How well Are High-End DSPs Suited for the AES Algorithms?

AES Algorithms on the TMS320C6x DSP

Presentation at the AES 3 Conference
April 13, 2000

Thomas Wollinger
Jorge Guajardo
Christof Paar

Cryptography and Information Security (CRIS) Group
Electrical & Computer Engineering Department
Worcester Polytechnic Institute
Worcester, MA, USA
http://ece.wpi.edu/Research/crypt

Min Wang

Texas Instrument Inc.
12203 S.W. Freeway, MS 722

Stafford, TX, USA

Acknowledgments

Special thanks for his support of our work related to crypto algorithms on TI DSPs go to:

- William Cammack

Overview

- Motivation
- Methodology
- Results
- Conclusion

Why DSPs ?

The main application of DSPs are embedded systems:

- Wireless devices
  - Wireless phones
  - Wireless PDAs
  - Wireless laptops
  - etc.
- Broadcast services
  - Pay-TV
  - Voice-over IP
  - etc.
- Consumer electronic devices
- Modems
- ...

Remark: Major increase of embedded applications is predicted

Why Crypto on DSPs ?

Many embedded applications need security:

- Many DSP applications are wireless
→ unsecure channel (easy eavesdropping + message alteration)
- eCommerce and payment schemes are security sensitive
- Embedded multimedia/broadcast application need copy protection and/or access control
- Many embedded applications will need IPsec capabilities

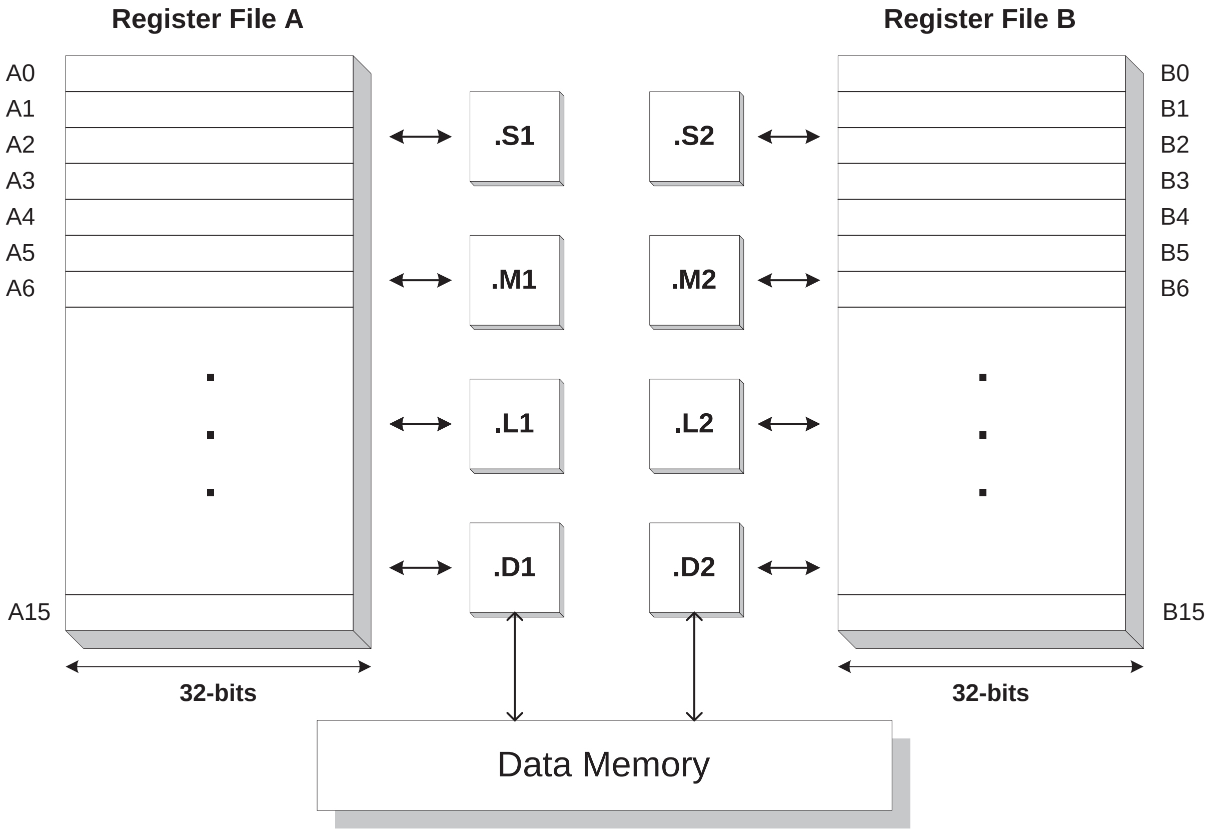
DSPs Features

In comparison to common general purpose processors (Intel,Motorola etc.) DSPs provide:

- Fast arithmetic
- Special instruction for signal processing application
- Real-time capabilities
- Relatively lower power
- Relatively lower price
- ...

The TMS320C62x DSP

High-end DSP in the current market:



- 1600 million instructions per second (MIPS)
- Clock rate 200 MHz
- 32 × 32-bit word registers
- 8 functional units

What did we do?

- Implementation of the 5 AES algorithms on the C62x
- C & *Linear Assembly* implementation
- Implementation of various modes of operation
- Optimized for speed
- RC6 results on (brand new) C64x

Methodology

1st step: Compiling C-code with TI C compiler with the highest level of optimization

2nd step: Restructure and rewrite the C-code

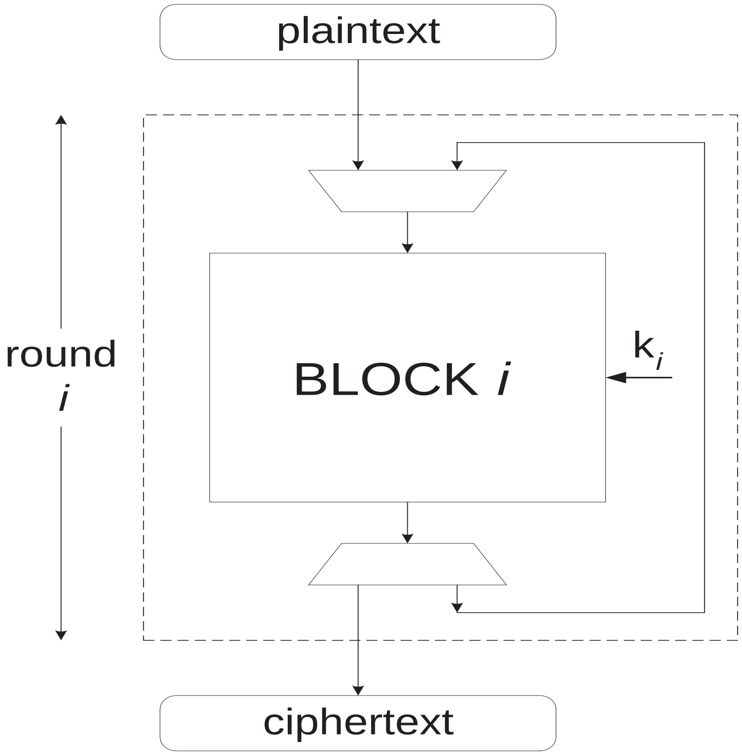
3rd step: Rewriting the encryption and decryption function in *linear Assembly*

`for example:` $add\ \ a, b, c$

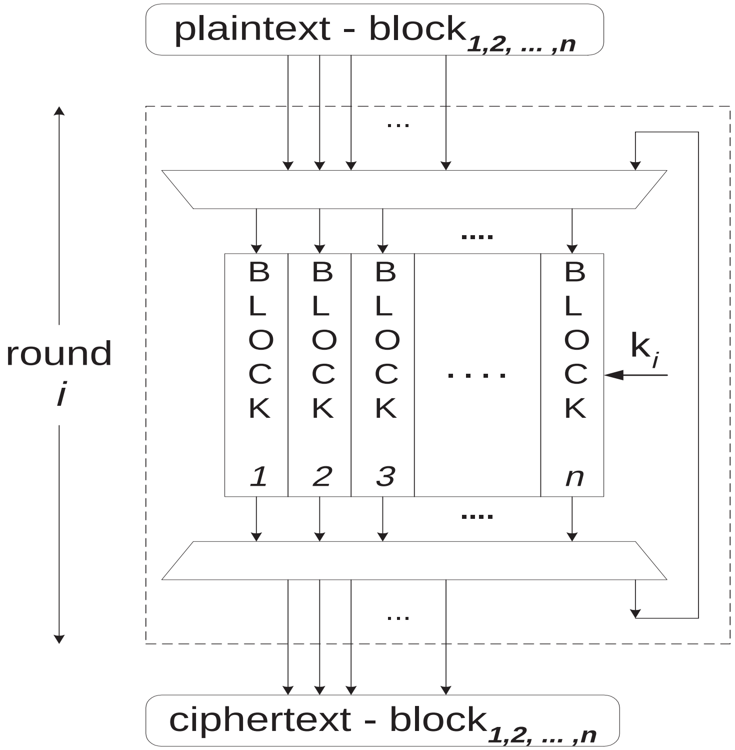
4th step: Implementation of a second version of code in which data blocks are processed in parallel

Single-Block Mode vs. Multi-Block Mode

Single-block mode
(CFB, OFB etc.)



Multi-block mode
(ECB, Counter Mode)



Results

		DSP multi-block mode @ 200MHz		DSP single-block mode @ 200MHz		Pentium-Pro @ 200MHz	DSP multi-block mode/Pentium
		cycles	Mbit/sec	cycles	Mbit/sec	Mbit/sec	
Twofish	encr.	184	139.1	308	83.1	95.0	1.5
	decr.	172	148.8	290	88.3	95.0	1.6
RC6	encr.	200[†]	128.0	292	87.7	97.8	1.3
	decr.	220[†]	116.4	281	91.1	112.8	1.03
Rijndael	encr.	228[‡]	112.3	228[‡]	112.3	70.5	1.6
	decr.	269[‡]	95.2	269[‡]	95.2	70.5	1.4
Mars	encr.	285	89.8	406	63.1	69.4	1.3
	decr.	280	91.4	400	64.0	68.1	1.3
Serpent	encr.	772	33.2	871[*]	29.4	26.8	1.2
	decr.	917[*]	27.9	917[*]	27.9	28.2	1.0

RC6 on the C64x

RC6	encr.	155	165.2	277	92.4	97.8	1.7
	decr.	154	166.2	278	92.1	112.8	1.5

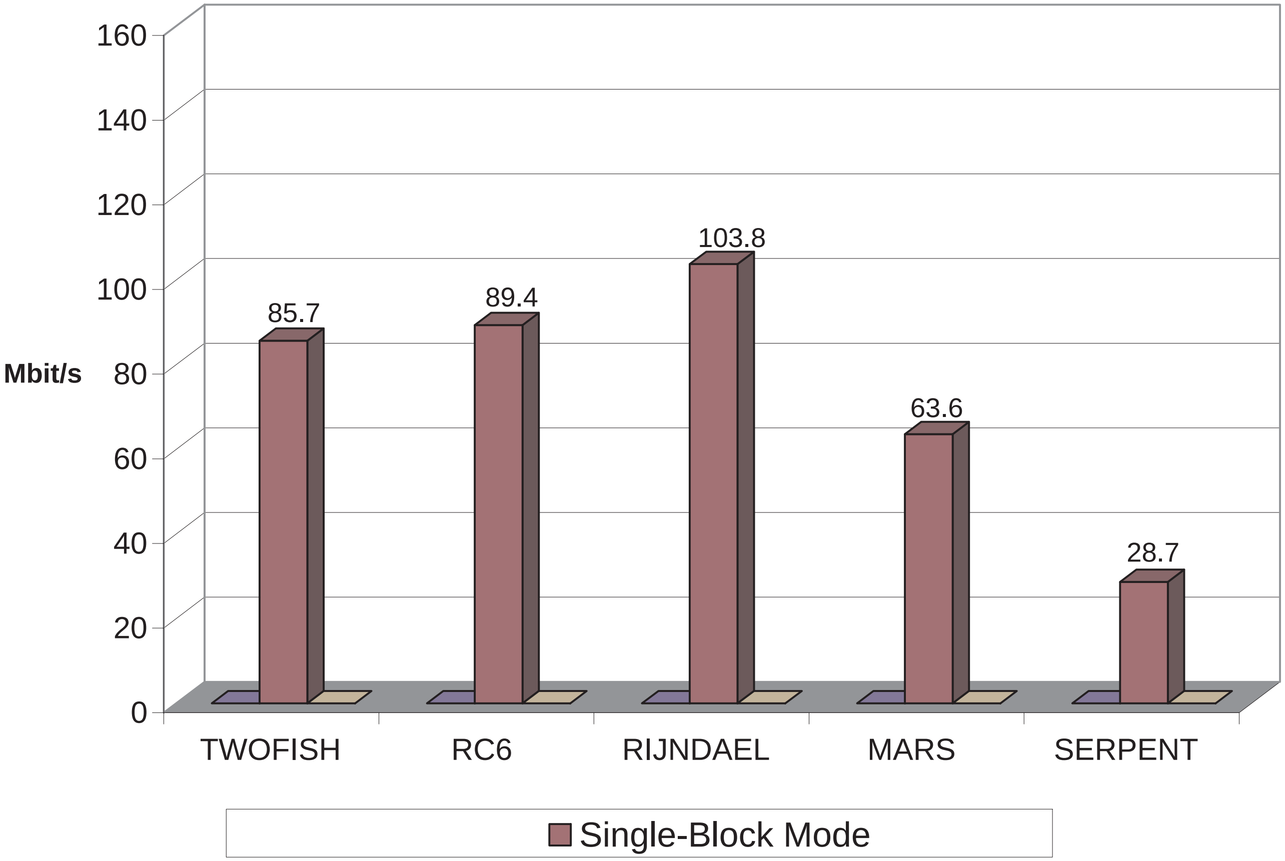
C implementation using the compiler version 4.0 unless otherwise indicated

[*] C implementation using compiler version 3.0

[†] Linear assembly implementation using compiler version 3.0

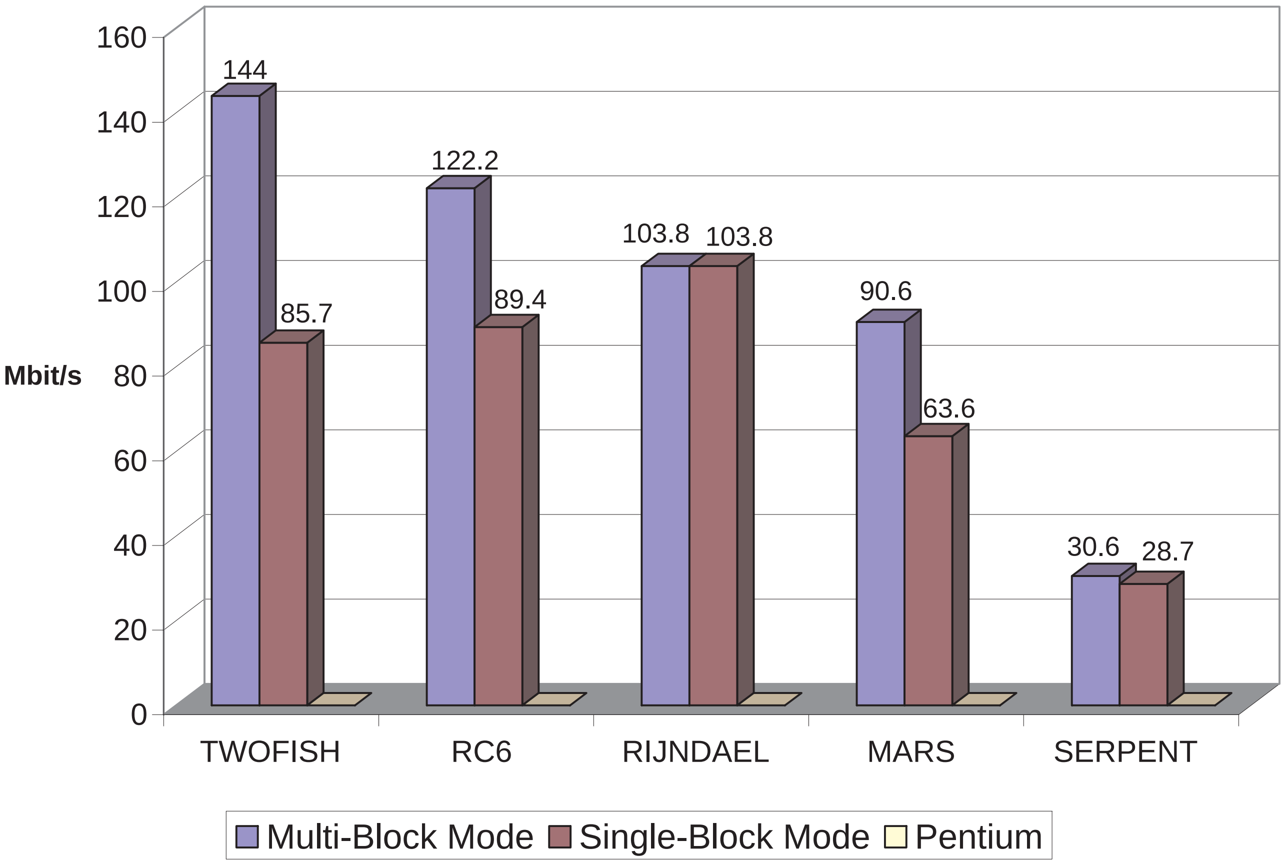
[‡] Linear assembly implementation using compiler version 4.0 alpha

Results



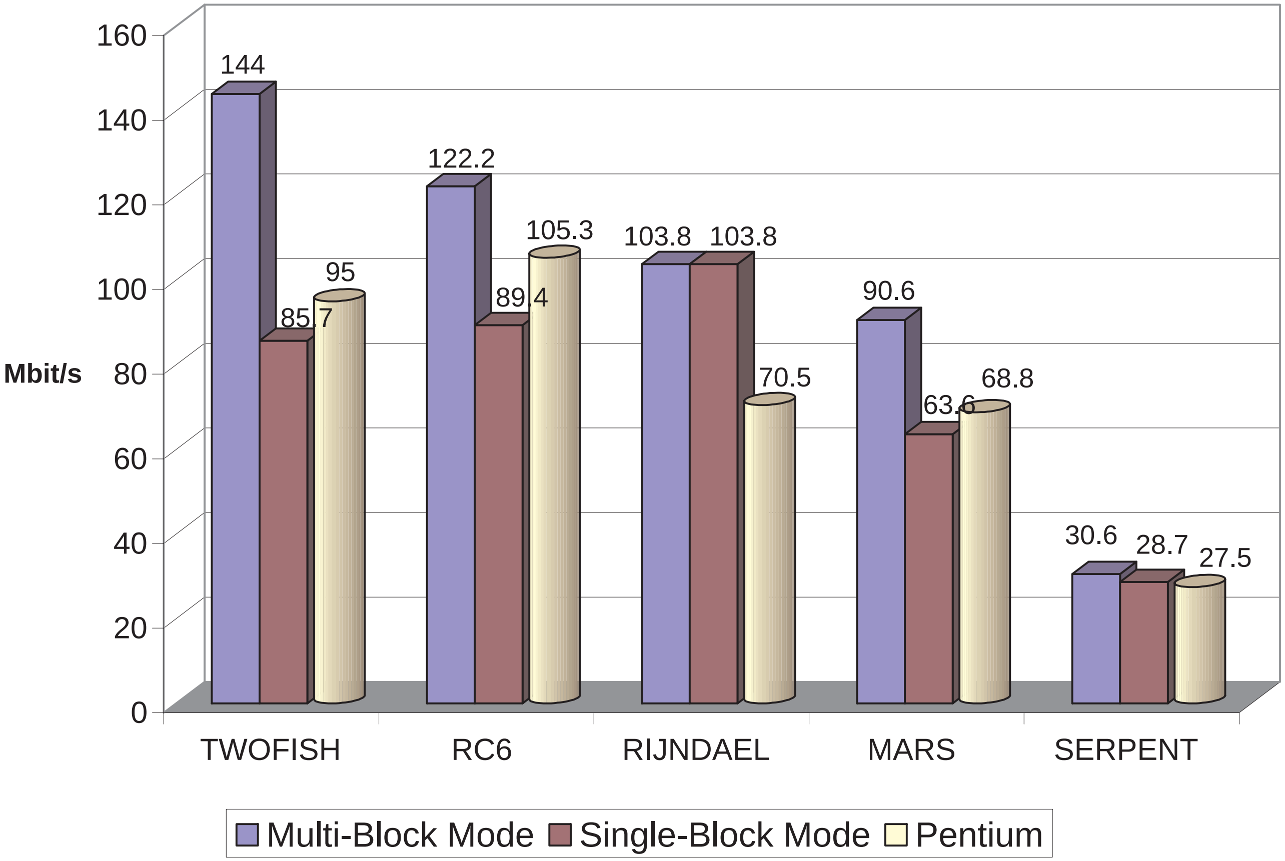
All results @ 200MHz

Results: Multi-Block Mode



All results @ 200MHz

Results - Comparison

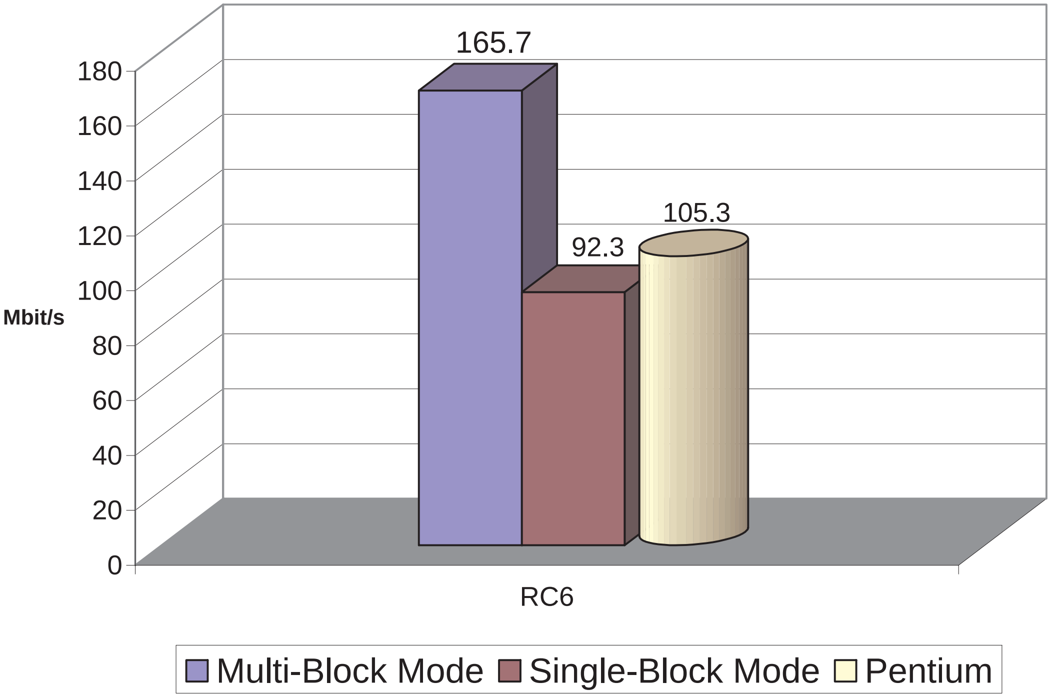


All results @ 200MHz

C64x DSP

- 8 functional units
- 64 × 32-bit registers
- up to 8800MIPS
- up to 1.1 GHz
- extented instruction set (e.g. rotation)

Results: RC6 on the C64x



All results @ 200MHz

Conclusions

- All algorithms in multi-block mode reached a higher speed than Pentium implementation with identical clockrate

- Throughput increase for some functions by over 50% on the 'C6201 compared with Pentium

- Highest speeds is single-block mode on the 'C62x:
  - Rijndael encryption 112.3 Mbit/sec
  - Rijndael decryption 95.2 Mbit/sec

- Highest speeds in multi-block mode on the 'C62x:
  - Twofish encryption 139.1 Mbit/sec
  - Twofish decryption 148.8 Mbit/sec

- Mean RC6 throughput on the C64x 165.7 Mbit/sec

→ State-of-the-art DSPs are well suited for the architecture of the AES finalists.