encrypt

A scalable and practical privacy-preserving framework

Hardware Acceleration

GPU Acceleration for Fully Homomorphic Encryption

Why GPU for FHE?

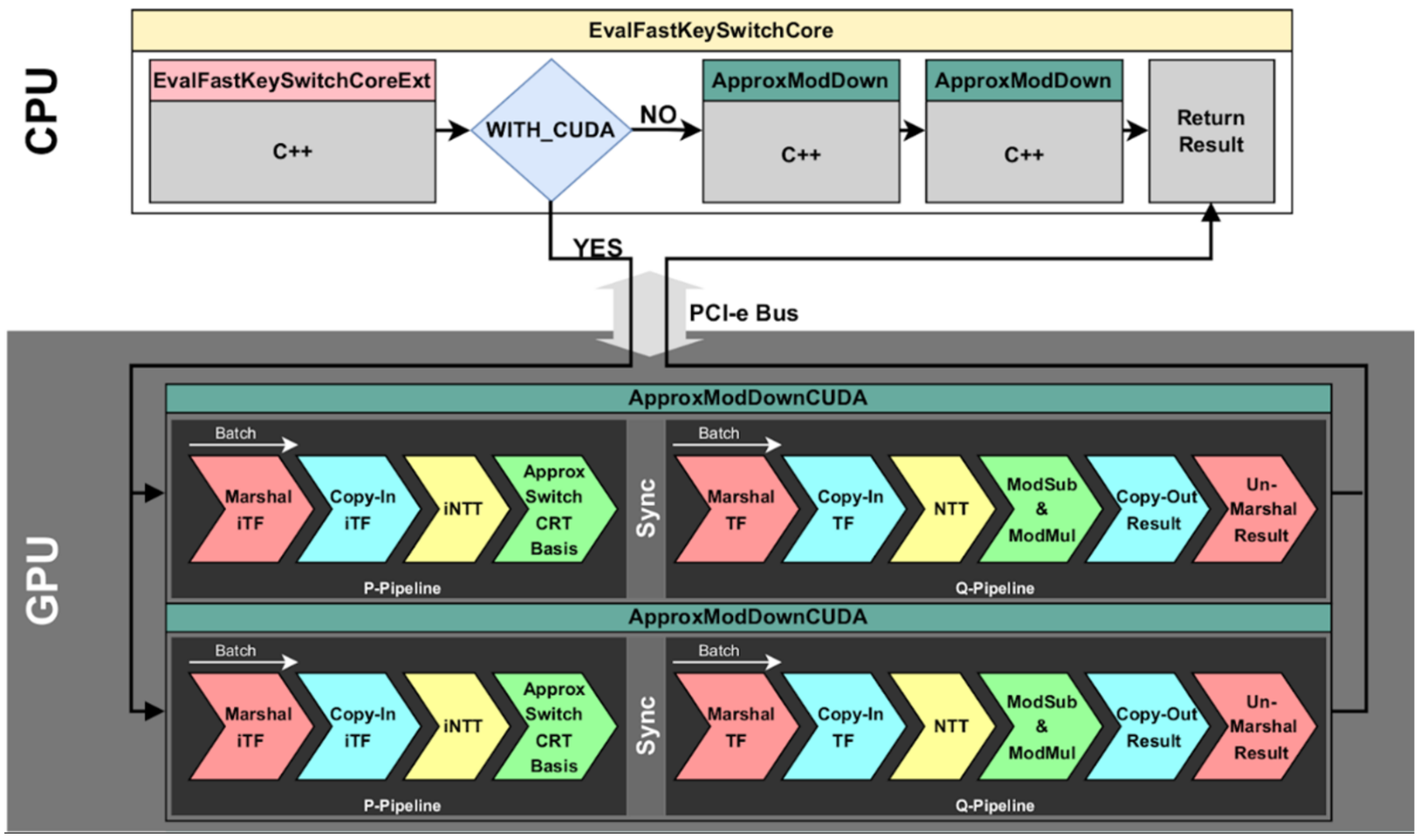
- FHE is secure but computationally intensive
- GPUs excel at parallelism → ideal for speeding up FHE
- No existing GPU support for BGV in OpenFHE → we fill that gap

What we Did?

- Profiled OpenFHE → identified bottlenecks
- Offloaded code to GPU
- Enabled 128-bit integer support
- Integrated seamlessly into OpenFHE
- Reduced data transfer cost using batch

Metric	Description
Speedup	4.58×
End-to-End Speedup	1.08× (depth 24)
Throughput Gain	+16%
Bottleneck at Low Depths	Data transfer & marshaling

Open Source Repository



Key Takeaways

- Best suited for deep FHE workloads
- Modular integration with OpenFHE
- Data movement optimization is key
- Enables real-world GPU-secure computing

In addition, this work is funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee for grant number 10039809.

Funded by the European Union

This work is supported by the European Union's Horizon Europe programme under grant agreement No 101070670.

Disclaimer: Views and opinions expressed are those of the ENCRYPT consortium authors only and do not necessarily reflect those of the European Union or its delegated Agency DG CNECT. Neither the European Union nor the granting authority can be held responsible for them.