FHE That Ships:
Our Journey From Research to Real Deployment

Ajay Joshi
CipherSonic Labs

FHE Hardware Acceleration Summit
Stanford University

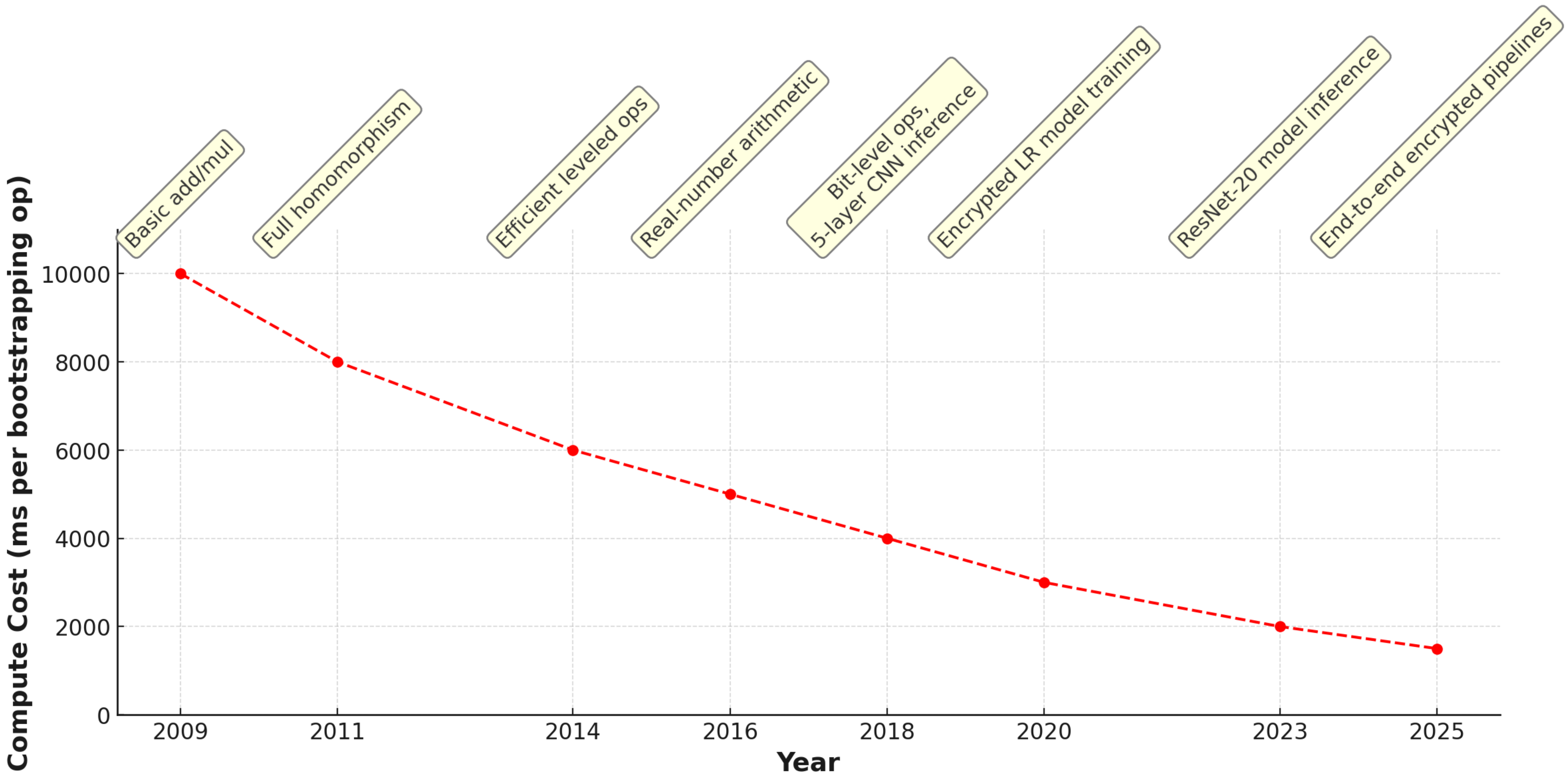
INCEPTION PROGRAM

Mentored by MIT Venture Mentoring Service

Ignition Award

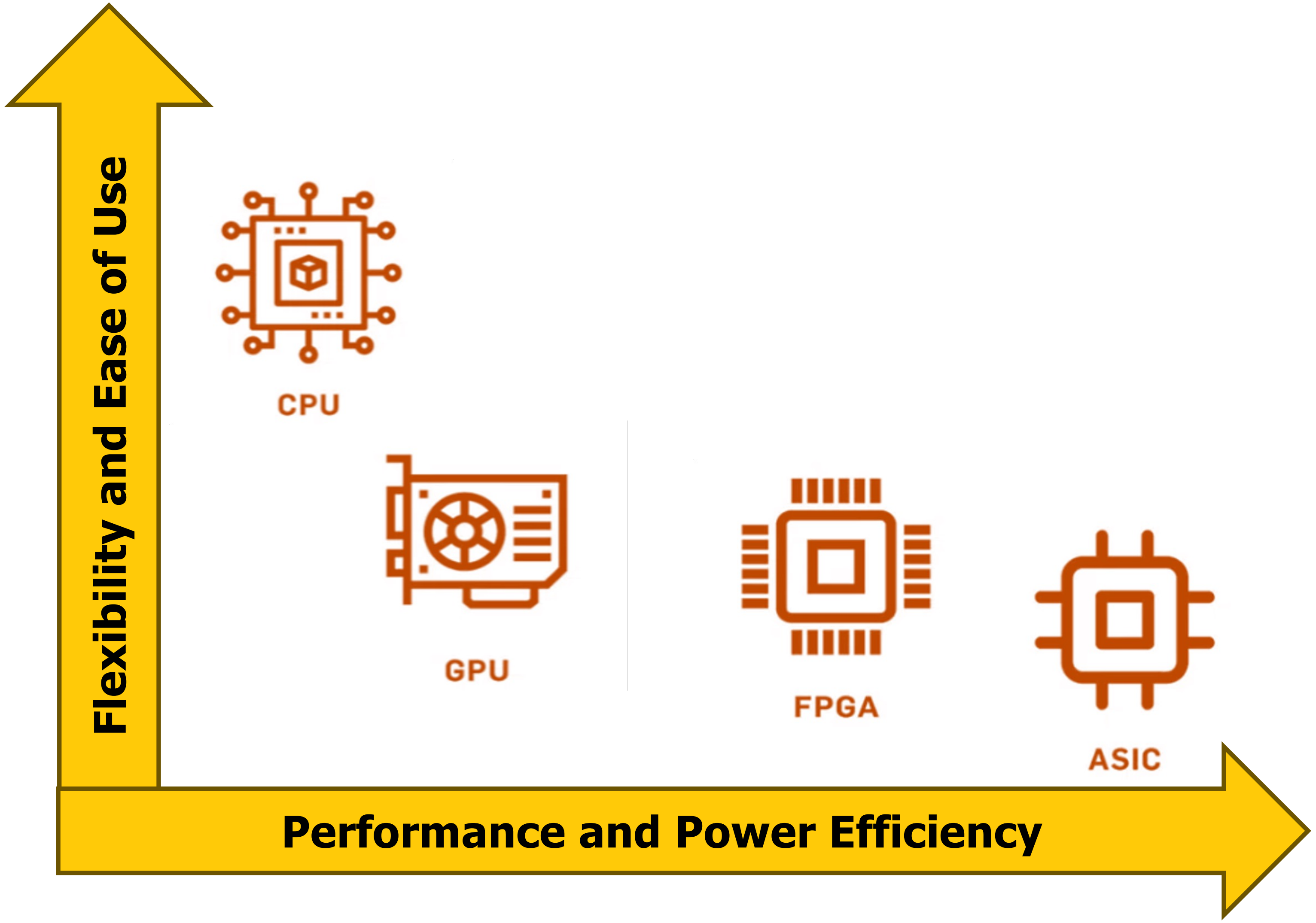
IDG CAPITAL STUDENT INNOVATION CENTER / BOSTON UNIVERSITY

FHE Landscape



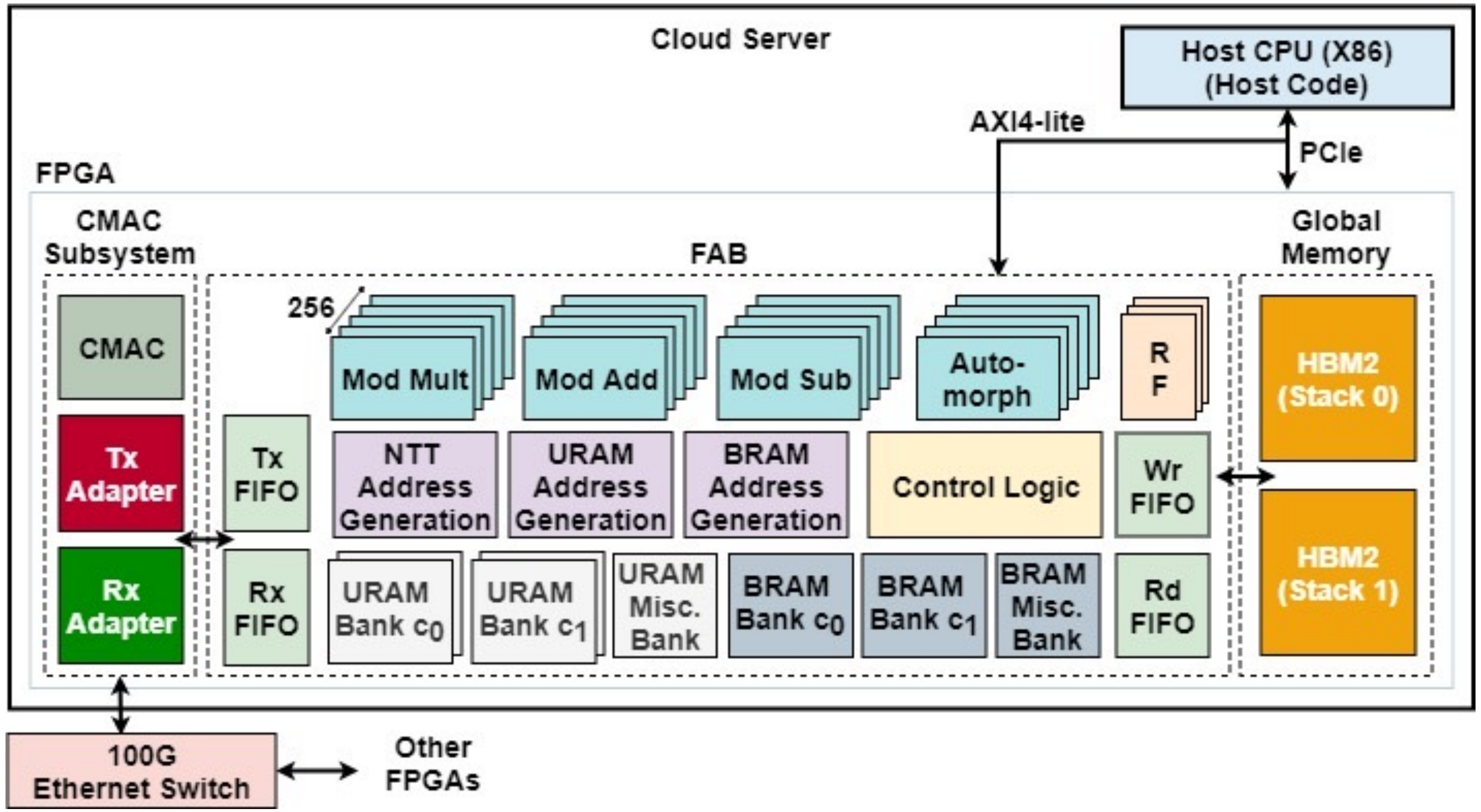
Algorithmic, hardware, and software optimizations have contributed

Why FPGAs are a natural fit?



- Reconfigurable architecture for FHE-specific optimization
- Custom memory hierarchy for primitive-level operations
- Compute units optimized for lower-frequency, high-efficiency execution

FAB highlights



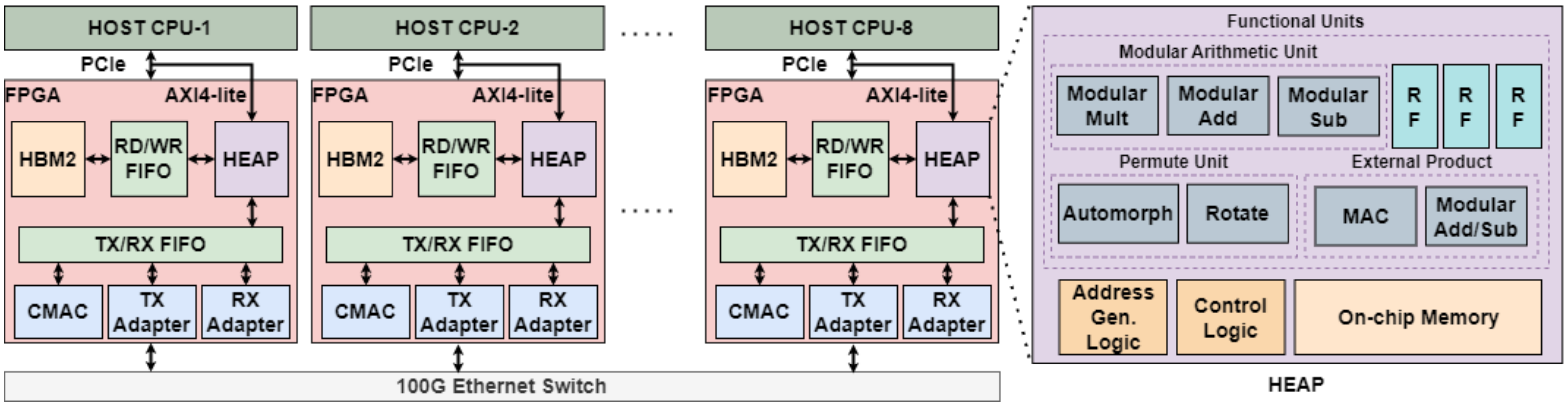
R. Agrawal et al., “FAB: An FPGA-based Accelerator for Bootstrappable Fully Homomorphic Encryption,” in Proc. IEEE International Symposium on High-Performance Computer Architecture (HPCA) 2023.

- Single FPGA architecture mapped to Alveo U280 FPGA accelerator card
- First ever 128-bit secure CKKS bootstrapping implementation on FPGA
- Bootstrapping and logistic regression model training
  - ~100x faster than CPU
  - ~10x faster than GPU
- When scaled to 8 FPGAs, performance limited by bootstrapping performance

CIPHERSONIC LABS

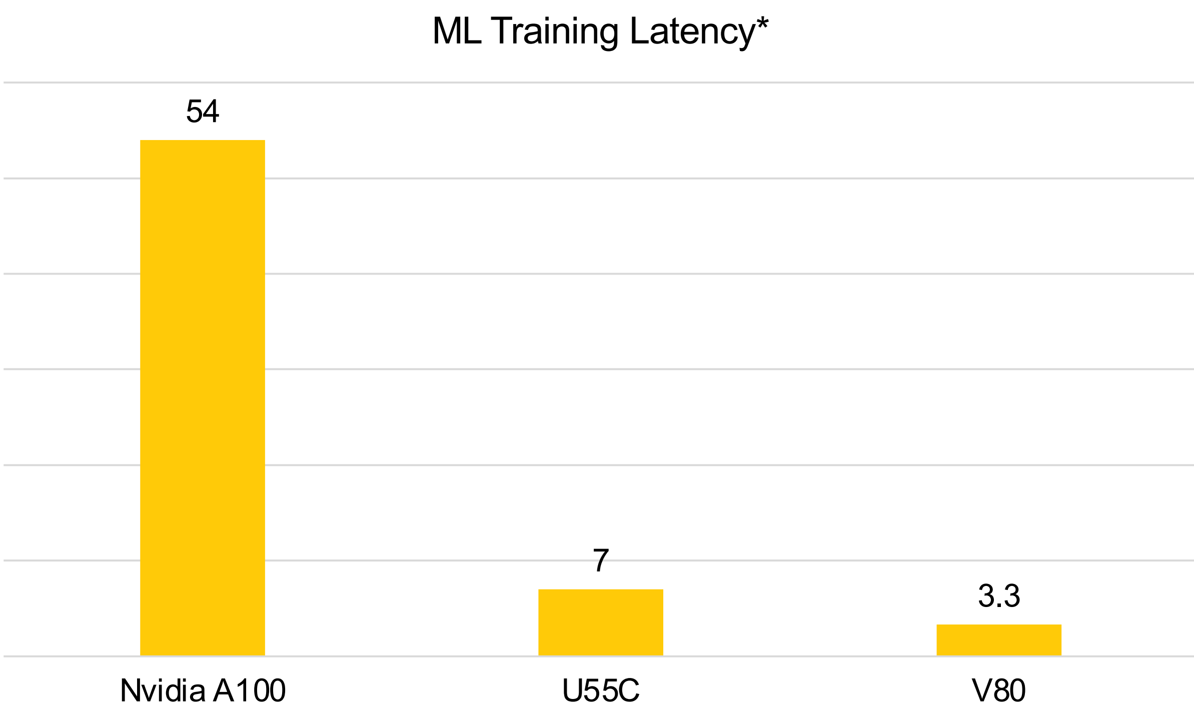
HEAP highlights

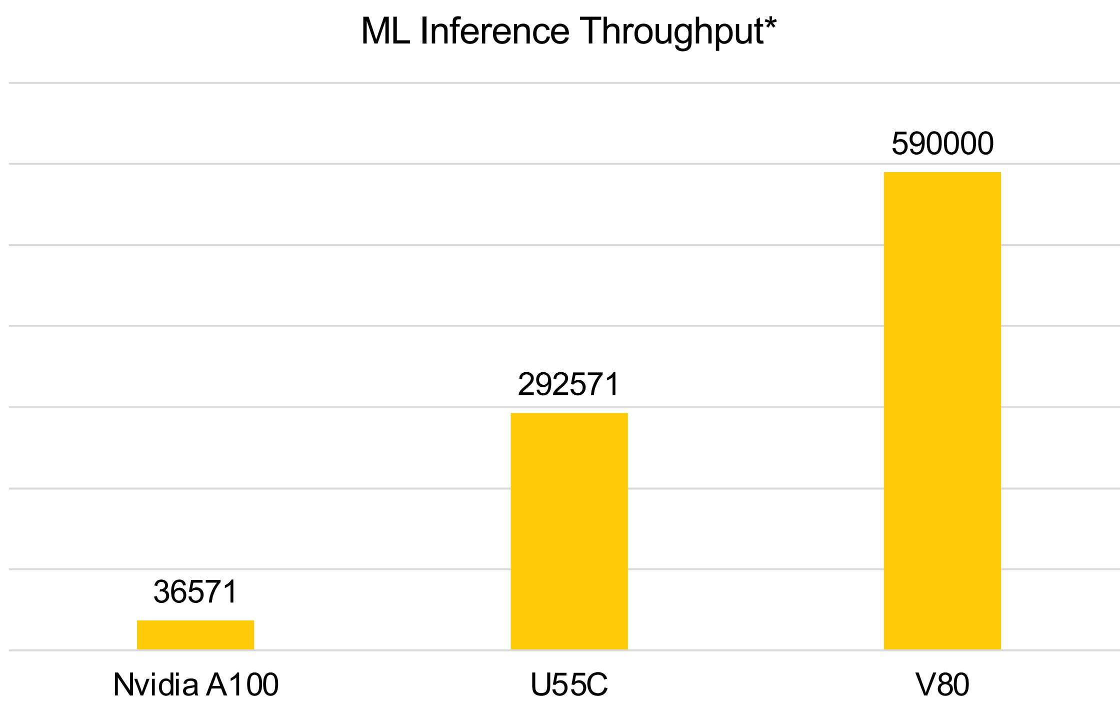
- Scalable bootstrapping accelerator → Multi-FPGA system
  - Parallelizable bootstrapping using scheme switching
  - ~15x better bootstrapping performance compared to FAB
  - ~11x better performance for logistic regression over 8-FPGA FAB



R. Agrawal et al., "HEAP: A Fully Homomorphic Encryption Accelerator with Parallelized Bootstrapping," in Proc. International Symposium on Computer Architecture (ISCA) 2024.

Performance – Credit card fraud detection





*Latency measured in milliseconds per training iteration

*Throughput measured in credit card transactions per second

Solutions Brief with AMD:
https://www.amd.com/content/dam/amd/en/documents/products/accelerators/alveo/v80/cipherSonic-solution-brief.pdf

CIPHERSONIC LABS

MVP live on AWS (Looking for early adopters)

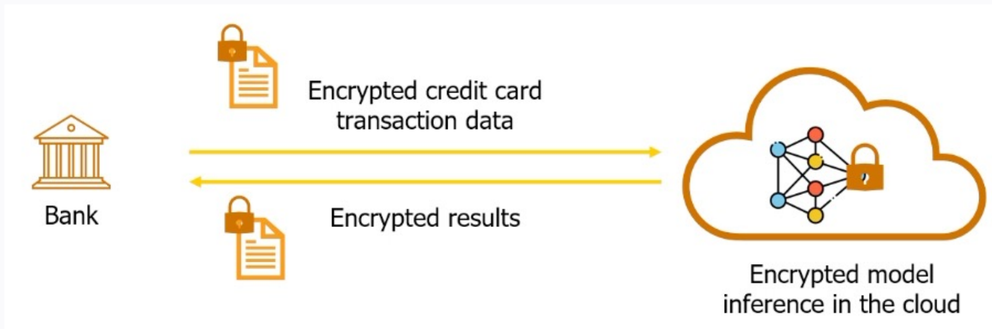
CIPHERSONIC LABS

Home Products About Us Blogs News Contact Us Try Demo

Credit Card Fraud Detection

According to WalletHub, the total value of credit card fraud surged to $246 million in 2023, reflecting a significant 12% increase from the previous year. This concerning rise has pushed credit card companies to explore innovative ways to prevent, detect, and mitigate fraud. Machine Learning stands out as a powerful tool in the fight against credit card fraud, with a well-trained Logistic Regression (LR) model offering the ability to assess whether a transaction is fraudulent, thereby reducing business risks and financial losses.

How does credit card fraud detection work with Fully Homomorphic Encryption (FHE)? FHE enables the creation of a fraud detection system that utilizes encrypted transaction data and encrypted model weights. In this setup, the LR model is trained on encrypted data to serve as a fraud detector. Once trained, the encrypted model can perform inference on new encrypted transaction data, ensuring enhanced security and protecting customer privacy. This method eliminates the need for anonymizing or depersonalizing data through third-party services.



Choose the transaction you want to verify

Call for action - Compiler stack for FHE on FPGAs

- What's missing today
  - No open-source, end-to-end compiler targeting FPGAs for FHE workloads

- What we need to build together
  - IR (Intermediate Representation) for encrypted ops targeting hardware
  - RTL & HLS codegen hooks for common FHE op-sets for CKKS
  - Integration with existing homomorphic libraries (OpenFHE, SEAL, Concrete)
  - Tooling for debugging and verifying encrypted dataflow

- Open sourcing is the way to go
  - This infrastructure should be open-source, accessible, and vendor-neutral
  - Collaborators can plug in passes, optimizations, backend targets

Summary

- FHE-based computing is becoming practical
- FPGAs provide a sweet spot for FHE acceleration
  - Existing clouds have FPGA COTS
  - Practical performance at a fraction of ASIC cost
- For widespread FHE adoption
  - Standardization of FHE algorithms
  - Proven use cases and success stories

ajay@ciphersoniclabs.io
rashmi@ciphersoniclabs.io