High-Speed MARS Hardware

A. Satoh N. Ooba K. Takano
E. D'Avignon

IBM

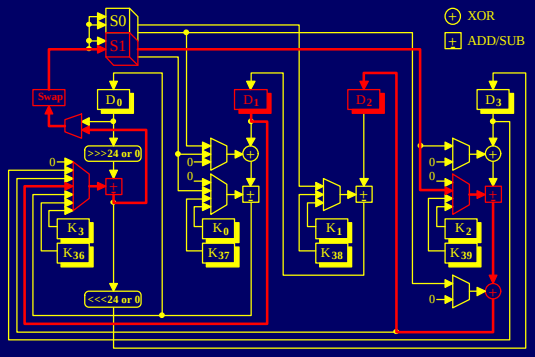
Contents

- MARS Hardware Architecture
- Performance Evaluation
- Conclusions

IBM

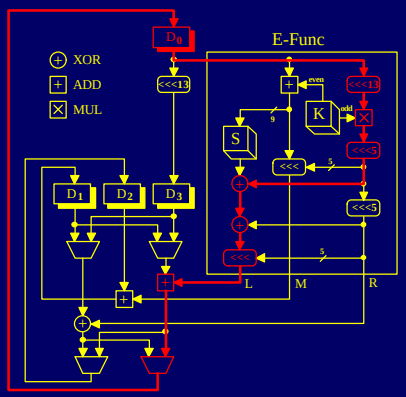
Hardware Architecture

- Forward / backward mixing
  - 3-port (1-write, 2-read) SRAM is used for S-box
  - Critical path contains 2 adders, S-box, XOR, and selectors
  - 9 cycles for each mixing



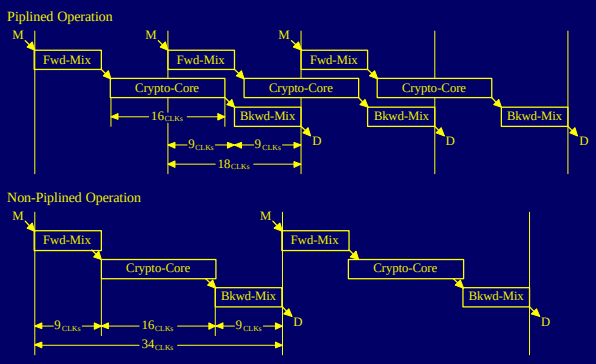
Hardware Architecture

- Cryptographic core
  - S-box is shared by forward/backward mixer
  - S-box read and multiplication are executed simultaneously
  - Critical path contains multiplier, adder, XORs rotator, and selectors
  - 16cycles



Hardware Architecture

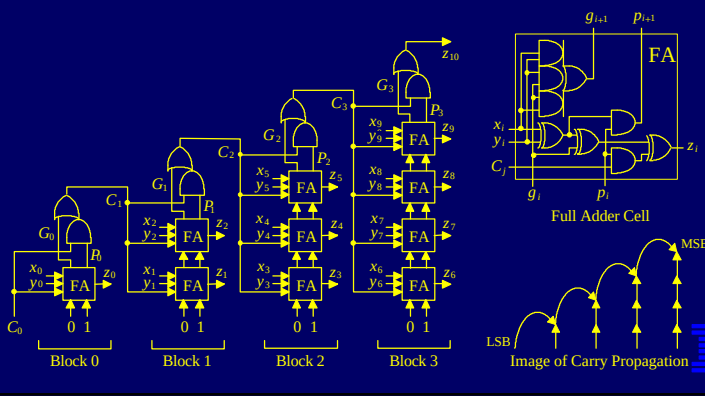
- Pipelined Operation
  - Cryptographic core and forward/backward mixer can operate simultaneously with 4-port SRAM S-box
  - Pipelined operation takes 18 cycles
  - Non-pipelined operations take 34 cycles



IBM

Hardware Architecture

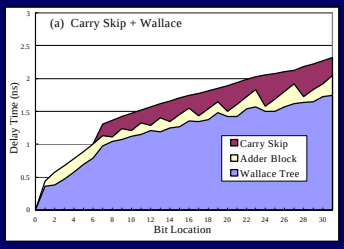
- High Speed Adder
  - Divide into ripple-carry adder blocks
  - Carry skips from block to block
  - Balance carry-propagation and block-internal delays
  - Adder outputs **z** immediately firm when carry reaches

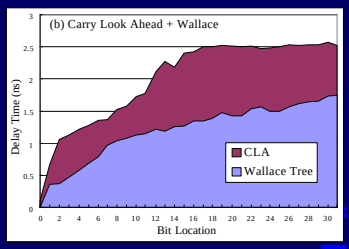


IBM

Performance Evaluation

- Custom MARS multiplier using carry-skip technique
- 0.18-µm CMOS standard cell technology
- High-speed
  - Carry Skip : 2.32ns (nominal) 3.41ns (worst)
  - CLA : 2.57ns (nominal) 3.82ns (worst)
- Compact
  - Carry Skip + Wallace : 3.2Kgates
  - CLA + Wallace : 3.5Kgates

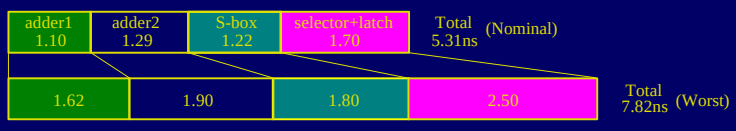




Performance Evaluation

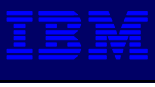
- Cryptographic core has critical delay path
  - 5.57ns (180MHz) in nominal case
  - 8.18ns (122MHz) in worst case

Forward / Backword Mixer



Cryptographic Core

Nominal Case : 1.8V, 25°C, Leff=0.11µm
Worst Case : 1.65V, 125°C, Leff=0.14µm



Performance Evaluation

- Total circuit size is 13.8Kgates+2.25Kbyte memory
- Throughput varies with S-box memory configuration
  - 4-port SRAM : forward/backward mixer (18 cycles) and cryptographic core (16 cycles) run simultaneously
  - 3-port SRAM : 34 cycles = f/b mixer (18) + c-core (16)
  - 1-port SRAM : 50 cycles = f/b mixer (34) + c-core (16)
  - ROM : 50 cycles. Lower operation frequency

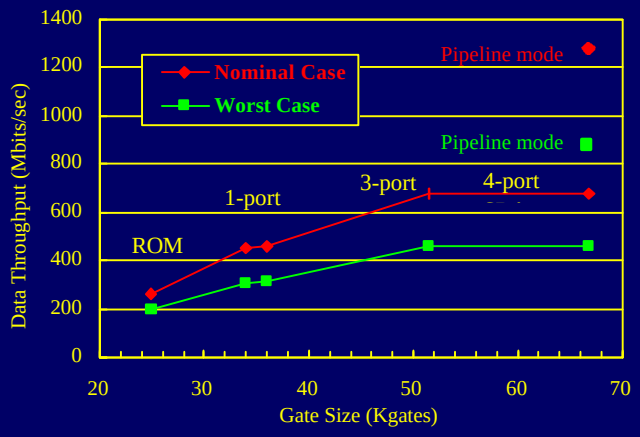
Circuit Block	Gate Size
Key Expansion	2.2K
Enc / Dec Controller	4.5K
Enc / Dec Data Path	6.1K
Interface + Mem Controller	1.0K
Total	13.8K

Function	Type	Gate Size
Key Register (256bytes)	3-port SRAM	6.8K
	2-port SRAM	4.8K
S-box (2Kbytes)	4-port SRAM	46.2K
	3-port SRAM	30.8K
	1-port SRAM	15.4K
	ROM	6.3K

IBM

Performance Evaluation

- 1.28 Gbit/sec for non-feedback cipher modes
- 677 Mbit/sec feedback cipher modes

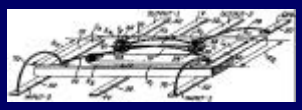


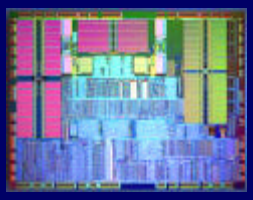
IBM

Conclusions

- 1.28Gbit/s is achieved by introducing high-speed adder and multiplier
- 13.8Kgats + 2.25Kbytes memory
- Future security is primary consideration
  - AES must resist any attacks over 20 years
  - Semiconductor technology is improved rapidly

×4 per 3years





IBM