HEAX: High-Performance Hardware Architecture for Microsoft SEAL

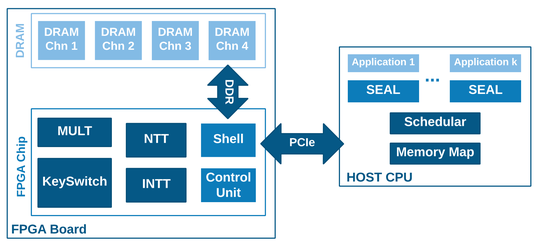
Sadegh Riazi, Kim Laine, Blake Pelton, Wei Dai

Microsoft Research

Abstract

HEAX is a high-performance hardware architecture for accelerating computation on Homomorphically encrypted data in the cloud. Each component within HEAX is fully pipelined, providing high-throughput computations on ciphertexts. Proof-of-concept implementation on FPGA demonstrates more than two orders of magnitude performance improvement that fully saturates the PCIe bus used to transfer data between CPU and FPGA board. Thus, HEAX achieves an optimal hardware acceleration for computing on Homomorphically encrypted data compared to other hardware-based acceleration solutions including any type of FPGAs or GPUs as they should be connected using PCIe bus. From system-view perspective, the bottleneck is the bandwidth of PCIe that is used to transfer data from host CPU to FPGA and vice versa.

High-level System View



FPGA Resource Utilization

Core Name	DSP	Registers	ALM	Delay
Dyadic	22	4526	1663	23
NTT	10	6297	2066	50
INTT	10	5449	2119	49

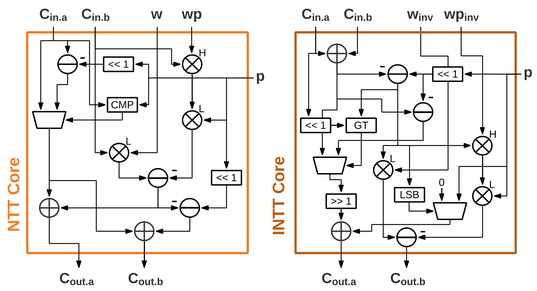
Module	#Cores	DSP #umul27	Registers	ALM	BRAM #bits	BRAM #M20K	Cycles
A10 Shell	-	1	79203	39222	886496	144	-
S10 Shell	-	2	86984	45612	1201096	173	-
MULT	4	88	42817	15795	1104384	65	1024
	8	176	61878	22160		65	512
	16	352	93594	35257		164	128
	32	704	181503	62157		293	64
NTT	4	40	61670	22316	1514496	86	6144
	8	80	96919	36336		185	3072
	16	160	196205	67865		380	1536
	32	320	387357	142300		725	768
INTT	4	40	63917	22700	1514496	86	6144
	8	80	104575	37331		185	3072
	16	160	182478	68645		380	1536
	32	320	384267	144957		724	768

FPGA Device	HE Param. Set	DSP (%)	Registers (%)	ALM (%)	BRAM bits (%)	BRAM #M20K (%)	Freq. (MHz)
Arria10	Set-A	1185 (78)	723188 (42)	246323 (58)	26596320 (48)	1731 (64)	275
Stratix10	Set-A	2018 (35)	1554005 (42)	582148 (62)	26907592 (11)	3986 (34)	300
	Set-B	2610 (45)	1976162 (53)	698884 (75)	201332624 (84)	10340 (88)	300
	Set-C	2370 (41)	1746384 (47)	599715 (64)	182847524 (76)	9329 (80)	300

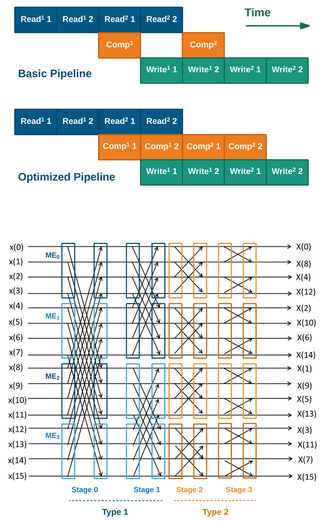
Performance Results

FPGA Device	HE Param. Set	NTT			INTT			Dyadic MULT			KeySwitch			MULT+ReLin		
		SEAL	HEAX	Speed-up	SEAL	HEAX	Speed-up	SEAL	HEAX	Speed-up	SEAL	HEAX	Speed-up	SEAL	HEAX	Speed-up
Arria10	Set-A	7222	89518	12.4	7568	89518	11.8	36931	1074219	29.1	488	44759	91.7	420	44759	106.6
	Set-A	7222	195313	27.0	7568	195313	25.8	36931	1171875	31.7	487	97656	200.5	420	97656	232.5
Stratix10	Set-B	3437	90144	26.2	3339	90144	25.5	18362	585938	31.9	97	22536	232.3	84	22536	268.3
	Set-C	1631	41853	25.7	1659	41853	25.2	9117	292969	32.1	16	2616	163.5	15	2616	174.4

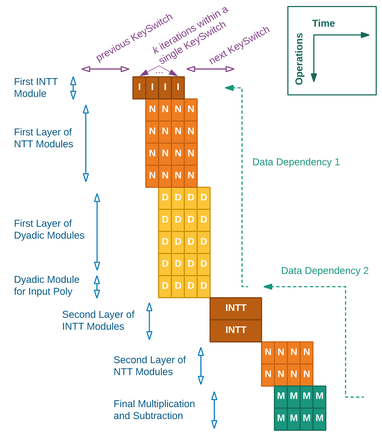
NTT/INTT Cores



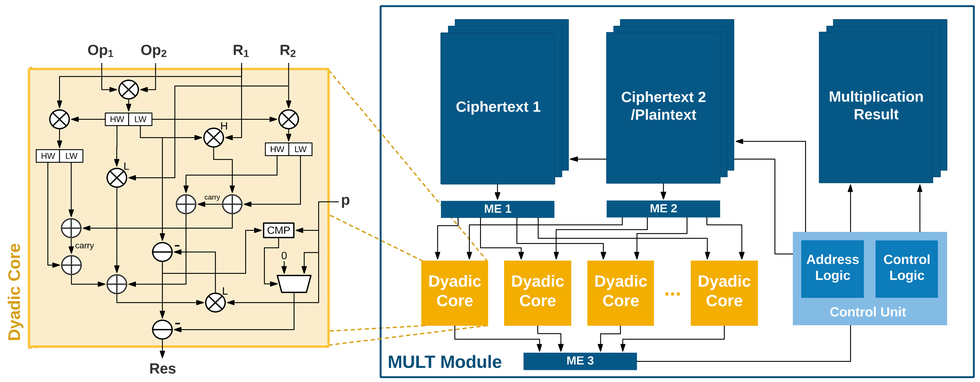
NTT Module Pipeline



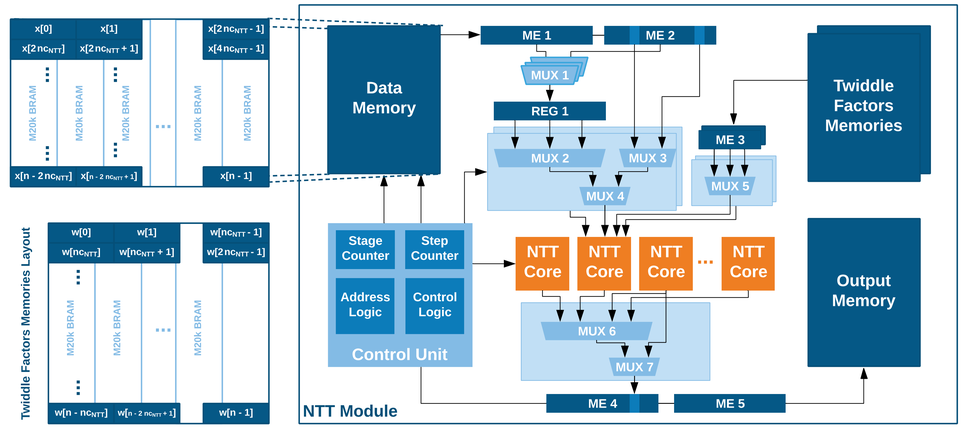
KeySwitch Module Pipeline



Multiplication Module Architecture



NTT Module Architecture



KeySwitch Module Architecture