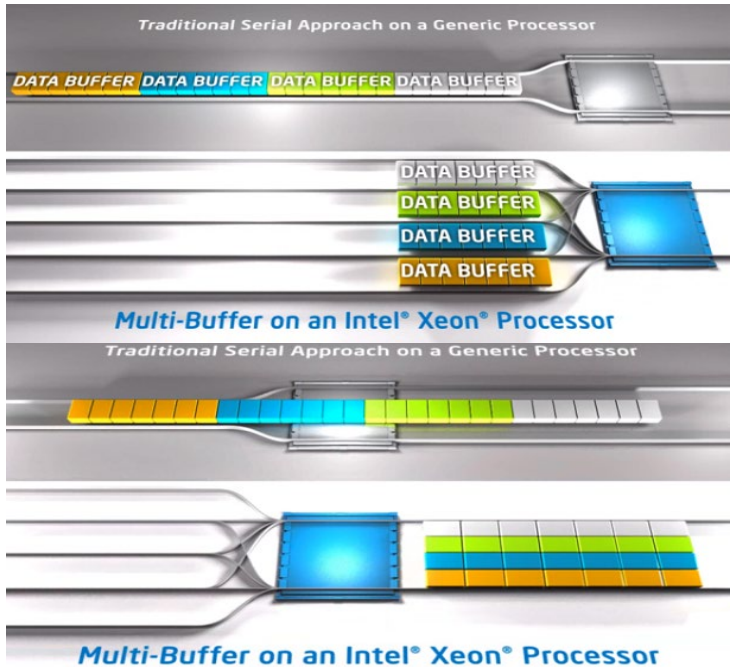
New SIMD ISA Utilizing AVX512 on ICX

- Vector CLMUL
- Vector AES
- VPMADD52
- SHA Extensions
- GFNI

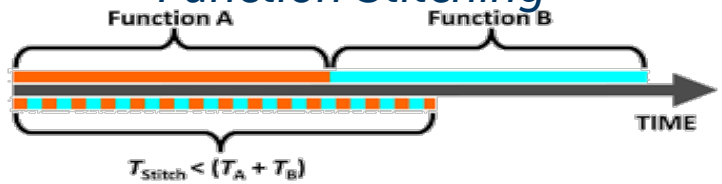
+

Software / Algorithms

Multi-Buffer



Function Stitching



Ice Lake vs. Cascade Lake Per Core Performance

ECDHE x25519	8X
RSA Sign 2048	7.5X
ECDHE p256	6X
AES-CTR	3.5X
AES-CMAC	3.5X
AES-XTS	3.5X
AES-GCM	3X
ECDSA Sign p256	3.5X
CRC	2X
ZUC	1.5X

Algorithms, HW and SW co-innovation results in unprecedented performance advances in cryptography

Per core results have been estimated based on pre-production tests at iso frequency as of August 2020. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

intel