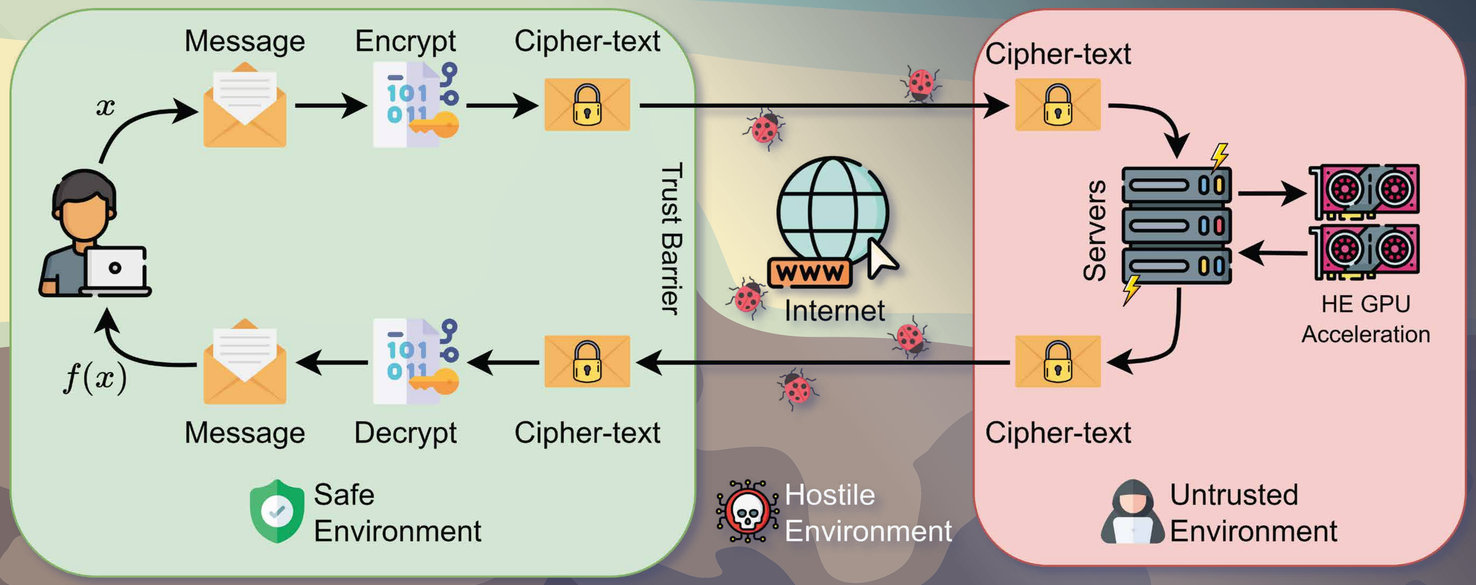
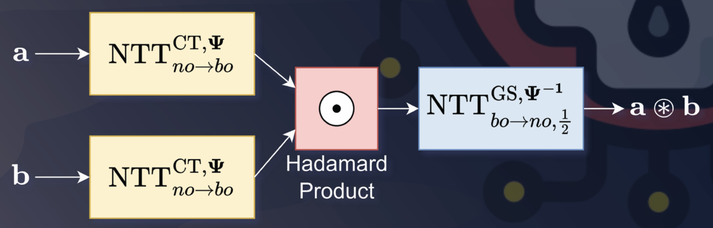
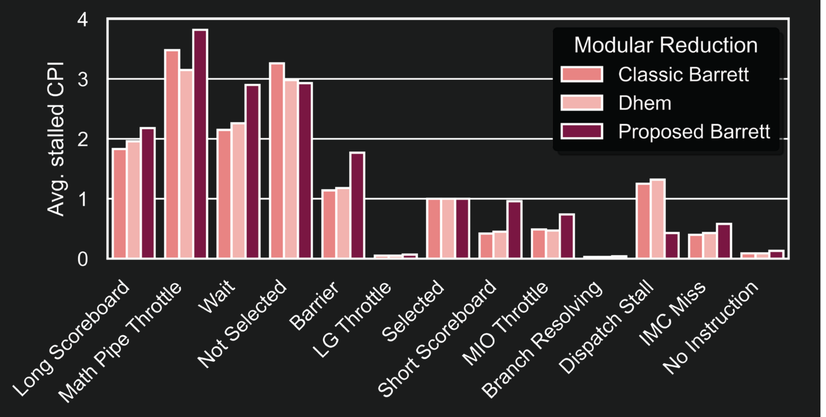
Accelerating FULLY HOMOMORPHIC ENCRYPTION using Custom Accelerators in Cloud Systems





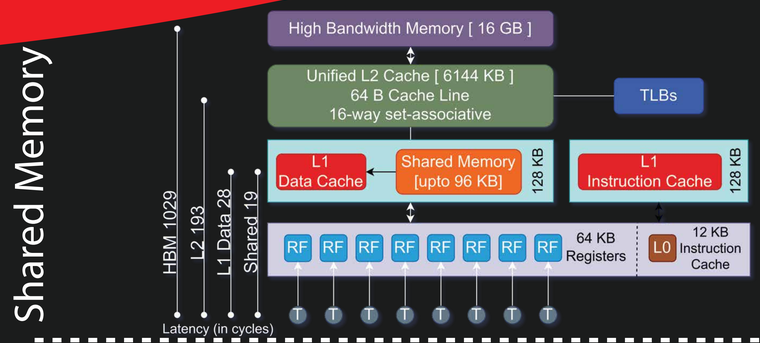
Bottlenecks

- 4-6 orders of magnitude slower
- Skewed memory access patterns
- Wide integer arithmetic
- Native modular reduction

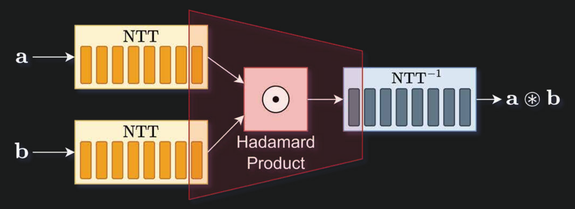


Optimizations

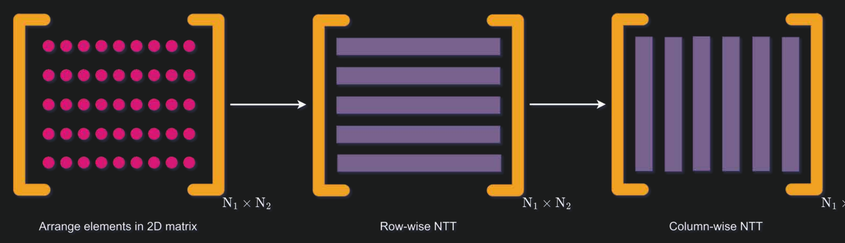
Shared Memory



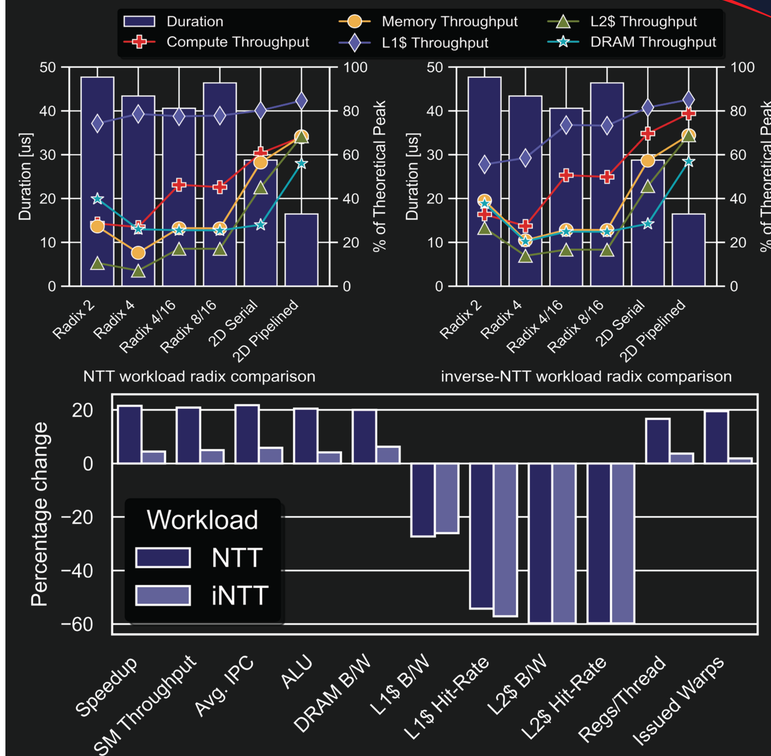
FUSED NTT



2D NTT



Results



Paper:

Kaustubh Shivdikar §
Gilbert Jonatan ¶
Ajay Joshi *
Evelio Mora †
Jose L Abellan †
Neal Livesay §
John Kim ¶
Rashmi Agrawal *
David Kaeli §

§ Northeastern University
* BOSTON UNIVERSITY
¶ KAIST
† UCAM Universidad Católica de Murcia