

Session 14
**An Embedded Cryptographic Processor for
the Rijndael AES Algorithm**

Henry Kuo (henrykuo@ee.ucla.edu)
Ingrid Verbauwhede (ingrid@ee.ucla.edu)

Department of Electrical Engineering
University of California Los Angeles

9/26/2000 1
Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

Introduction

- Data encryption in wireless communication, PDA's, Internet is very important
- Co-processors with high encryption power, small area, and low power consumption

9/26/2000 2
Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

AES (Advanced Encryption Standard)

- NIST introduced DES (Data Encryption Standard) in 1977
- AES by NIST is due in Fall 2000
- Finalists: Mars, RC6, Rijndael, Serpent, Twofish

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

3

AES Candidate: Rijndael

- One of the fastest and strongest algorithms
- Variable block length: 128, 192, 256 bits
- Variable key length: 128, 192, 256 bits
- Variable number of rounds (iterations): 10, 12, 14
- Number of rounds depend on key/block length

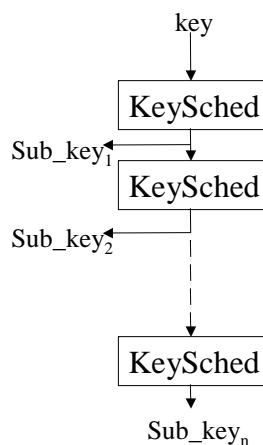
9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

4

Key Scheduling

- Each encryption round needs specific sub-key
- Generation of sub-key is a separate process
- Each sub-key depends on previous sub-key
- Key scheduling can be done in advanced or on the fly



9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

7

Transition to Hardware

- Originally in C and Java for 8-bits (Intel 8051) and 32-bits (Intel P200) processors
- Mobile phone or smart card need low power solution
- Implement Rijndael algorithm on ASIC
- Goal: optimize for throughput and power consumption

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

8

Memory Access Problem

- Goal: 1 clock cycle per algorithm round
- In 1 round, large amount of memory read

Tables	Log[256]	Alog[256]	S[256]	rcon[30]	shift[24]
Reads	128	64	36	1	32

- Worst case: 261 memory reads per round
- Parallelism problem in hardware

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

9

Memory Access Problem (Cont'd)

- Only one memory, 261 cycles
- 5 memories, one of each kind, 128 cycles
- If we want 1 clock cycle per algorithm round, at least 261 memories (58KB in size)

# memory modules	Min. # clock cycles
1	261
5	128
66	4
131	2
261	1

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

10

Memory Access Problem (Cont'd)

Log[256]		Alog[256]		S[256]		rcon[30]		shift[24]	
256	HW	256	HW	256	HW	256	HW	256	HW
128	32	64	64	36	40	1	1	32	4

- In MixColumn, same value is read 4 times!
- In ShiftRow, same value is read 8 times!
- In order to use 1 cycle for each encryption, we need 141 memory modules (35KB in size) and 141 read ports, 8 bits each

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

11

Other Modifications

	Software	Hardware
Block/key Length	Dynamic	Internal datapath 256 bits. I/O are variable
Key Scheduling	Pre-done (buffer) / on the fly	On the fly
Division (for addresses)	64 8-bits divisions	None (no need to calculate)

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

12

Hardware Implementation

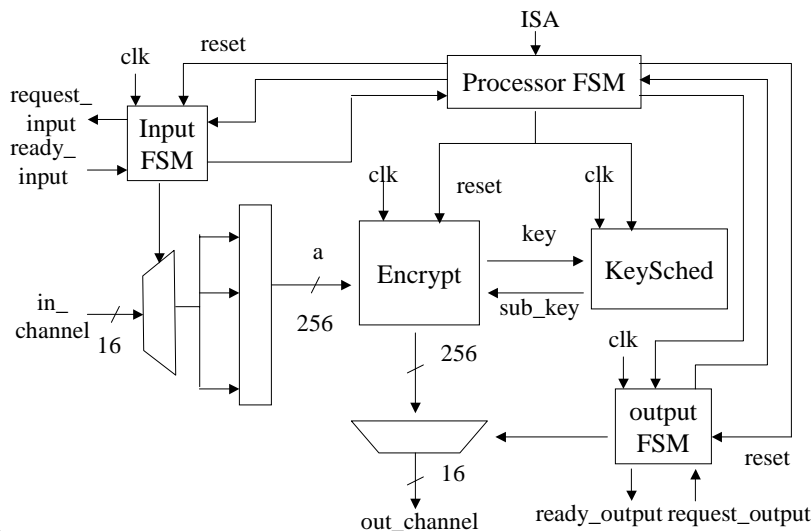
- Minimize memory accesses
- Implementation of I/O FSM
- Implementation of key scheduling so that it is aligned with encryption block

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

13

Block Diagram



9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

14

CAD Tools Used

- Cadence Verilog XL
- Synopsys version 1999.10
- Silicon Ensemble
- Library choice: NSC 0.18 μ m technology

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

15

Area and Speed Estimation

- Iterative flow, 1 cycle / 1 encryption round
- Throughput: 2.15Gbits/sec
- Area: 1.4mm²

	Software (32 bits)	Hardware
clock frequency	200MHz	125MHz
Throughput	19.8Mbits/sec	2.15Gbits/sec
Program size	47KB	35KB

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

16

Future Development

- Fabrication of the design
- Actual throughput and area measurement
- Time for initialization and one encryption
- Energy consumption per encryption
- Resistance to timing and power attack
- Overhead for decryption

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

17

Summary

- Need of AES to replace DES
- Need for high throughput and low power embedded chip for encryption (>2Gbits/sec)
- Implementation of Rijndael on ASIC
- Applicable to future generation mobile phones or smart cards

- Acknowledgement: UC Micro, Panasonic, Atmel

9/26/2000

Annual Research Review 2000
Henry Kuo, Ingrid Verbauwhede

18