Evaluating 16-bit Processors for Elliptic Curve Cryptography

Erich Wenger and Mario Werner

IAIK – Graz University of Technology
Erich.Wenger@iaik.tugraz.at
www.iaik.tugraz.at

Overview

- Motivation
- Algorithms
- Processors
- Results

Motivation

We want to:

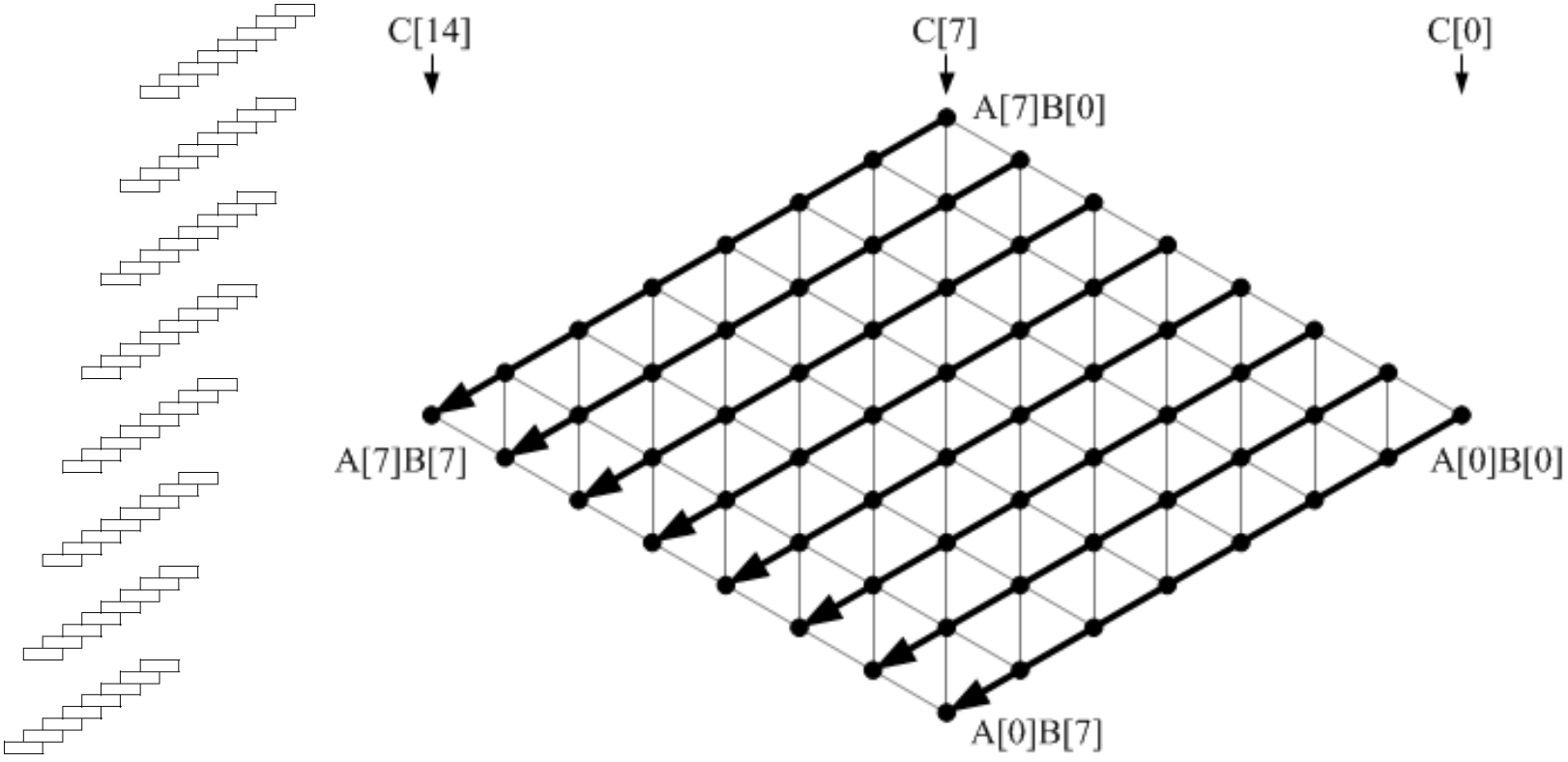
- Investigate current CPUs for ECC
- Find their limitations
- Save energy
- Improve performance

Point Multiplication Algorithm

- Montgomery Ladder [Hutter]
  - 7 registers
- Point Verification [Ebeid]
- Randomized Projective Coordinates [Coron]

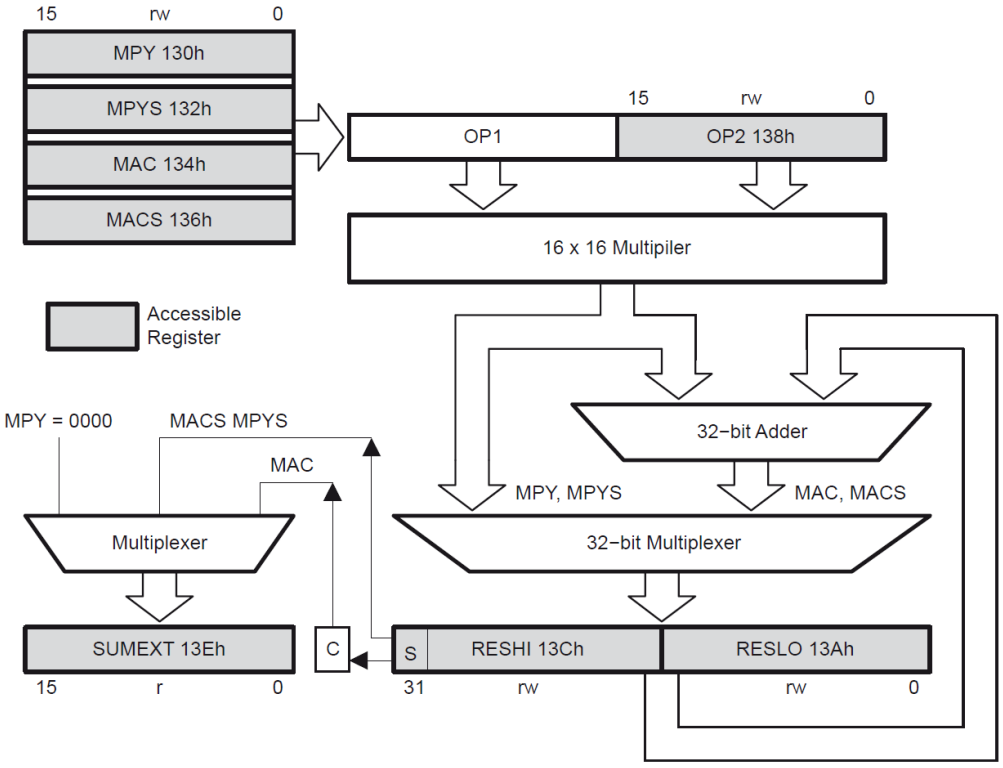
Multi-Precision Multiplication

- Operand Scanning



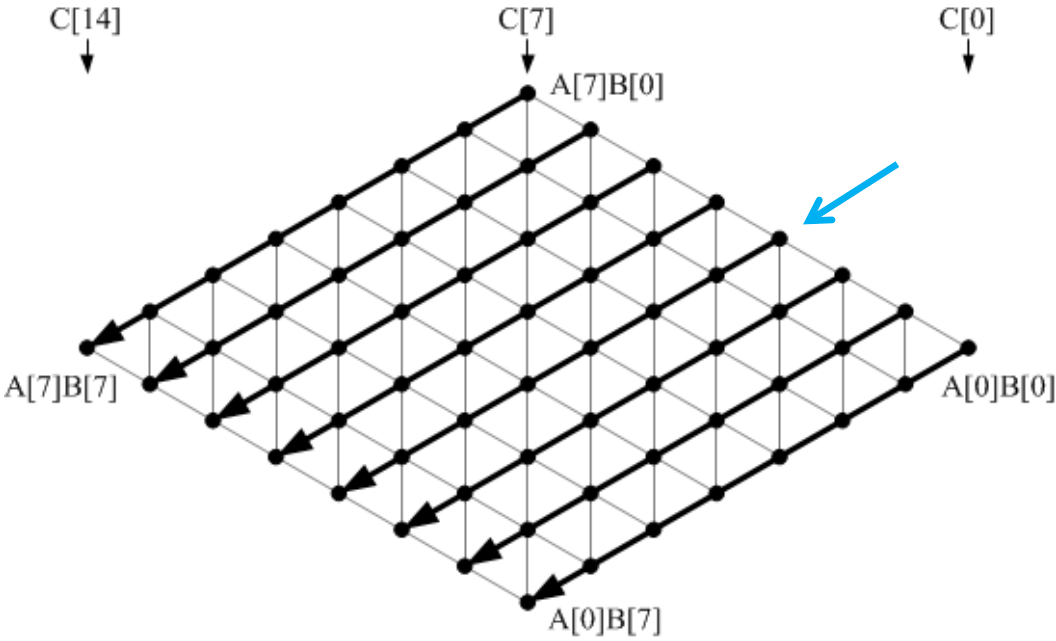
MSP430

- Manufacturer: Texas Instruments
- Low-Power RISC Processor
- 16 Registers (12 useable)
- 27 Instructions
- Memory Mapped Multiplier



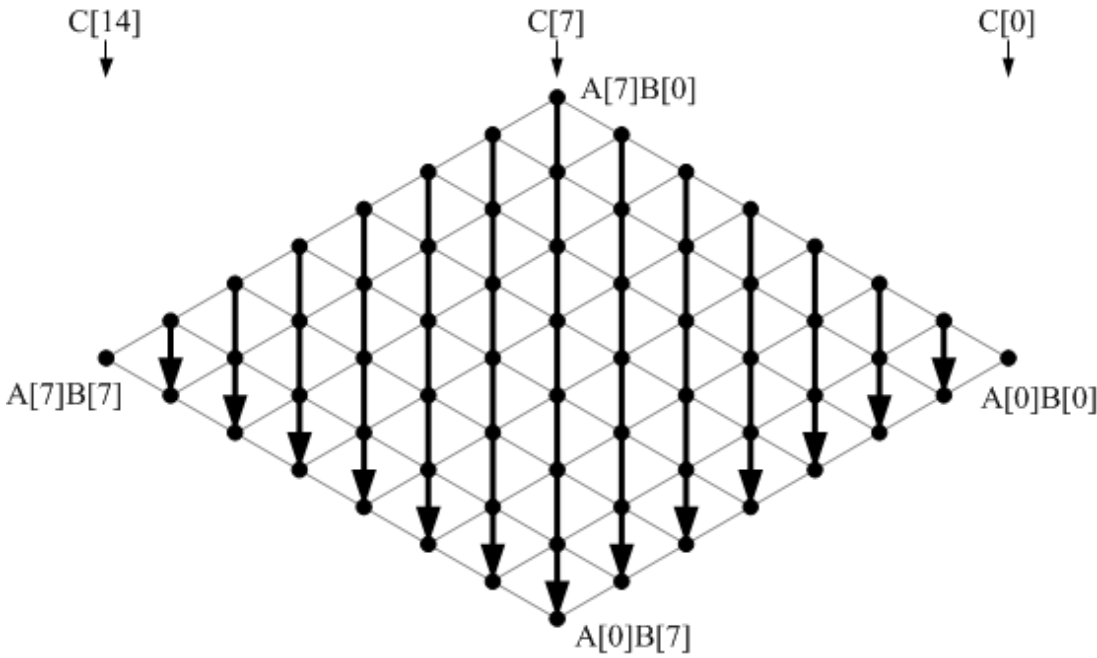
MSP430 – Operand Scanning

```
outer_loop:
   MOV.W @R12+, &MPY
inner_loop:
   MOV.W @R13+, &OP2
   ADD.W  &RESLO, R6
   ADDC.W &RESHI, R7
```



MSP430 – Product Scanning

```
inner_loop:
   MOV.W @R12+, &MAC
   MOV.W @R13 , &OP2
   DECD   R13
   ADD.W &SUMEXT, R11
```



PIC24 vs. dsPIC

Both Processors:

- 16-bit RISC
- 24-bit Instruction Word
- 16 registers (14 useable)
- Used for:
  - Motor Control
  - Signal Processing

dsPIC:

- Digital Signal Processing Engine
  - Multiply-Accumulate
- Two Address Generation Units
- Loop Instructions
  - `DO`
  - `REPEAT`

dsPIC – Product Scanning

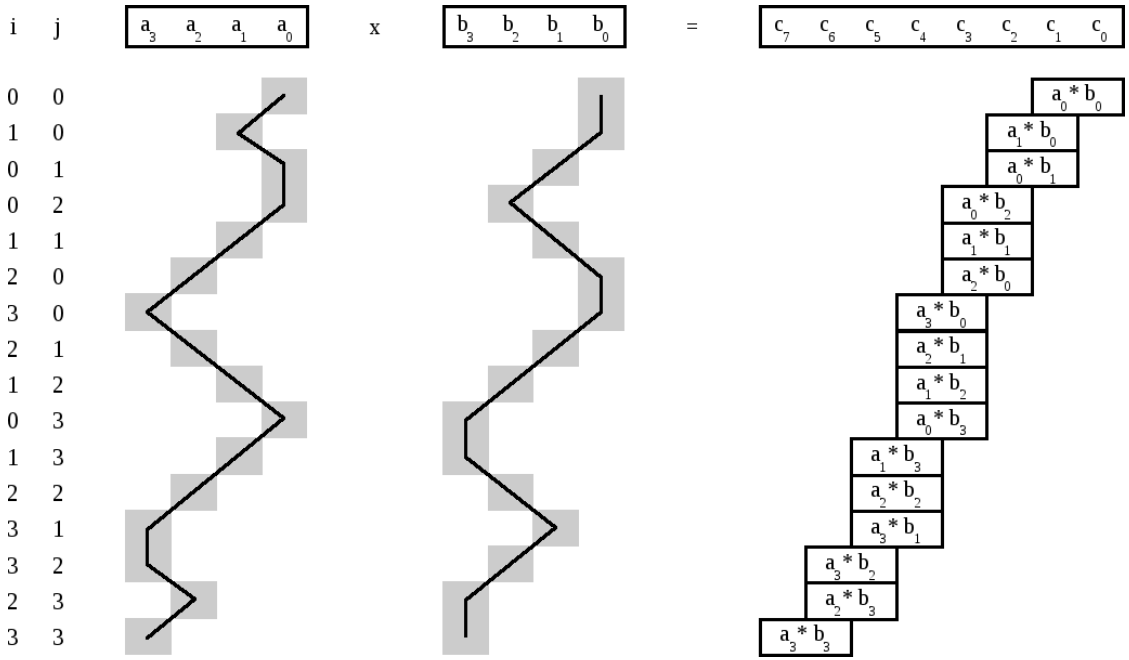
- 16-bit Multiplication
- 32-bit Addition (plus Overflow)

$$ACC \leftarrow ACC + A[i] \cdot B[j]$$

- Load A[i] and B[j]
- Memory Addressing ($i \leftarrow i + 1$, $j \leftarrow j - 1$)

```
REPEAT W4
MAC W5*W6, A, [W8]+=2, W5, [W10]-=2, W6
```

dsPIC – Unrolled Product Scanning




```
MAC W5*W6, A, [W9]-=2, W5, [W11]+=2, W6
MAC W5*W6, A, [W9], W5, [W11]+=2, W6
MAC W5*W6, A, [W9]+=2, W5, [W11]-=2, W6
MOV [W7],[W2++]
SFTAC A, #16
```

```
MAC W5*W6, A, [W9]+=2, W5, [W11]-=2, W6
MAC W5*W6, A, [W9]+=2, W5, [W11]-=2, W6
MAC W5*W6, A, [W9]+=2, W5, [W11], W6
MAC W5*W6, A, [W9]-=2, W5, [W11]+=2, W6
MOV [W7],[W2++]
SFTAC A, #16
```

dsPIC – Montgomery Multiplication

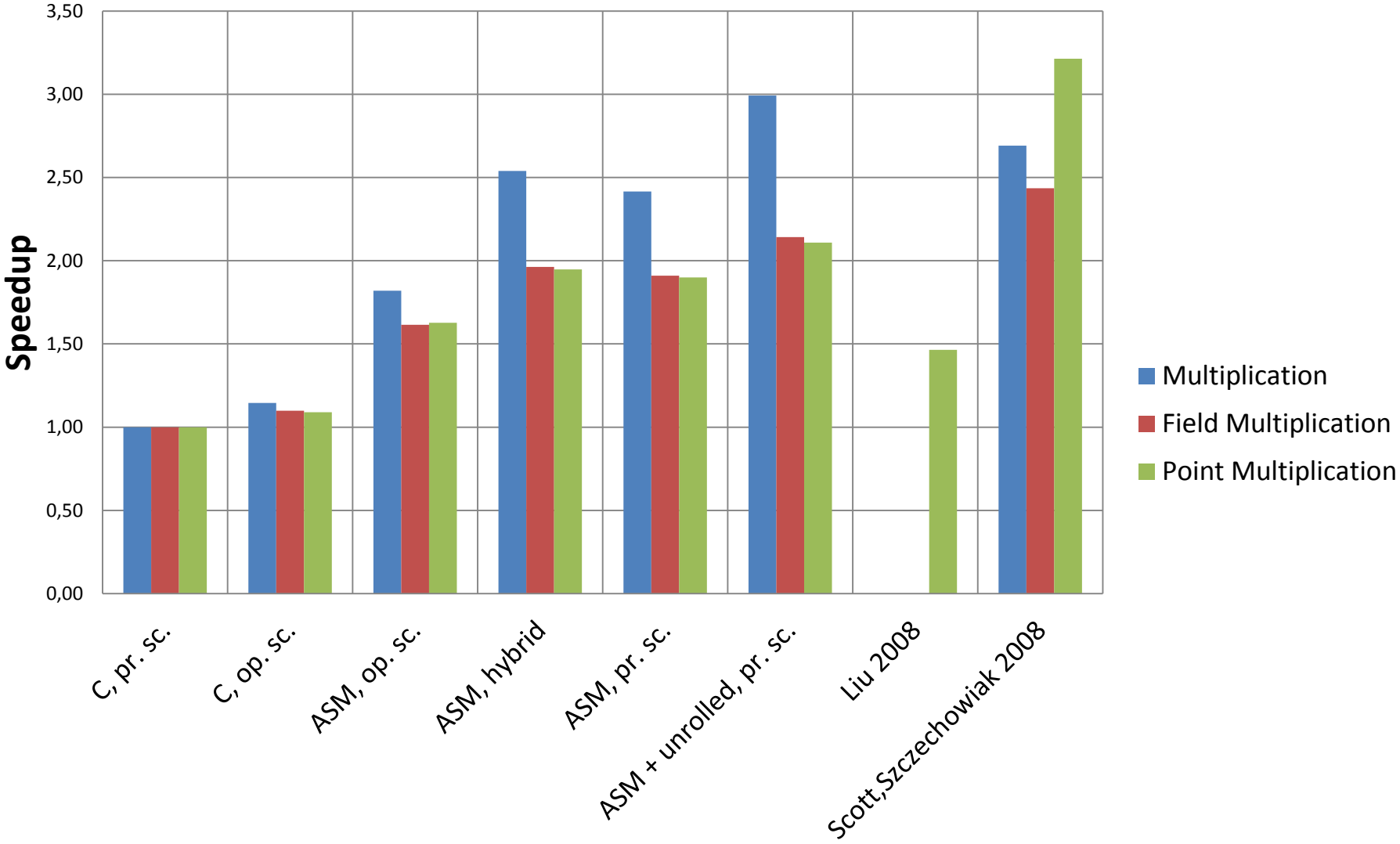
$$R = 2^{WN} > p$$
$$\tilde{a} \equiv aR \ (mod\ p)$$
$$\tilde{b} \equiv bR \ (mod\ p)$$
$$\tilde{c} \equiv Mont(\tilde{a}\tilde{b})$$
$$\equiv (aR)(bR)R^{-1}$$
$$\equiv abR \equiv cR \ \ (mod\ p)$$
$$\tilde{a} \equiv Mont(a, R^2)$$
$$\equiv aR^2R^{-1} \equiv aR$$
$$c \equiv Mont(\tilde{c}, 1)$$
$$\equiv (cR)R^{-1}$$

NIST Reduction…

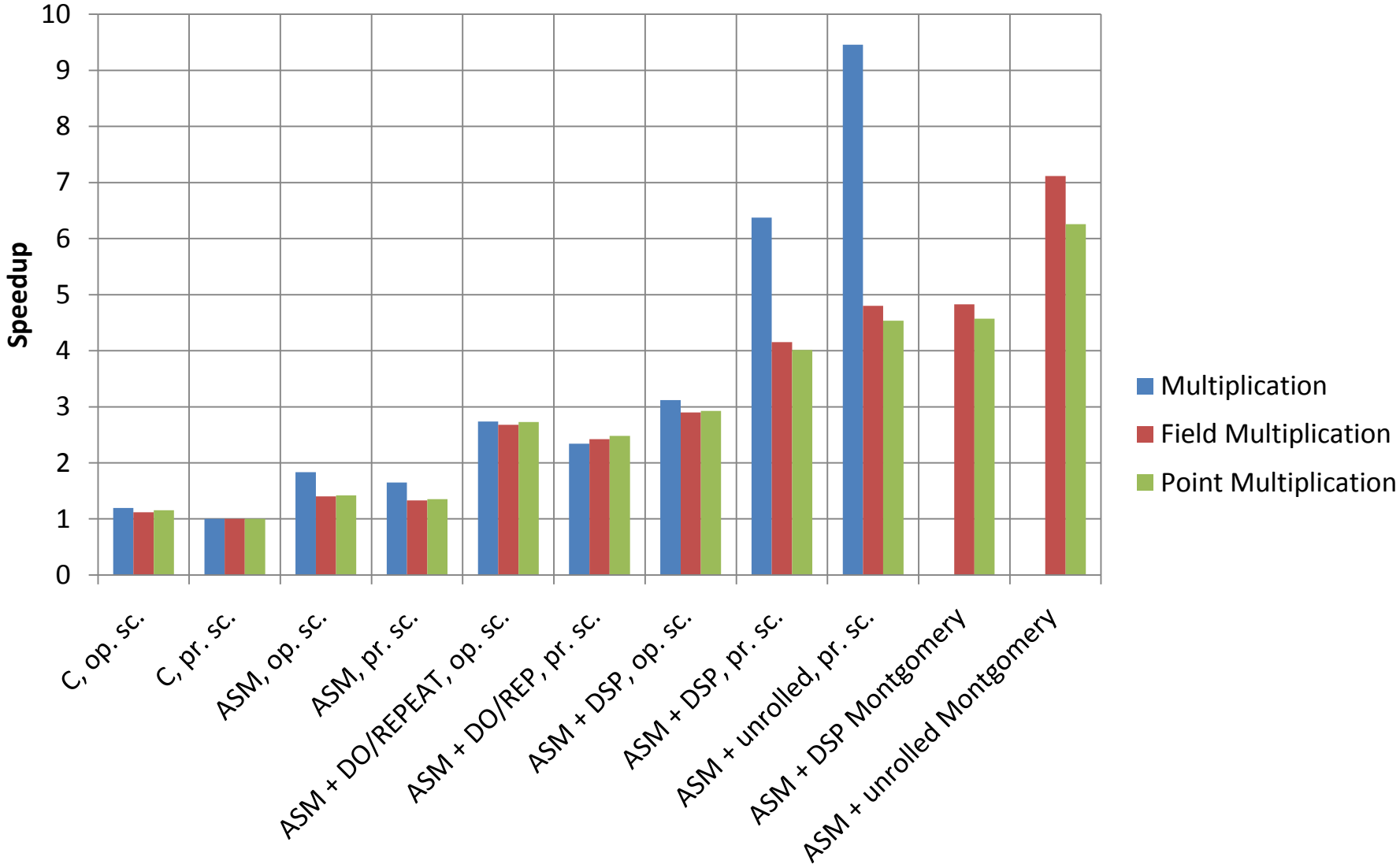
Results

- SECG:
  - secp160r1
    removed in 2010
- NIST:
  - P-192
  - P-224
  - P-256
- IAR Embedded Workbench 5.20
- Microchip MPLAB C30 v3.25

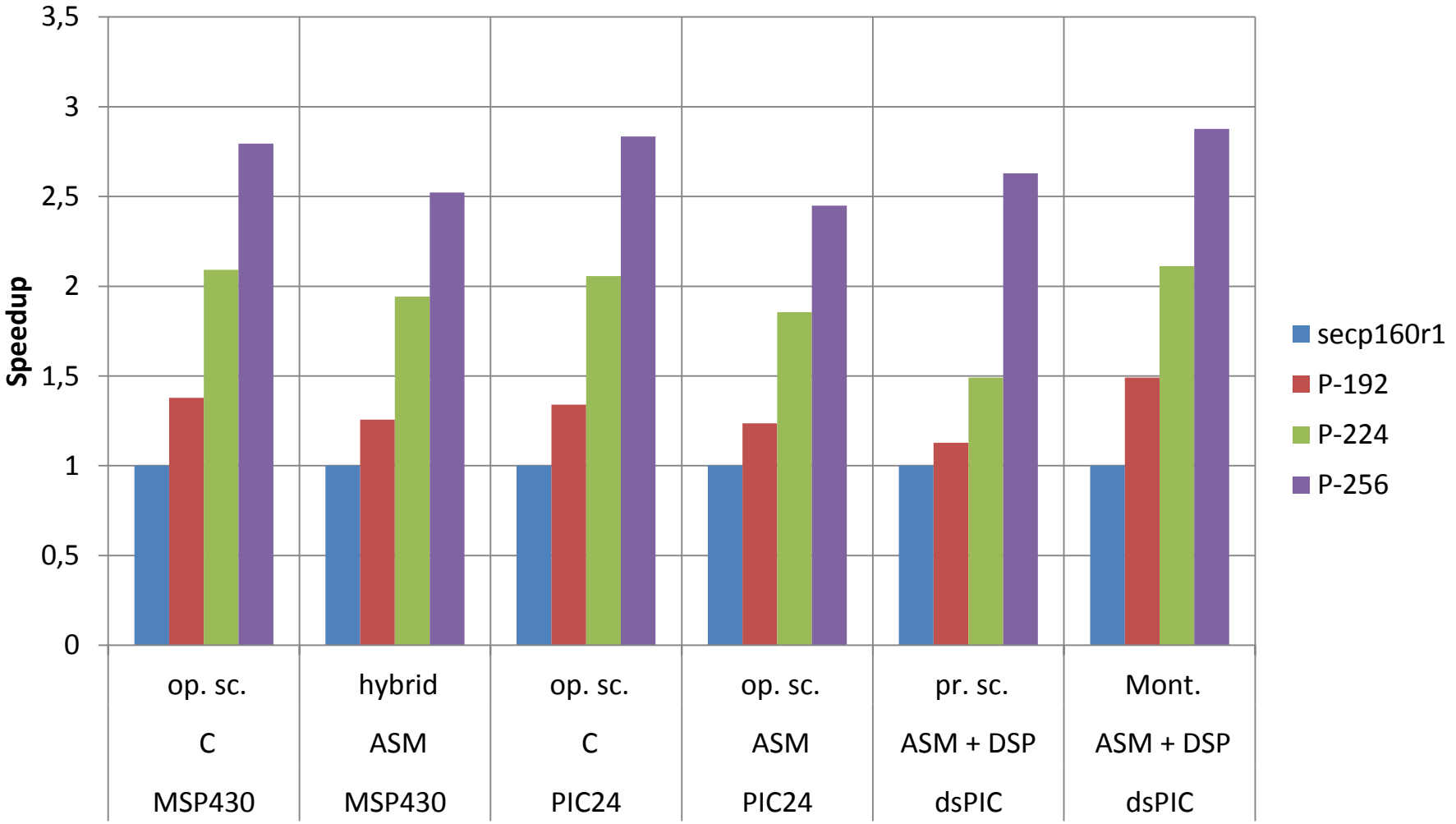
Results: MSP430



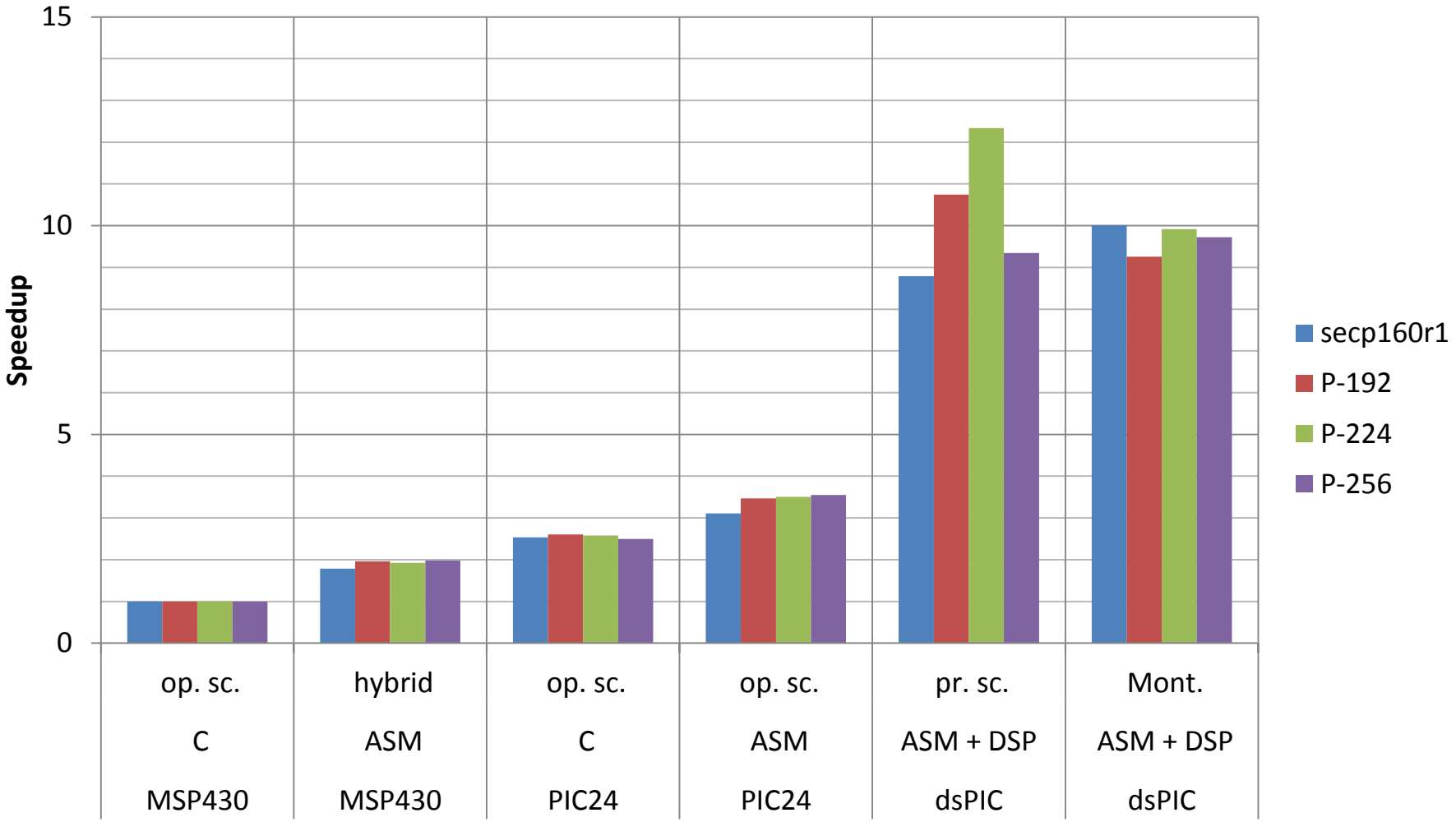
Results: PIC24, dsPIC



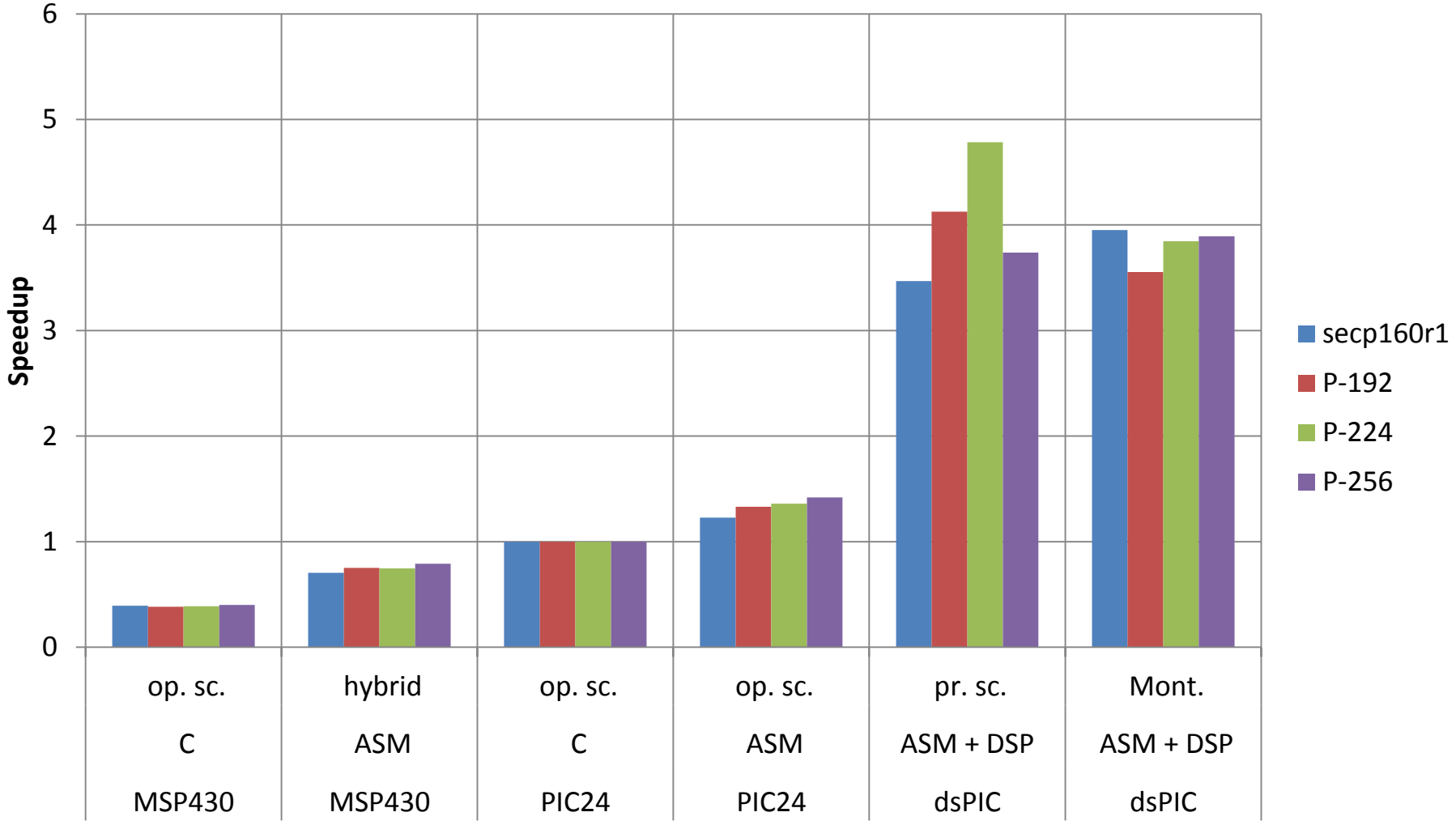
Results: Point Multiplication



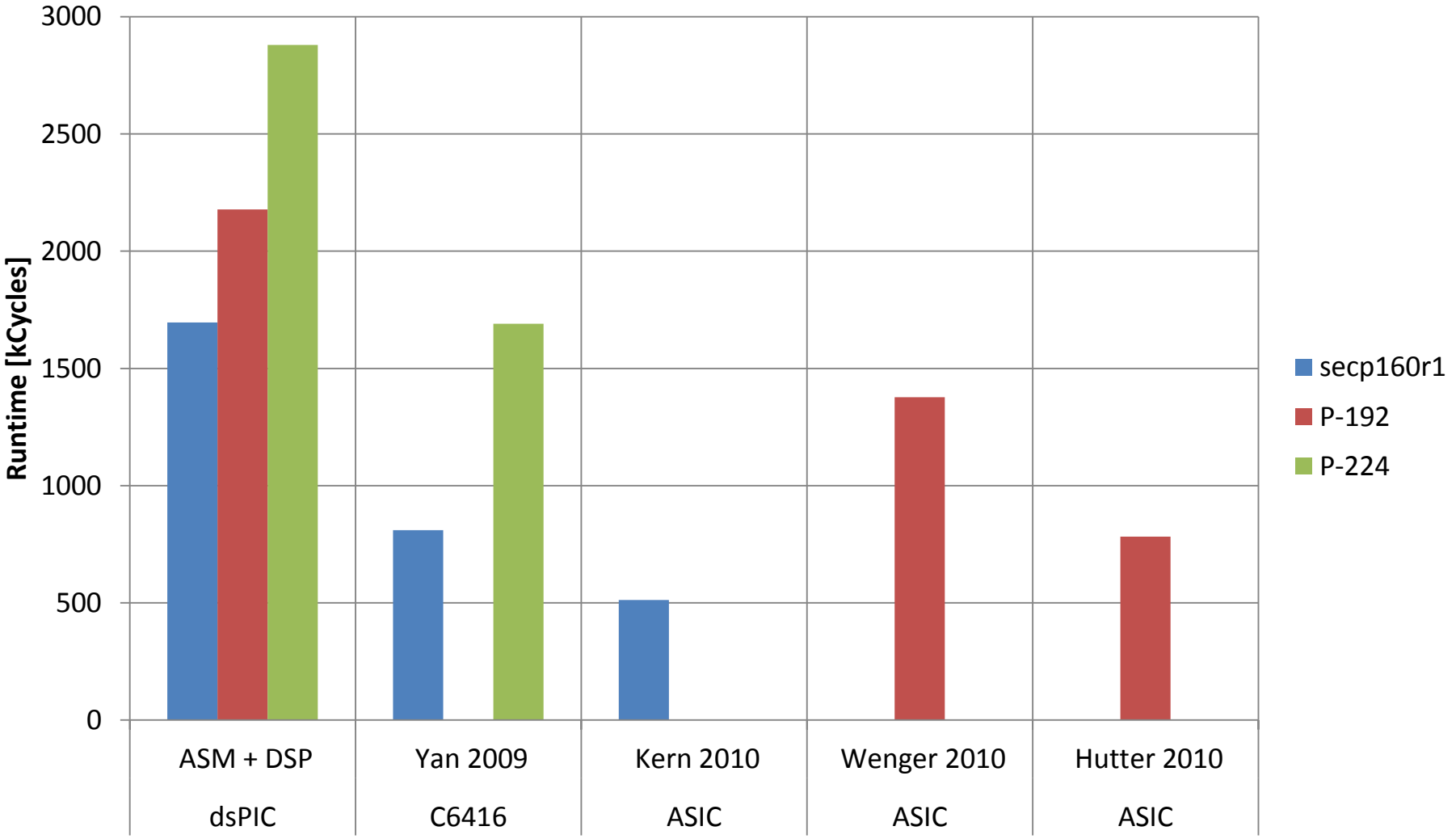
Results: Point Multiplication



Results: Point Multiplication



Results: Related Work



Thank you…

This work has been supported by the Austrian Government through the research program FIT-IT Trust in IT Systems under the project number 825743 (project PIT).

Results

Implementation		Multi-Prec. Mult.	$\mathbb{F}_{p_{160}}$ Mult.	Point Mult.
MSP430	C	op. sc.	4,103	6,069	16,985,654
MSP430	C	pr. sc.	4,699	6,665	18,512,606
MSP430[a]	ASM	op. sc.	2,583	4,127	11,380,361
MSP430[a]	ASM	pr. sc.	1,945	3,489	9,745,805
MSP430[a]	ASM	hybrid	1,851	3,395	9,504,977
MSP430[a]	ASM + unrolled	pr. sc.	**1,570**	**3,112**	**8,779,931**
PIC24	C	op. sc.	1,423	2,393	6,703,476
PIC24	C	pr. sc.	1,702	2,675	7,753,292
PIC24[b]	ASM	op. sc.	**929**	**1,909**	**5,463,648**
PIC24[b]	ASM	pr. sc.	1,031	2,011	5,739,732
dsPIC[c]	ASM + DO/REP.	op. sc.	622	998	2,840,921
dsPIC[c]	ASM + DO/REP.	pr. sc.	727	1,104	3,127,253
dsPIC[c]	ASM + DSP	op. sc.	546	923	2,648,377
dsPIC[c]	ASM + DSP	pr. sc.	267	644	1,932,431
dsPIC[c]	ASM + unrolled	pr. sc.	**180**	557	1,709,537
dsPIC[c]	ASM + DSP	Montgomery	—	554	1,696,433
dsPIC[c]	ASM + unrolled	Montgomery	—	**376**	**1,239,281**
MSP430	Liu *et al.* [20]				12,645,040
MSP430[d]	Scott *et al.* [29, 31]		1,746	2,736	5,760,000
TMS320	Yan *et al.* [36]		150	290	810,000
ASIC	Kern *et al.* [18]	pr. sc.		167	511,864

Results

	Implementation		secp160r1	P-192	P-224	P-256
MSP430	C	op. sc.	16,986	23,405	35,531	47,455
MSP430	ASM	hybrid	9,505	11,949	18,464	23,973
PIC24	C	op. sc.	6,703	8,985	13,781	18,992
PIC24	ASM	op. sc.	5,464	6,754	10,138	13,379
dsPIC	ASM + DSP	pr. sc.	1,932	**2,178**	**2,880**	5,079
dsPIC	ASM + DSP	Mont.	**1,696**	2,528	3,582	**4,879**
MSP430	Liu *et al.* [20]		12,645			
C6416	Yan *et al.* [36]		810		1,690	
ASIC	Kern *et al.* [18]	pr. sc.	512			
ASIC	Wenger *et al.* [35]	pr. sc.		1,377		
ASIC	Hutter *et al.* [15]	pr. sc.		783		