A Comparative Study of Performance of AES Final Candidates Using FPGAs

A. Dandalis, V. K. Prasanna, and J. D. P. Rolim

University of Southern California
maarcII.usc.edu
(DARPA ACS)

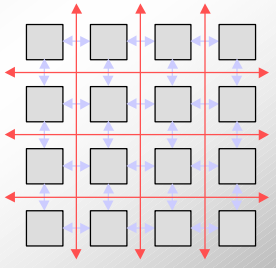
3rd AES Conference, New York, April 2000

Outline

- Why FPGAs?
- Design decisions
- Results

FPGAs Overview

- Configurable hardware
  - programmable logic cells
  - programmable interconnection
  - can be reconfigured
- Performance crux
  - massive parallelism
  - hardware specialization
  - hardware reuse



Why FPGAs ?

	Low		High
Efficiency	µP	FPGA	ASIC
Flexibility	ASIC	FPGA	µP
Power	ASIC	FPGA	µP
Cost	FPGA	µP	ASIC

Design Decisions

MAARC II

- Maximize time performance
- Metrics
  - throughput (bit/sec)
  - latency (key-setup)
- Encryption
  - 128-bit data block and key size

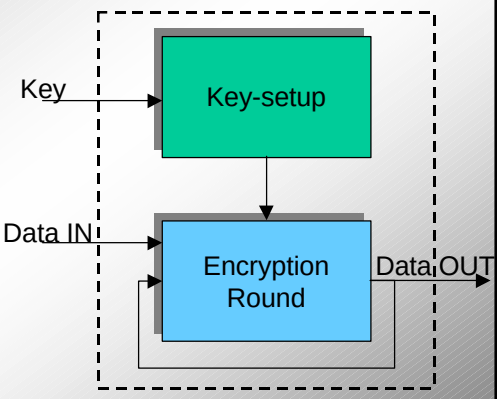
5

“Single-round” Implementations

MAARC II

- Key-setup on-the-fly
  -

  Focus in algorithmic characteristics
  - parallelism at the round level
  -



t_{round}) bit/sec

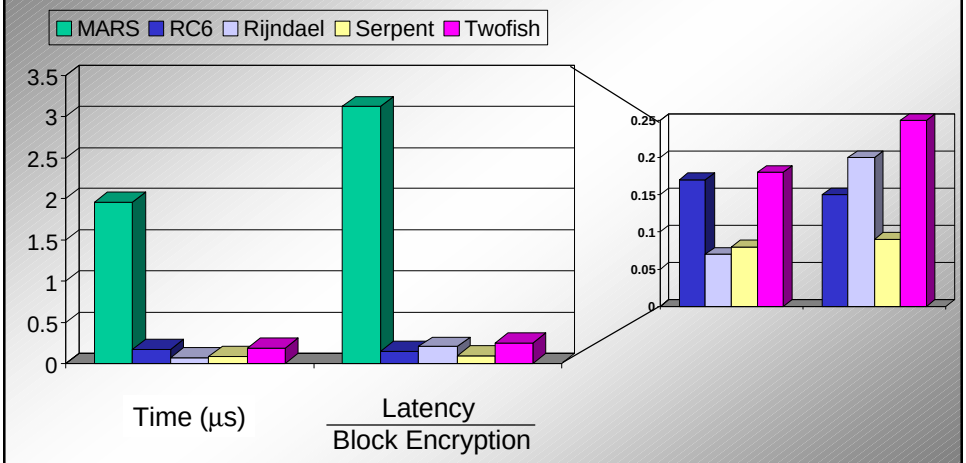
n: # of rounds
t_{round} : encryption time per round

6

Hardware Target

- Xilinx VIRTEX FPGAs
  - speed -6
- Explore on-chip memory blocks
  - key-dependent data
    - sub-keys, S-boxes
- Software tool
  - Xilinx Foundation 2.1i
    - logic synthesis
    - place & route

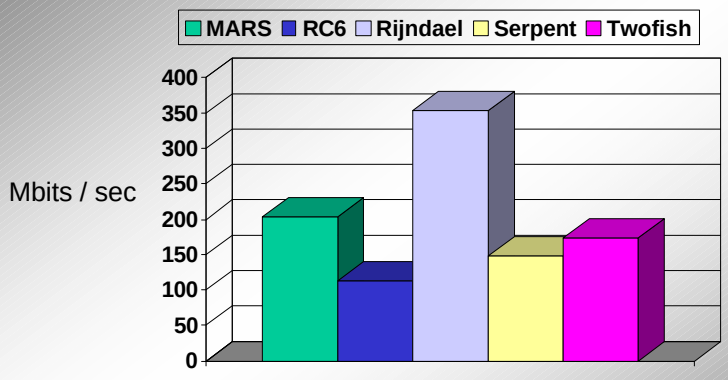
Latency Results



Compared with NIST Efficiency Testing Round 1: 20 - 700x speed-up

Throughput Results

MAARC II

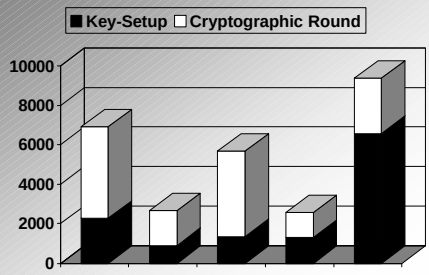


Compared with NIST Efficiency Testing Round 1: 4 - 20x speed-up

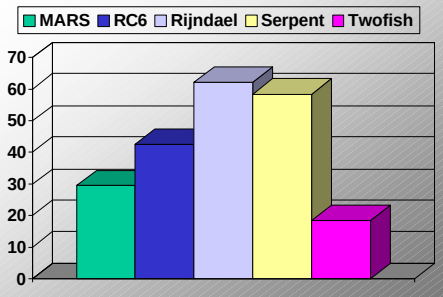
9

Area Results

MAARC II



# of VIRTEX slices

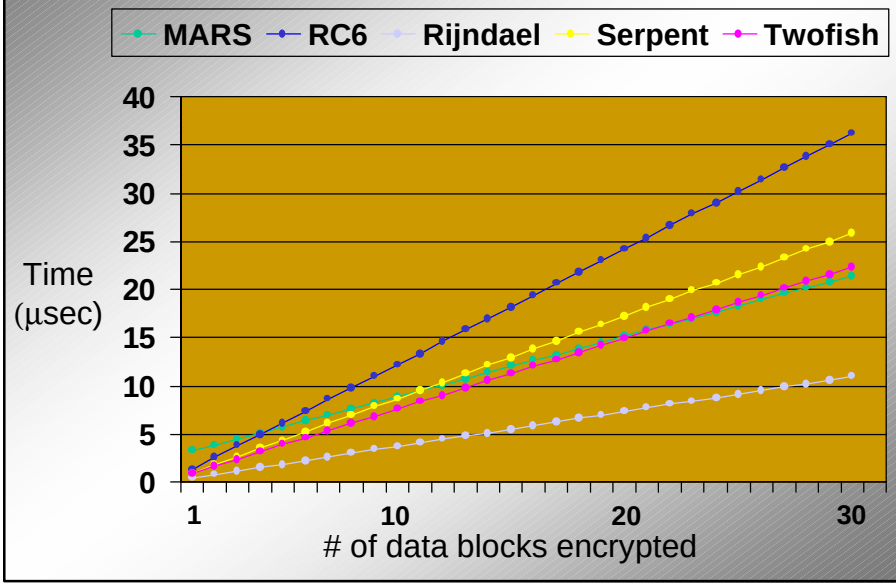


Kbits/(sec*slice)

10

Time Performance Summary

MAARC II



11

Conclusions

MAARC II

- FPGAs
  - hardware-like performance
  - software-like flexibility
- Latency/Throughput metrics
- Performance analysis can be extended
  - parallelism among rounds
  - relative comparisons in terms of …
- Which algorithm “fits” FPGAs the *best* ?
  - Rijndael, Serpent

12