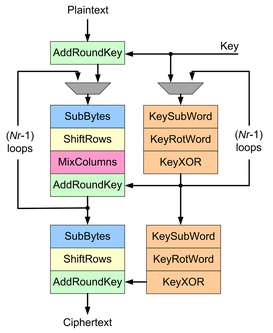
Energy-Efficient AES Ciphers on a Fine-Grained Many-Core System

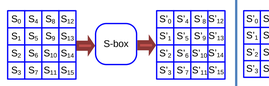
Bin Liu and Bevan M. Baas

Department of Electrical and Computer Engineering, University of California, Davis, CA 95616

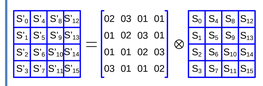
1. Advanced Encryption Standard



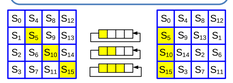
SubBytes: byte substitution from a look up table



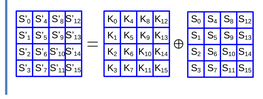
MixColumns: each column multiplies a fixed polynominal over GF(2^8)



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

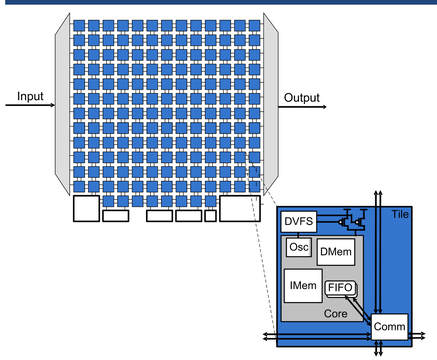


Length of *Round Key* (bits)	Number of Rounds (N_r)
128	10
192	12
256	14

- **KeySubWord** $[K_0\ K_1\ K_2\ K_3]$ → S-box → $[K'_0\ K'_1\ K'_2\ K'_3]$
- **KeyRotWord** $[K_0\ K_1\ K_2\ K_3]$ → $[K_1\ K_2\ K_3\ K_0]$
- **KeyXOR**: $W[i] = W[i-1] \oplus W[i-N_K]$

  Nk equals 4, 6 and 8 for the key length of 128, 192 and 256 bits

2. Targeted Fine-Grained Many-Core Platform

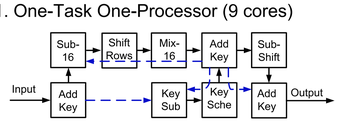


AsAP2 Single Tile (164 total)	
Area	**0.17 mm²**
Transistors	**325,000**
CMOS Tech.	**65 nm low-leakage**
Max. frequency	**1.2GHz @ 1.3 V**
Instru. Memory	**128 x 32-bit**
Data Memory	**128 x 16-bit**

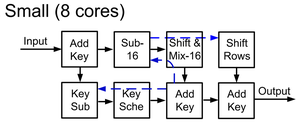
- In-order single-issue 6-stage pipeline
- No-specialized instructions
- Reconfigurable 2D-mesh network
- Per-core dynamic voltage and frequency scaling

3. Proposed AES Implementations (1)

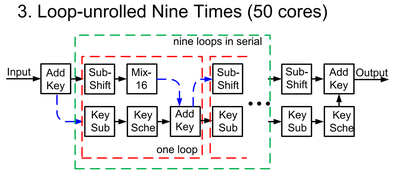
1. One-Task One-Processor (9 cores)



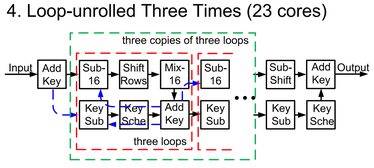
2. Small (8 cores)



3. Loop-unrolled Nine Times (50 cores)

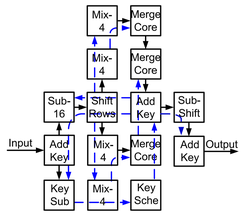


4. Loop-unrolled Three Times (23 cores)

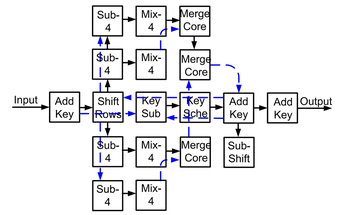


4. Proposed AES Implementations (2)

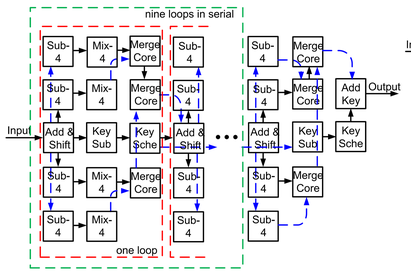
5. Parallel-MixColumns (15 cores)



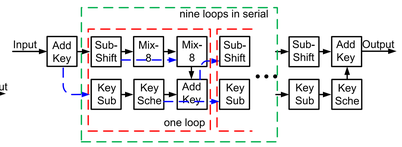
6. Parallel-SubBytes-MixColumns (18 cores)



7. Full-parallelism (137 cores)



8. No-merge-parallelism (59 cores)



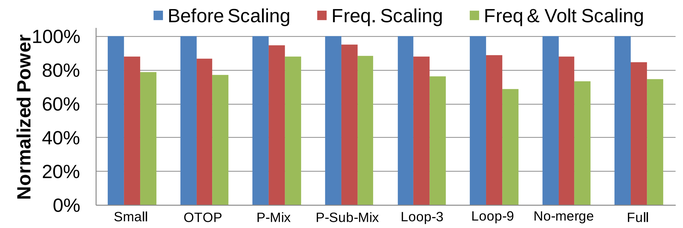
- Explore as much parallelism as possible without introducing any communication-dedicated cores

5. Summary of Proposed AES Ciphers

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**

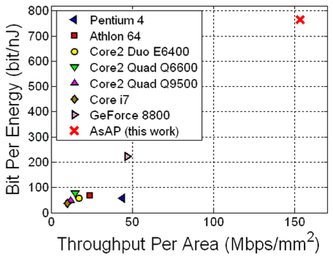
- Maximum throughput of Full-parallelism implementation is 2.2 Gbps when processor runs at 1.2GHz.
- AES ciphers with offline key expansion save 29% cores compared with online ones.

6. Power Optimization



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

7. Comparison with Related Work



- Compared with general purpose processors
  - AsAP has 3.5-15.6x higher throughput per area
  - AsAP has 9.8-21.7x higher energy efficiency
- Compared with TI C6201 DSP
  - AsAP has 2.0x higher throughput
- Compared with GeForce 8800 GTX
  - AsAP has 3.3x higher throughput per area
  - AsAP has 3.4x higher energy efficiency

8. Short Bio and Technology Transfer

Bin Liu received the B.S. degree in information engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007, and the M.S. degree in electrical and computer engineering from the University of California, Davis, in 2010, where he is currently pursuing the Ph.D. degree.

His research interests include high-performance many-core processor architecture, dynamic voltage and frequency scaling algorithm and circuits, and parallel encryption engines.

He received the Best Paper nomination at Asilomar 2011.

- "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.

Acknowledgments: The authors gratefully acknowledge support from NSF Grant 0430090, 0903549 and CAREER Award 0546907, SRC GRC Grant 1598 and 1791, CSR Grant 1659, UC Micro, ST Microelectronics, Intel, and Intellasys. The authors also acknowledge the support of the C2S2 Focus Center, one of the six research centers funded under the Focus Center Research Program (FCRP), a Semiconductor Research Corporation entity.