Energy-Efficient AES Ciphers on a Fine-Grained Many-Core System

Bin Liu and Bevan M. Baas

University of California, Davis

binliu@ucdavis.edu

Theme/Task: 1971.001

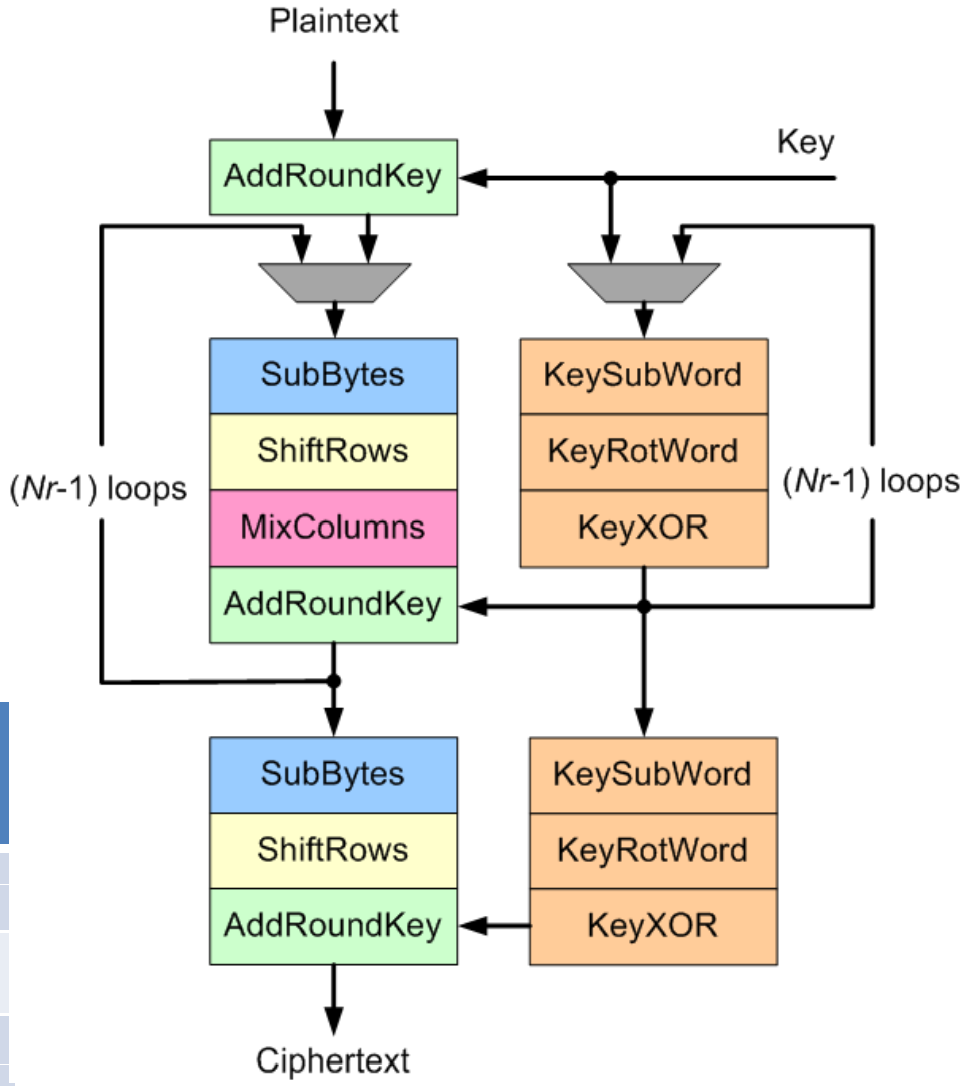
Outline

- Advanced Encryption Standard
- Targeted Fine-Grained Many-Core Platform
- Proposed AES Implementations
- Power Optimization Based on VFS
- Comparison with Related Work

Advanced Encryption Standard

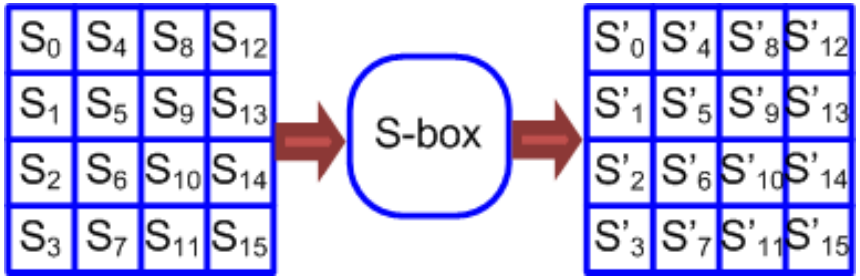
- Plaintext: 128 bits, a 4-by-4 byte array
- Four basic operations in the main loop
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey

Length of *Round Key* (bits)	Number of Rounds (N_r)
128	**10**
192	**12**
256	**14**

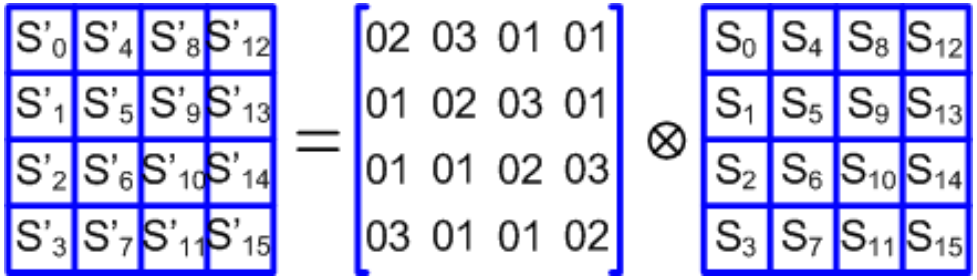


AES Basic Operations

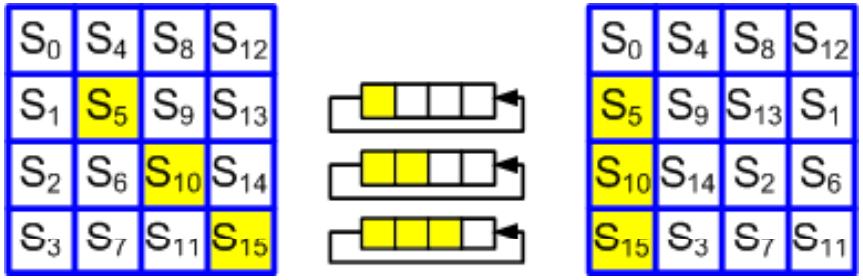
SubBytes: byte substitution from a look up table



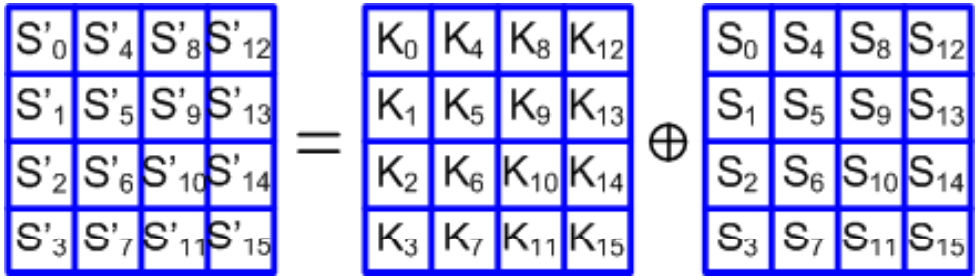
MixColumns: each column multiplies a fixed polynominal over GF(2^8)



ShiftRows: cyclically shift by one, two and three bytes in the 2nd, 3rd and 4th row



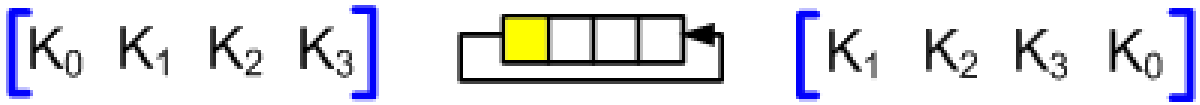
AddRoundKey: round key is added to input using a bitwise XOR



AES Key Expansion

- **KeySubWord**: byte substitution from a look up table for a four-byte word

- **KeyRotWord**: left cyclic shift one byte

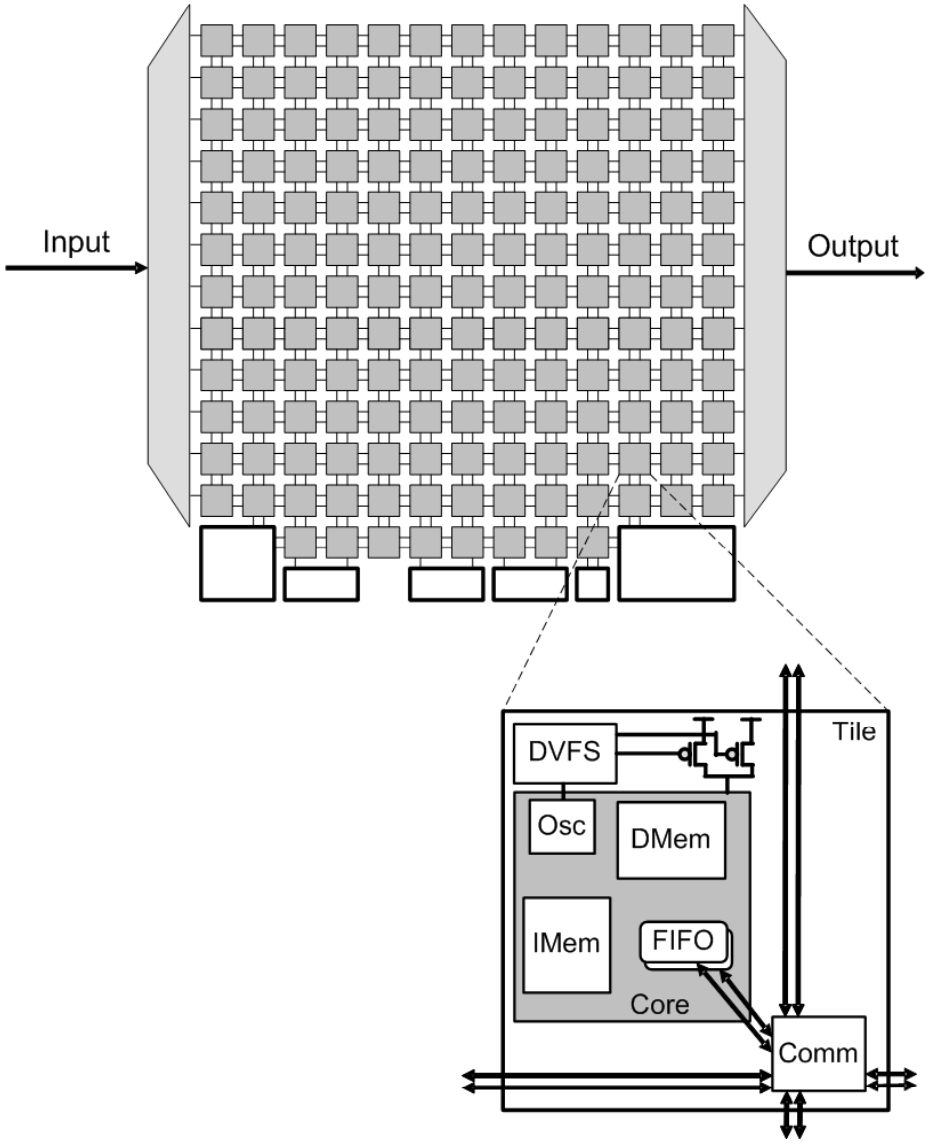


- **KeyXOR**: $W[i] = W[i-1] \oplus W[i-N_K]$

  where N_K equals 4, 6 or 8 for the key length of 128, 192 or 256 bits

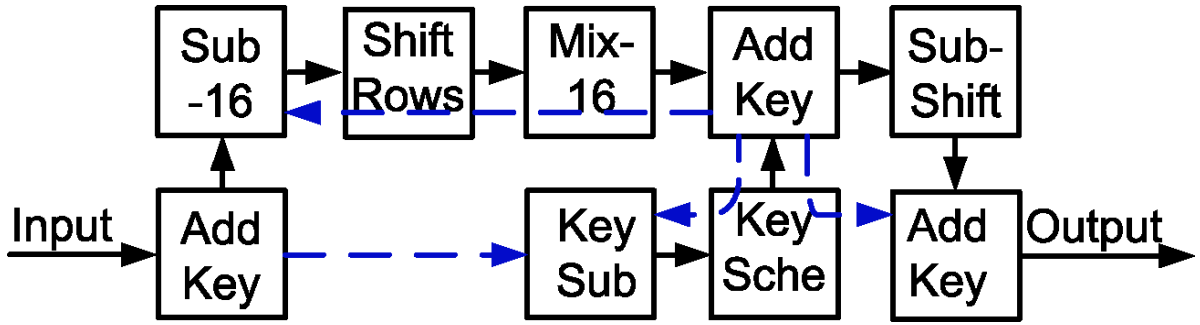
Targeted Fine-Grained Many-Core Platform

- 164 homogeneous fine-grained cores
  - no specialized instructions
  - 128 x 32-bit instruction memory
  - Max. frequency 1.2GHz @ 1.3V
  - 0.17 mm^2 in 65nm CMOS
- On-chip reconfigurable 2D-mesh network
  - Nearby & long-distance comm.
- Per-processor dynamic volt. and freq. scaling (DVFS)
  - Programmable OSC for each core
  - Each core can tie one of the two power supply voltages

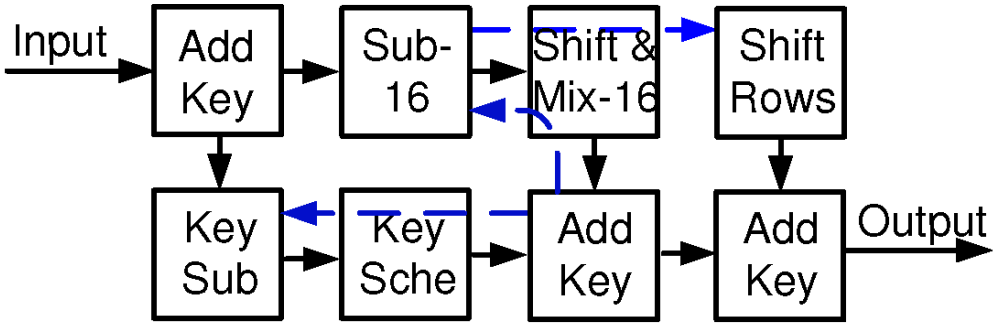


Proposed AES Implementations (1)

- One-Task One-Processor (# of cores = 9)
  - Map each task in the algorithm to one processor

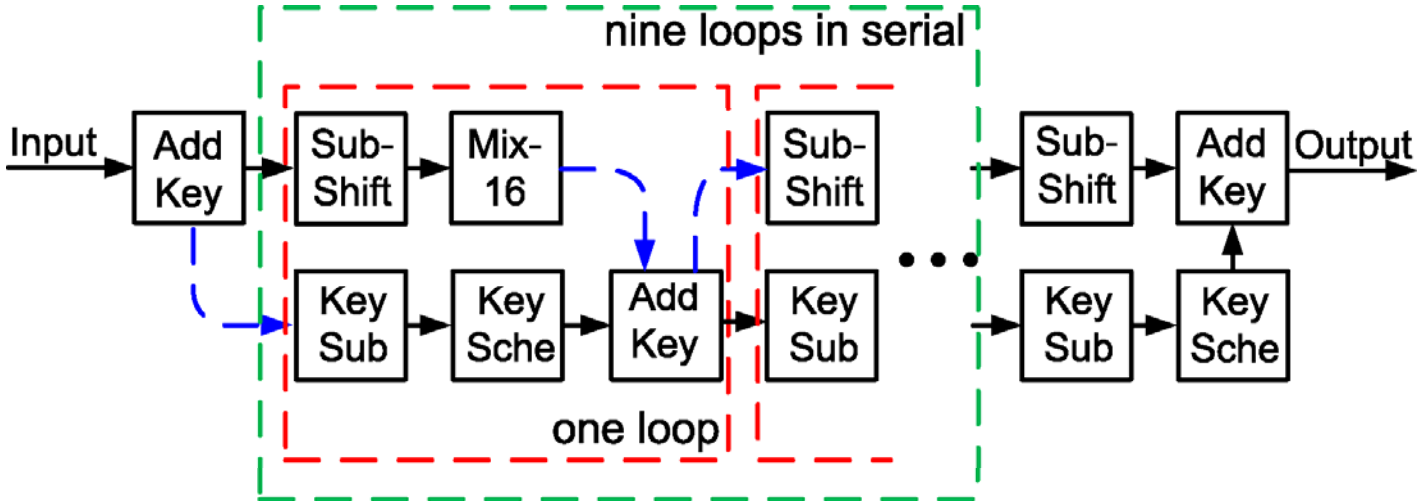


- Small (# of cores = 8)
  - Uses the smallest number of cores

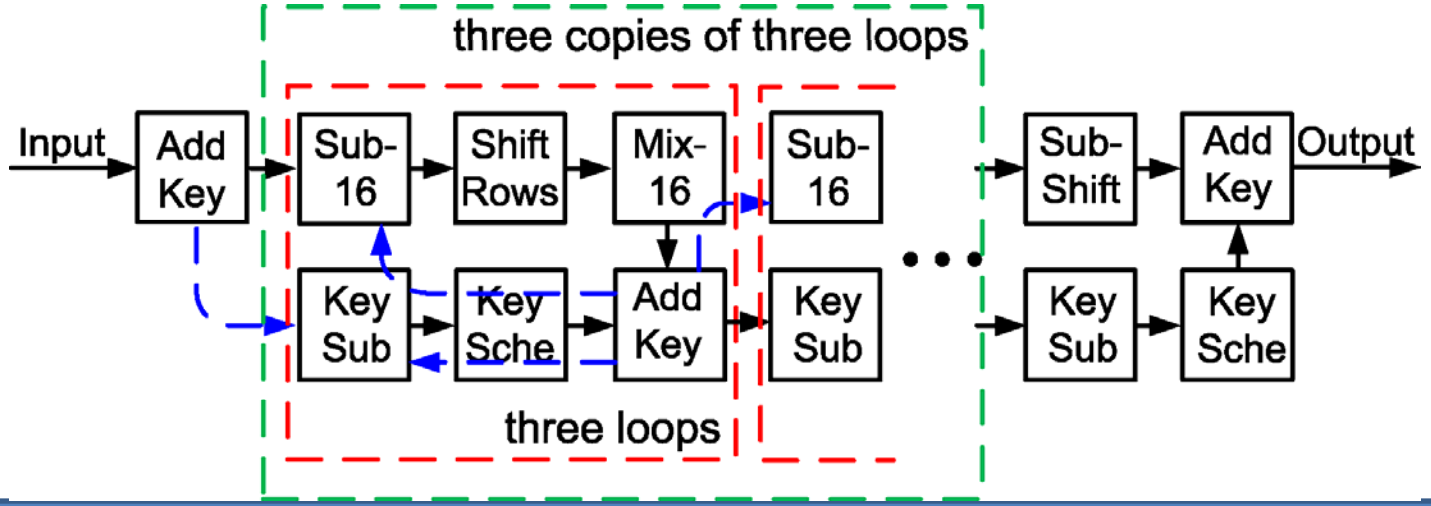


Proposed AES Implementations (2)

- Loop-unrolled Nine Times (# of cores = 50)

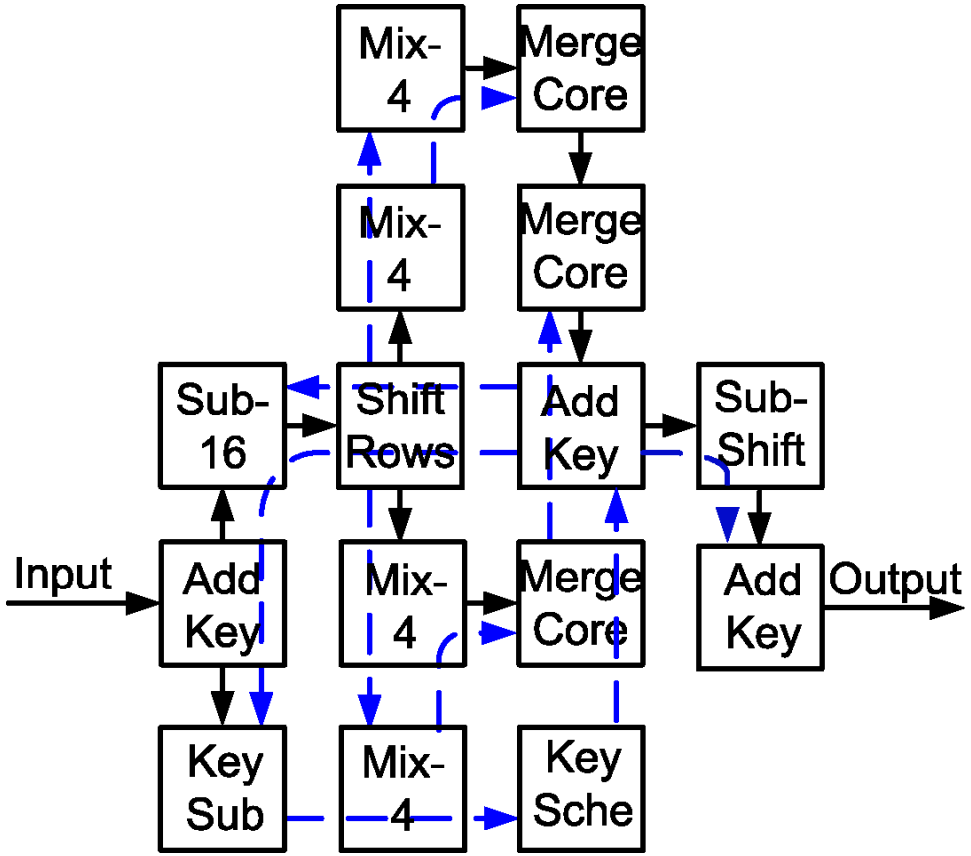


- Loop-unrolled Three Times (# of cores = 23)



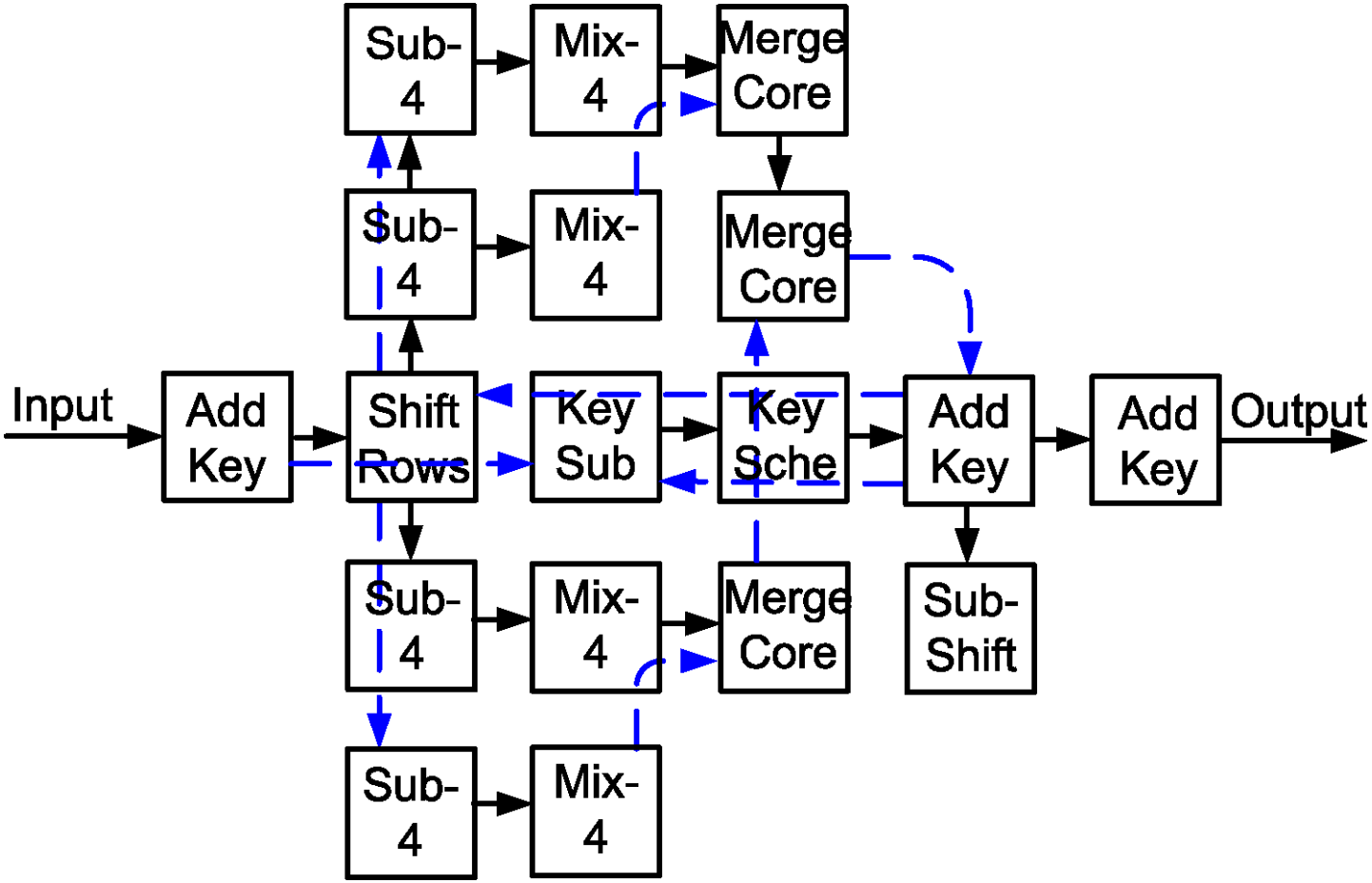
Proposed AES Implementations (3)

- Parallel-MixColumns (# of cores = 15)
  - Each ***MixColumns-4*** computes one column of the data block
  - ***MergeCores*** are added for routing purpose only



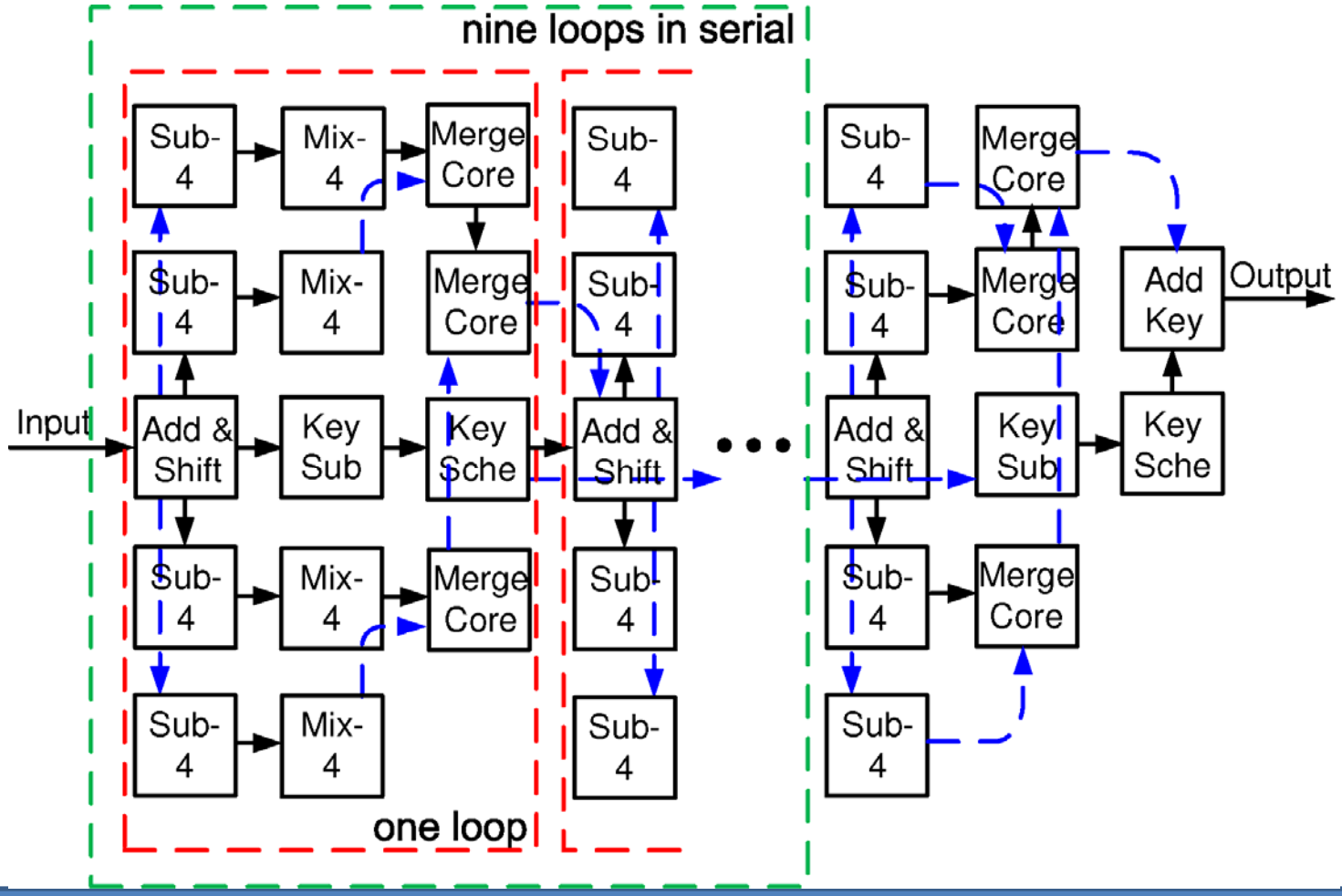
Proposed AES Implementations (4)

- Parallel-SubBytes-MixColumns (# of cores = 18)



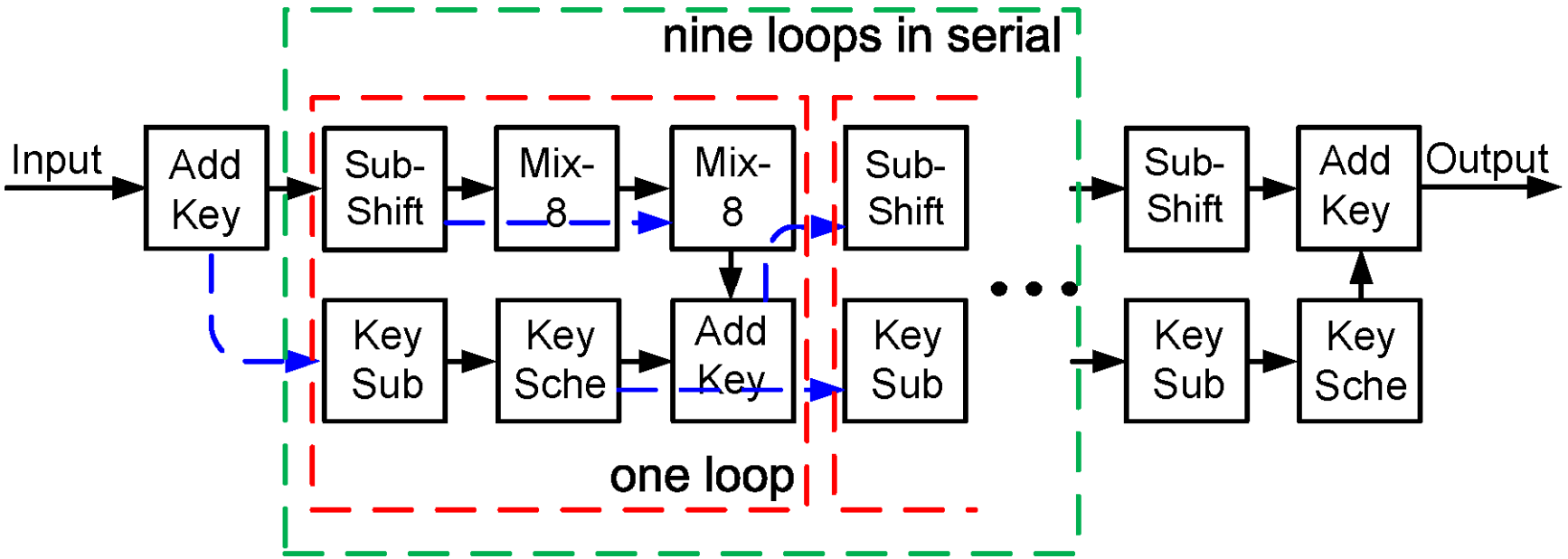
Proposed AES Implementations (5)

- Full-parallelism (# of Cores = 137)
  - Apply loop unrolling on Parallel-SubBytes-MixColumns



Proposed AES Implementations (6)

- No-merge-parallelism (# of Cores = 59)
  - Exploits as much parallelism as possible without introducing any communication-dedicated cores



Proposed AES Implementations (7)

Imp.	1/Thruput. (cycles/byte)	Online Key Expansion		Offline Key Exapnsion	
		Core #	Normalized Thrupt. / Core	Core #	Normalized Thrupt. / Core
Small	167.375	8	1.53	6	2.04
OTOP	223.875	9	1.01	7	1.30
P-Mix	136.250	15	1	12	1.25
P-Sub-Mix	84.375	18	1.35	15	1.61
L-Three	68.625	23	1.29	15	1.99
L-Nine	16.625	50	2.46	30	4.10
No-merge	9.500	59	3.65	39	5.52
Full	4.375	137	3.41	107	4.37

- Full-parallelism could achieve a throughput of 2.21Gbps, when processor runs at 1.2 GHz.
- AES engines with offline key expansion save 29% cores compared with online ones.

Power Optimization (1)

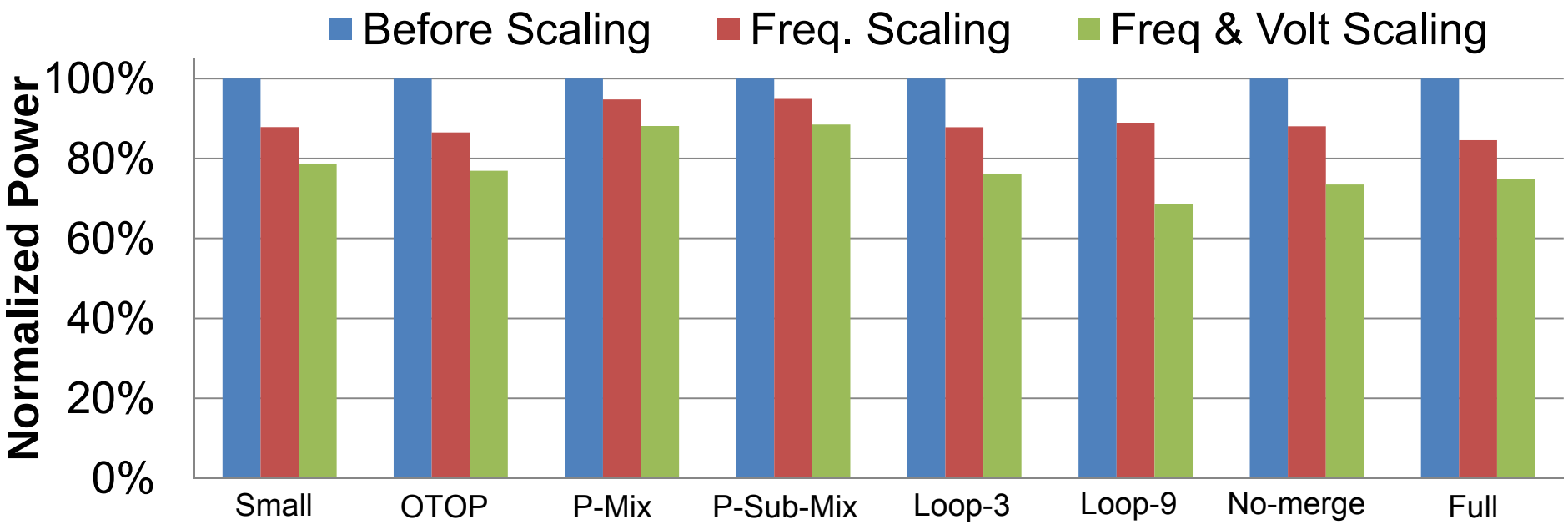
- Frequency Scaling
  - The frequencies of critical processors are determined by throughput requirement
  - Non-critical processors run at

$$f_{opt,i} = \frac{N_{Exe,i}}{N_{Exe,critial}} \times f_{critical}$$

- Dual Supply Voltage Scaling
  - Choose optimal Vdd_{Low} to achieve the highest energy efficiency

$$Vdd_{opt,i} = \begin{cases} Vdd_{High} & \text{if } f_{opt,i} > f_{max}(Vdd_{Low}) \\ Vdd_{Low} & \text{otherwise} \end{cases}$$

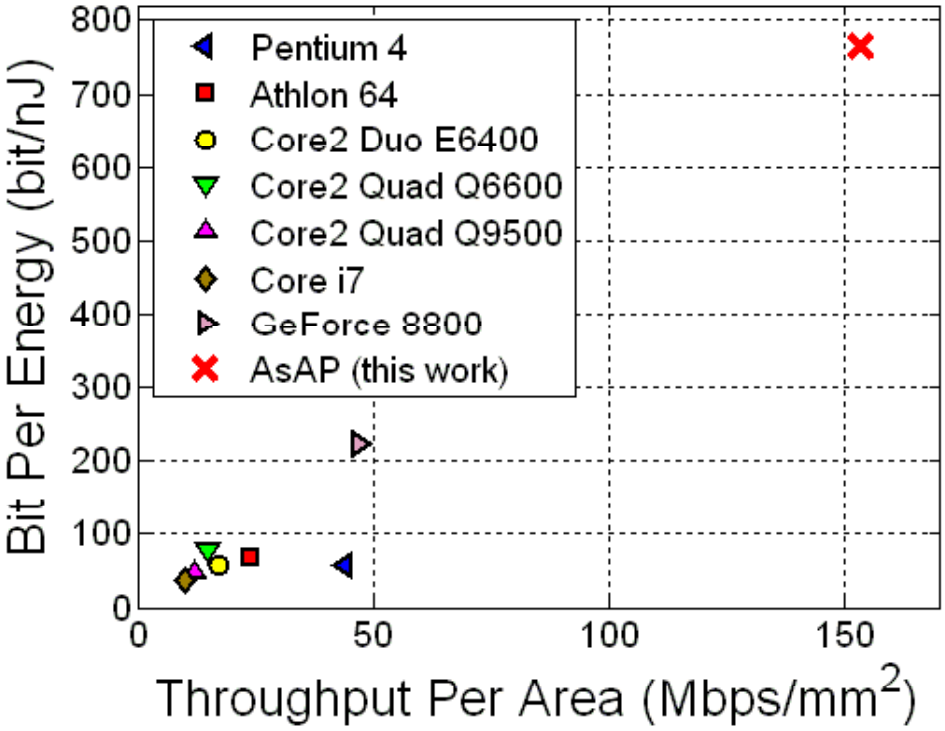
Power Optimization (2)



- Freq. scaling could reduce the power consumption as much as 16%, with an average 11% power saving.
- Freq. & voltage scaling could reduce the power up to 32% with an average of 22% power saving.

Comparison with Related Work

- Compared with general purp. proc.
  - AsAP has 3.5-15.6x higher thruput/area
  - AsAP has 9.8-21.7x higher energy efficiency
- Compared with TI C6201 DSP
  - AsAP has 2.0x higher thruput
- Compared with GeForce 8800 GTX
  - AsAP has 3.3x higher thruput/area
  - AsAP has 3.4x higher energy efficiency



Summary

- 16 AES cipher implementations have been proposed for both online and offline key expansion
- The smallest design requires only 6 fine-grained cores
- The fastest design achieves a throughput of 2.2Gbps when processors run at 1.2 GHZ
- The proposed AES cipher could achieve 3.3-15.6x higher performance per area, and 3.4-21.7x higher energy efficiency than other software platforms

Tech Transfer

- Publications and reports
  - “Parallel AES Encryption Engines for Many-Core Processor Arrays”, to appear in the *IEEE Trans. Computers.*
  - “A High-Performance Area-Efficient AES Cipher on a Many-Core Platform”, *ACSSC*, 2011. (Nominated for Best Student Paper)
  - “Computing Enterprise Workloads with Many-Core Arrays and Special-Purpose Processors”, 2011.
  - “Preliminary Results of Study on Specialized Configurable Accelerators”, 2010.

Acknowledgements

- SRC GRC Grant 1598, 1971 and CSR Grant 1659
- NSF Grant 0430090, 0903549 and CAREER Award 0546907
- ST Microelectronics
- Intel
- UC Micro
- C2S2
- SEM
- Intellasys