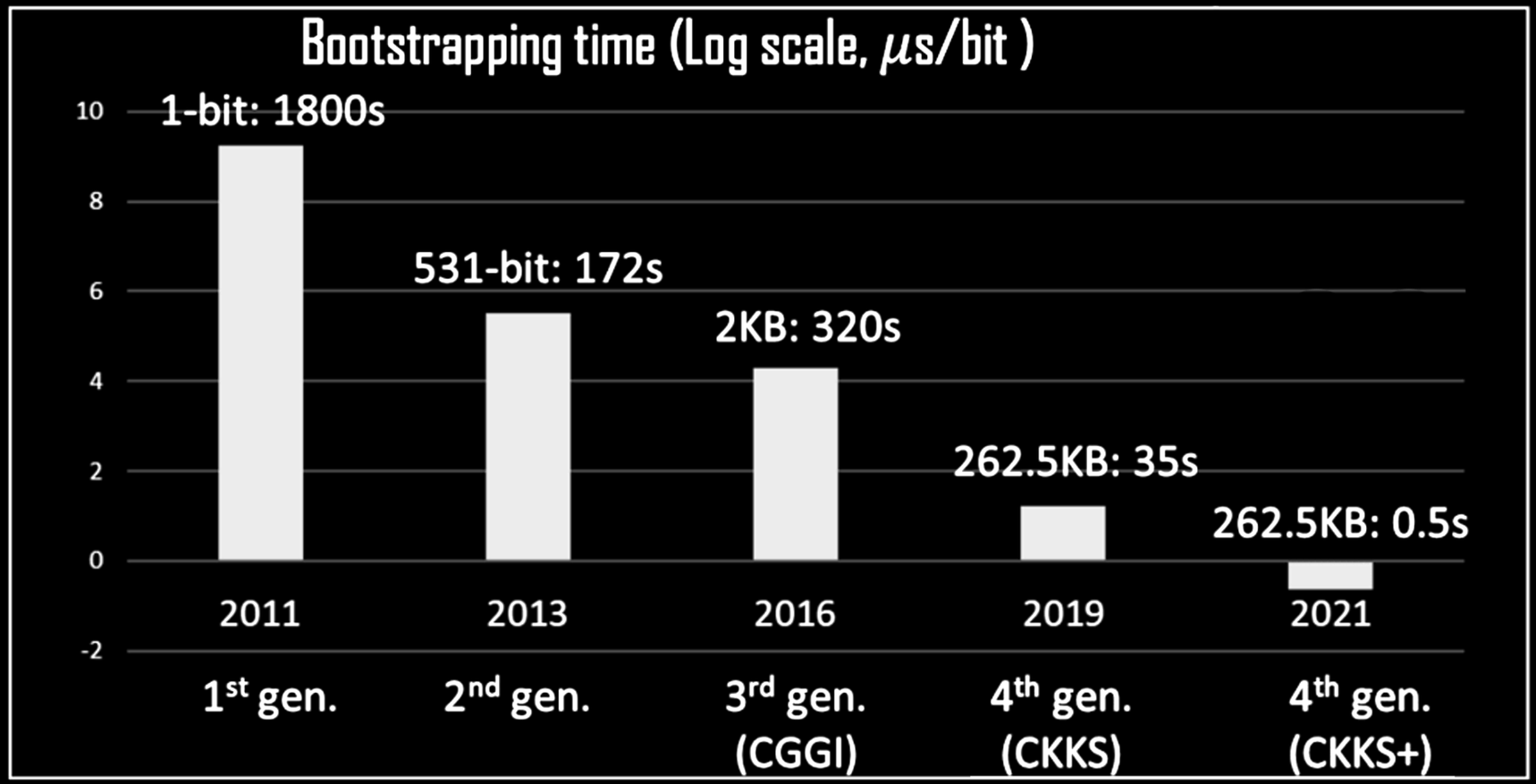
The megatrend in cryptography of the 2010s was elliptic curves, pairings and general purpose ZKPs/SNARKs.

The megatrend of the 2020s will be (in addition to broad adoption of the above) lattices, LWE, multilinear maps, homomorphic encryption, MPC and obfuscation.

4:08 AM · Apr 11, 2020

It is getting 8x faster every year

e.g. Bootstrapping time: the most time-consuming operation in HE



Homomorphic Encryption for Large Integers from Nested Residue Number Systems

Dan Boneh and Jaehyung Kim

Stanford University

dabo@cs.stanford.edu, jaehk@stanford.edu

June 10, 2025

Abstract

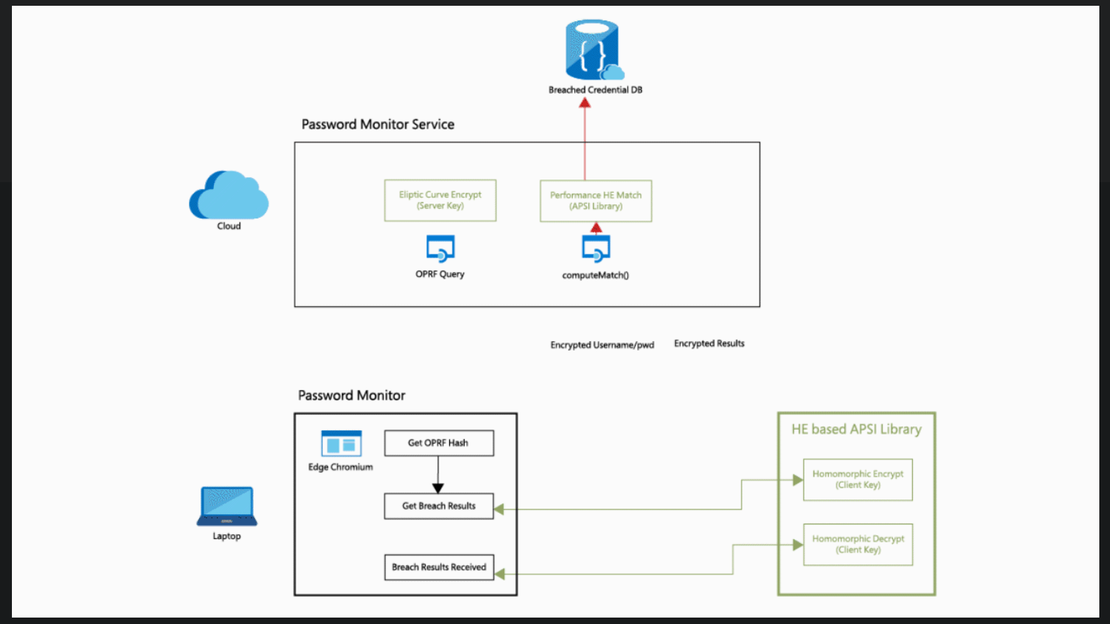
Existing fully homomorphic encryption (FHE) schemes primarily support a plaintext space defined over a relatively small prime. However, in some important applications of FHE one needs arithmetic over a large prescribed prime. In this paper we construct a new FHE system that is specifically designed for this purpose. Our system composes three layers of residue systems to enable much better performance than was previously possible. Our experiments show that for arithmetic modulo a 256-bit integer, when compared to the TFHE-rs implementation of 256-bit arithmetic, our new system achieves a factor of two thousand better multiplication throughput and a factor of twenty better latency. Moreover, for a 2048-bit prime modulus we achieve far better performance than was previously possible.

Applications

Password Monitor: Safeguarding passwords in Microsoft Edge

Published January 21, 2021

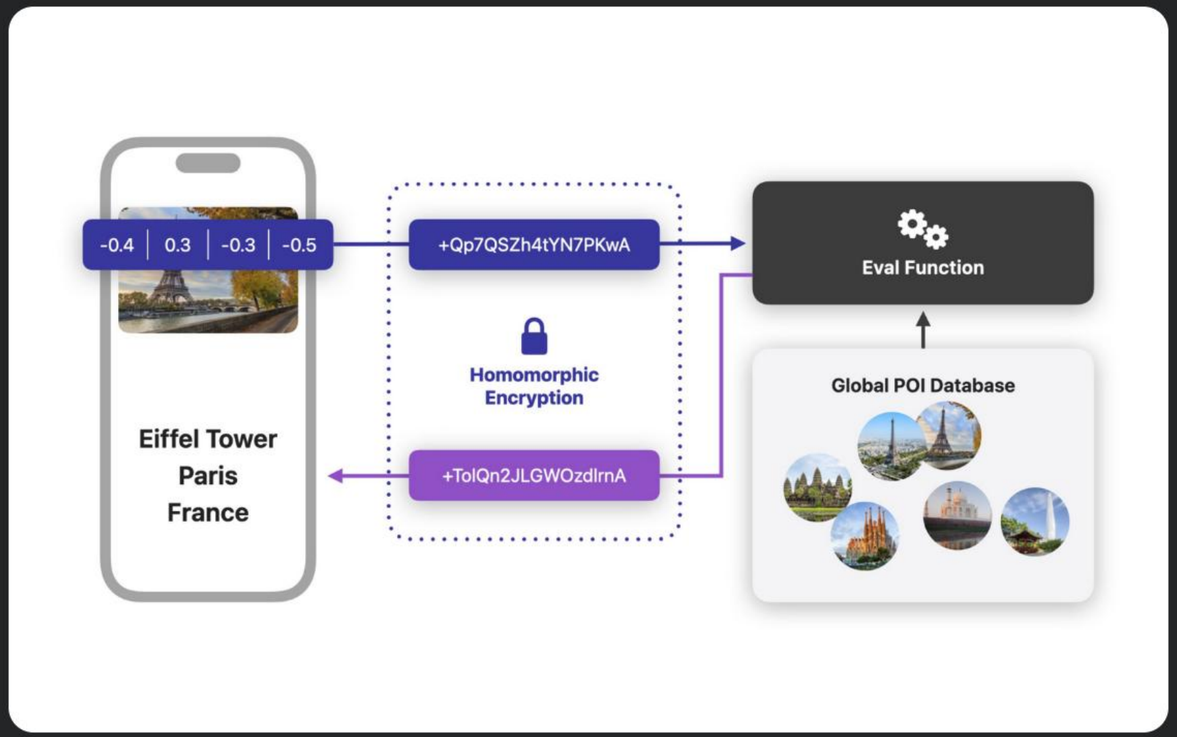
By Kristin Lauter, Principal Researcher and Partner Research Manager; Sreekanth Kannepalli, Principal Group Manager; Kim Laine, Principal Researcher; Radames Cruz Moreno, Senior Research SDE



Highlight | October 24, 2024

Privacy

Combining Machine Learning and Homomorphic Encryption in the Apple Ecosystem

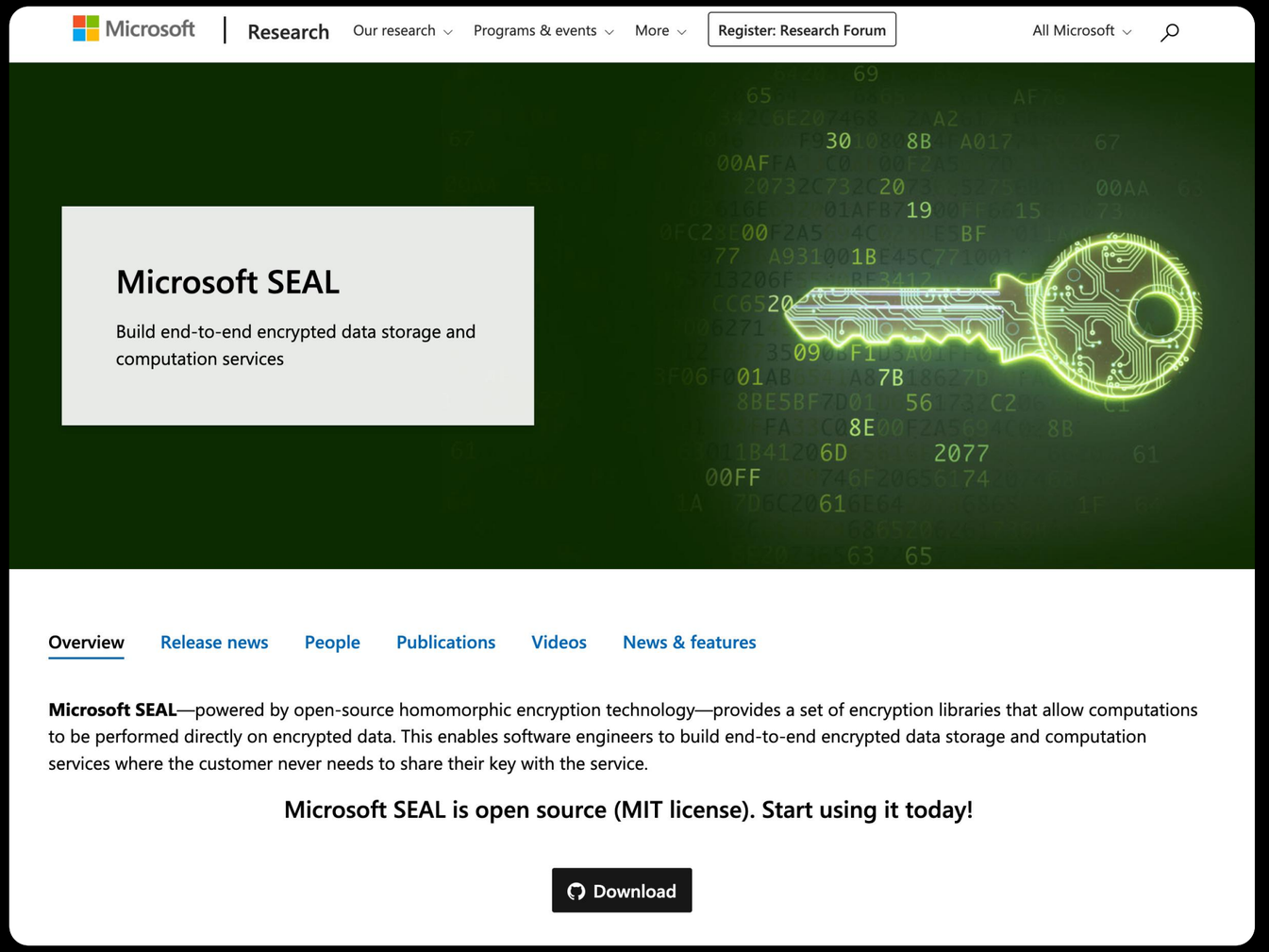


Using Private Nearest Neighbor Search for Enhanced Visual Search for photos.

Tools

SEAL

https://github.com/Microsoft/SEAL



HEIR

https://heir.dev

HEIR: Homomorphic Encryption Intermediate Representation

What is HEIR?

HEIR is a compiler toolchain for fully homomorphic encryption (FHE). We aim to be the industry-standard compiler for FHE. Application developers, compiler engineers, hardware designers, and cryptography researchers can build upon HEIR to accelerate the research and development of production-strength privacy-first software systems.

Why HEIR?

For application developers, HEIR aims to provide a simple entrypoint to start working with FHE. Write a program in Python, annotate the types to mark which are secret, and HEIR will compile the rest.

“Using encryption on the Internet is the equivalent of arranging an armoured car to deliver credit card information from someone living in a cardboard box to someone living on a park bench.”

– Gene Spafford (a.k.a Spaf)

cesarsotovalero.net