SCIENCE ▪ PASSION ▪ TECHNOLOGY

Aloha-HE

A Low-Area Hardware Accelerator for Client-Side Operations in Homomorphic Encryption

Florian Krieger, Florian Hirner, Ahmet Can Mert, Sujoy Sinha Roy

Institute of Applied Information Processing and Communications ■ Inffeldgasse 16a, 8010 Graz, Austria ■

Institute of Applied Information Processing and Communications, Graz University of Technology
{florian.krieger, florian.hirner, ahmet.mert, sujoy.sinharoy}@iaik.tugraz.at

Homomorphic Encryption (HE)

What is it about?

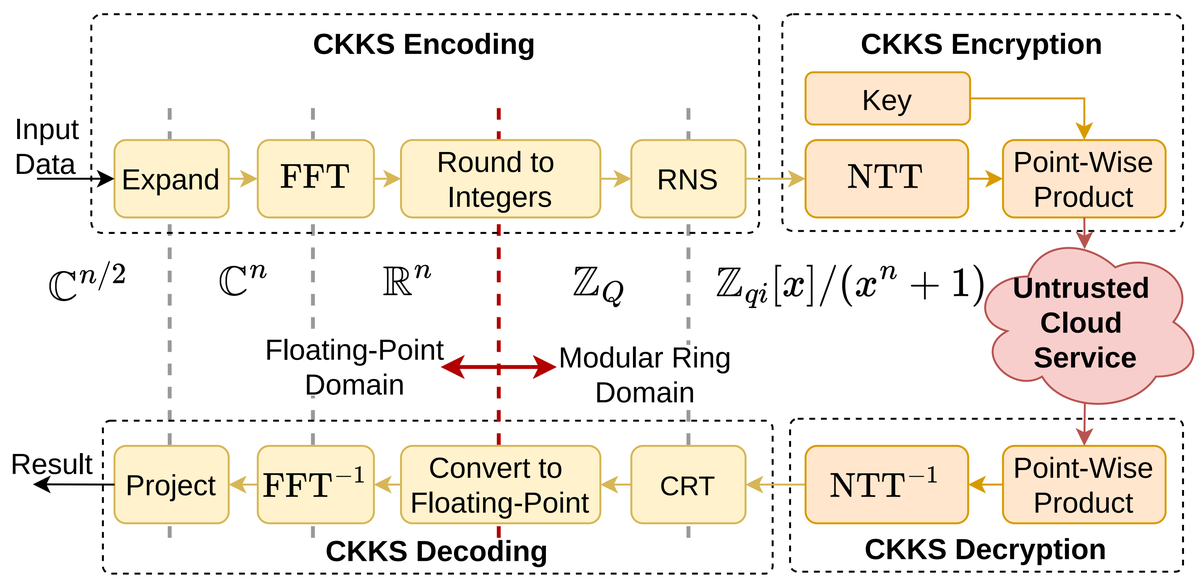
Homomorphic encryption (HE) is in the limelight of contemporary research since it allows computations directly on encrypted data. Sensitive data can remain encrypted when sending, storing, and evaluating on untrusted platforms. This property opens novel opportunities in privacy-preserving cloud computing.

Why is dedicated hardware needed?

Besides its benefits, HE comes with the drawback of huge performance overheads preventing its practical adoption. Latest research improves this limitation via hardware acceleration of server-side operations. **Yet, only little focus has been given to client-side operations** which are mathematically involving and computationally expensive.

The CKKS scheme

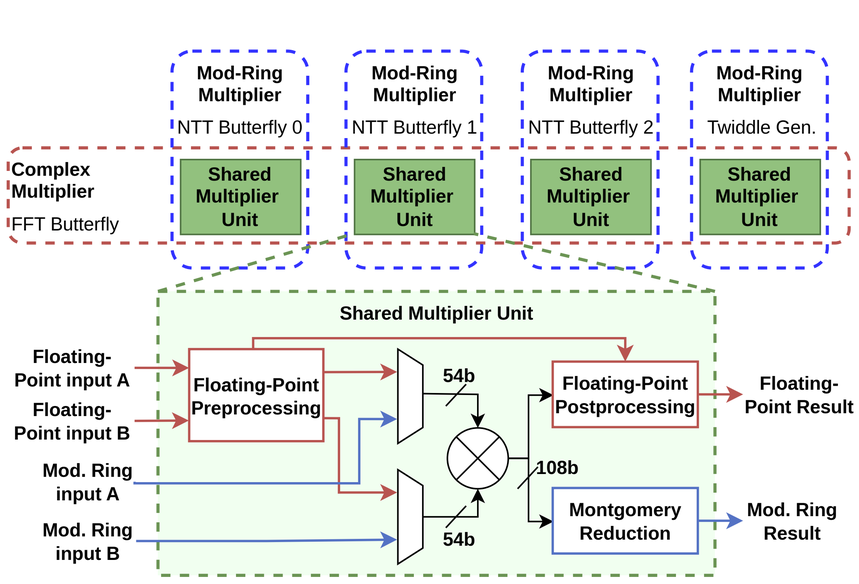
- State-of-the-art HE scheme
- Homomorphically computes on floating-point numbers
  - Suited for AI tasks
- Uses *Approximate Arithmetic* with special encoding
  - Encodes complex-valued input to polynomial ring element
  - Uses a Fast Fourier Transformation for encoding
  - Encoding is the main difference from other HE schemes
- Relies on Ring-LWE to encrypt the encoded data

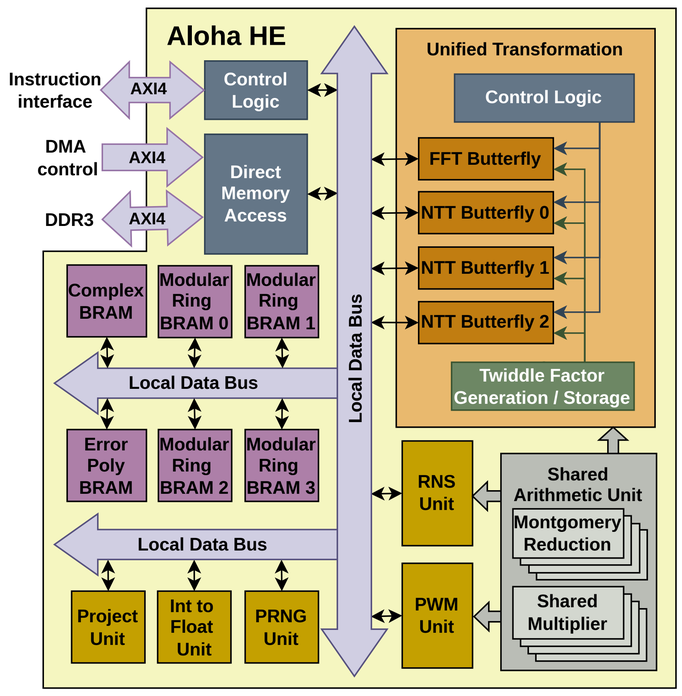


Aloha-HE's Hardware Design

Contributions of Aloha-HE

- First end-to-end hardware accelerator for client-side CKKS
  - Supports encoding/decoding and
  - Encryption/decryption
- Implements an IEEE-754 compliant floating-point unit to perform the FFT
- **Exploits similarities between FFT and NTT by sharing hardware components** between these operations
- Proposes a novel hardware-friendly approach to compute the RNS

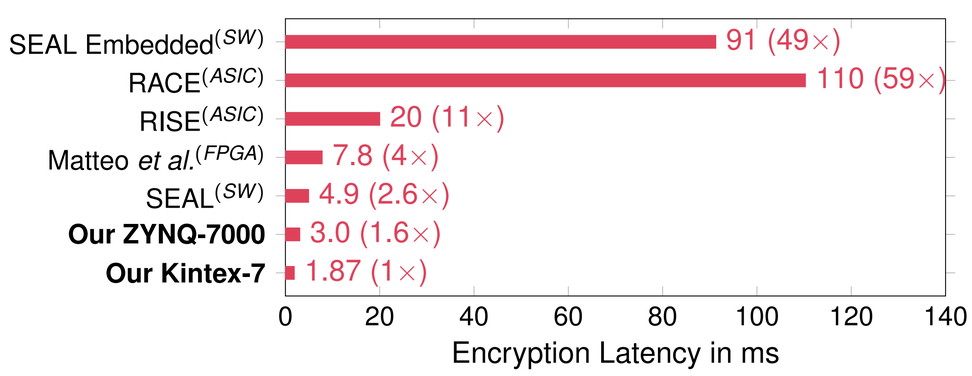




Results & Comparison

Latency Comparison

The chart below compares the latency of a full CKKS encode+encrypt procedure. RACE [2] and RISE [3] are ASICs while Matteo *et. al* [4] presents an FPGA for client-side CKKS. All three works perform just the encryption in hardware while leaving the encoding in software. Aloha-HE significantly increases the performance between 4× and 59× compared to these works. Aloha-HE also outperforms SEAL Embedded [1] / SEAL [5] by 49× / 2.6×.

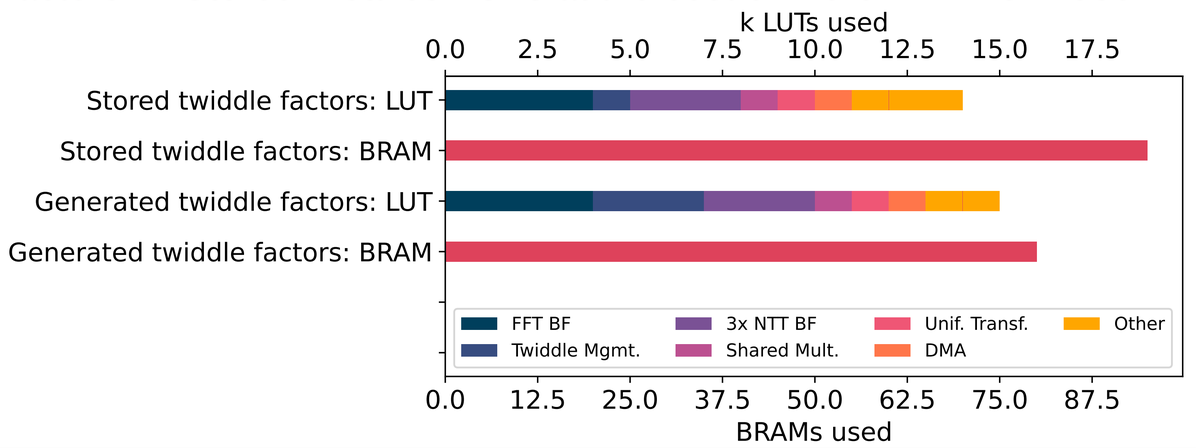


Comparison to Intel Core CPU

	Our accelerator	Intel Core CPU	Improvement
Clock frequency	200 MHz	2.3 GHz	11.5× lower
Encryptions/sec	534 Enc/s	204 Enc/s	2.6×
Energy/encryption	5.8 mJ/Enc	73.5 mJ/Enc	12.7×

Area Consumption

This compares the resource utilization for generated and stored twiddle factors ω. Stored ω saves LUTs at the cost of more BRAMs in use.



References:

[1] D. Natarajan and W. Dai, "Seal-embedded: A homomorphic encryption library for the internet of things," *IACR TCHES*, 2021.
[2] Z. Azad et al., "Race: Risc-v soc for en/decryption acceleration on the edge for homomorphic computation," in *Proceedings of the ACM/IEEE ISLPED*, 2022.
[3] Z. Azad et al., "Rise: Risc-v soc for en/decryption acceleration on the edge for homomorphic encryption," in *IEEE TVLSI*, 2023.
[4] S. D. Matteo, *et al.*, "Vlsi design and fpga implementation of an ntt hardware accelerator for homomorphic seal-embedded library," *IEEE Access*, 2023.
[5] "Microsoft SEAL (release 4.1)," https://github.com/Microsoft/SEAL, 2023, Microsoft Research, Redmond, WA