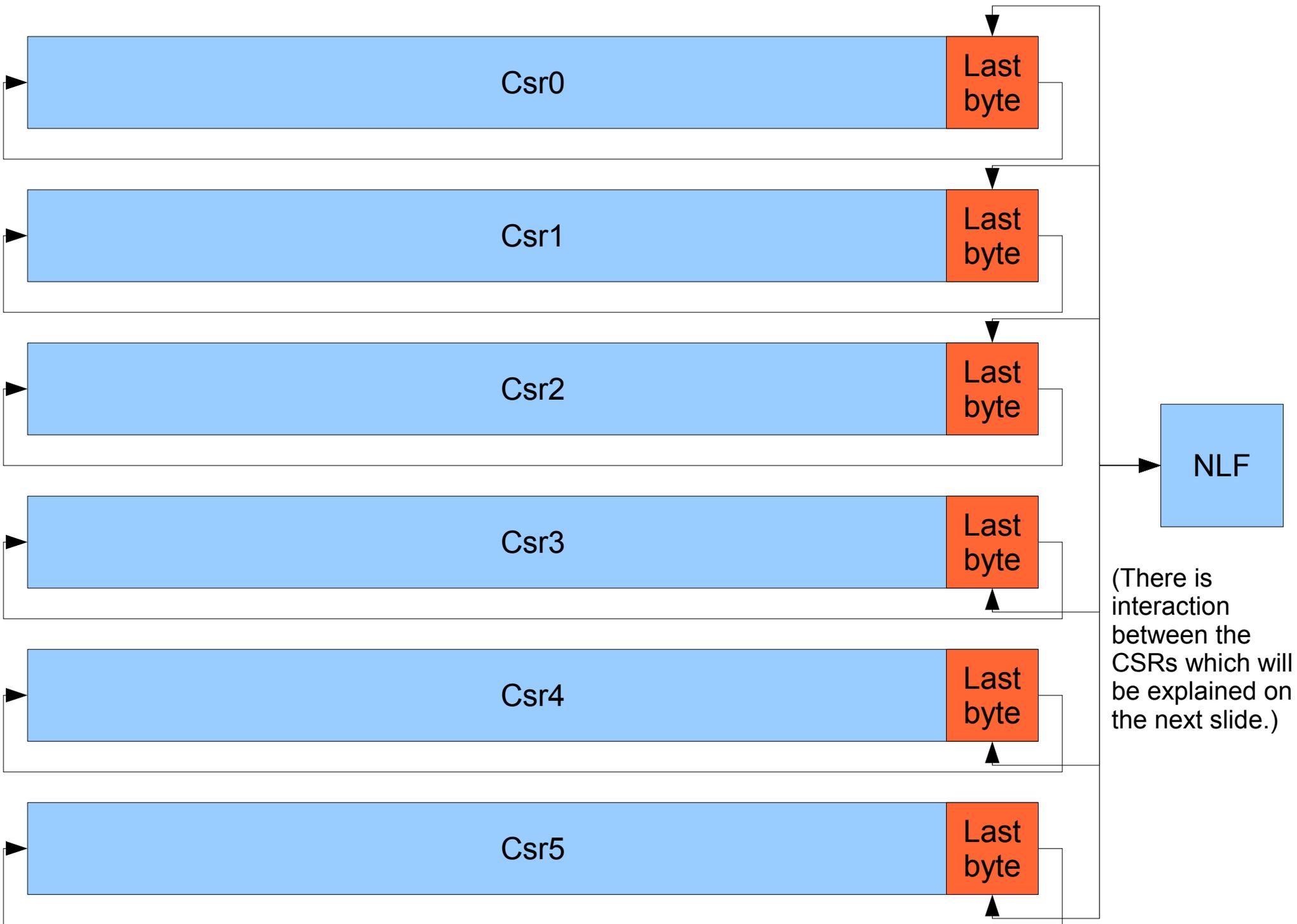
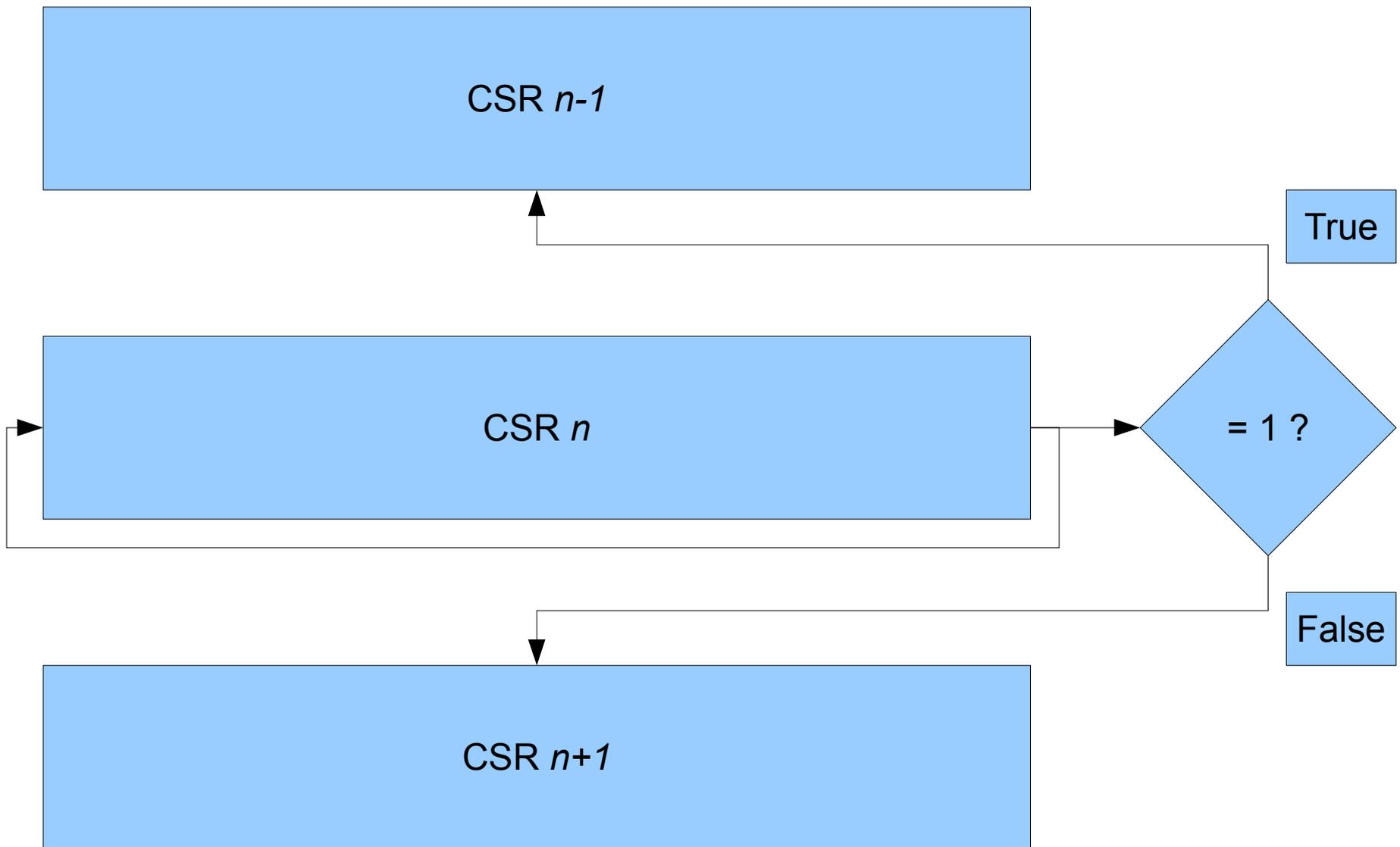


Ponic

The third slowest algorithm submitted!

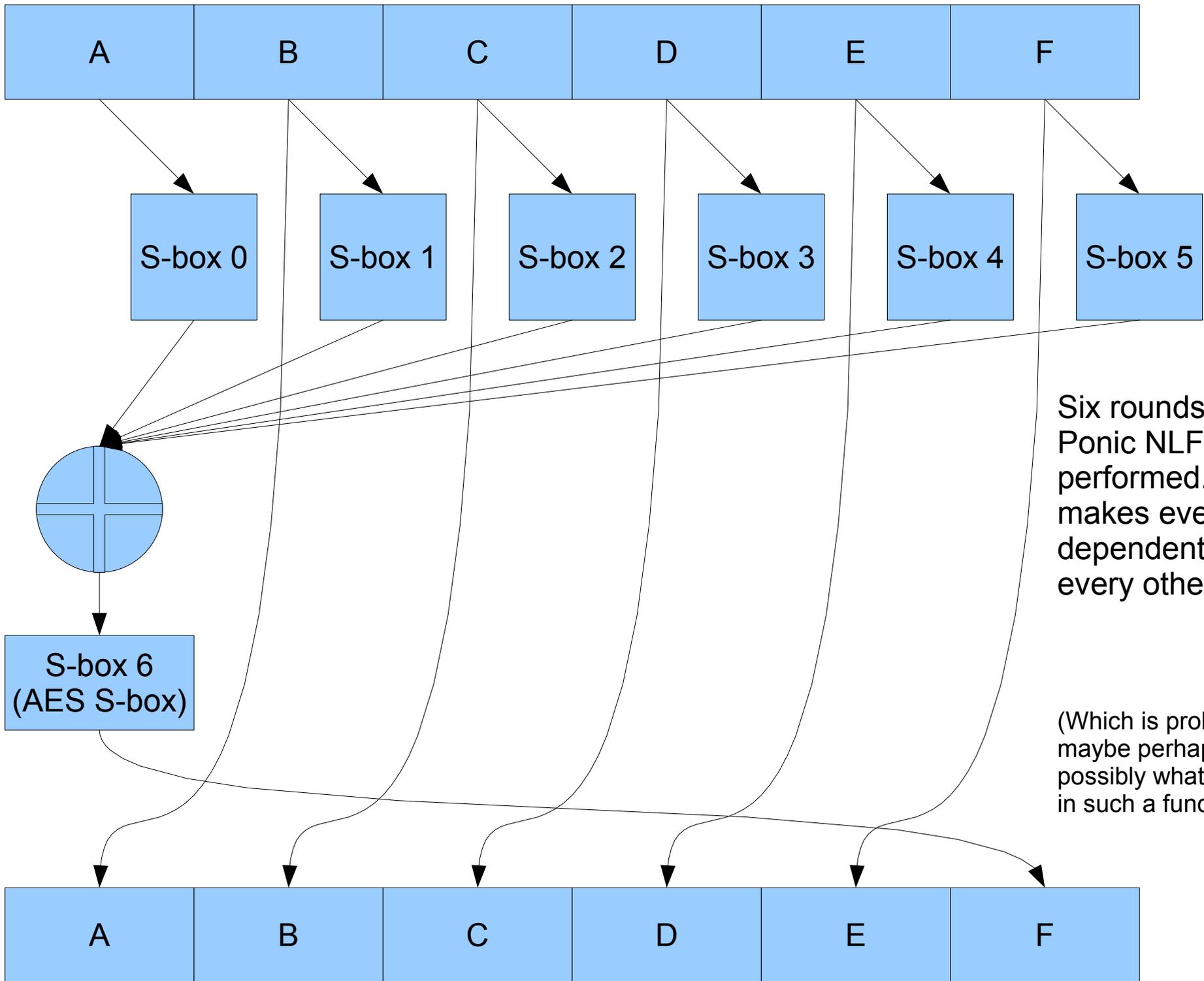
Designed by Peter Schmidt-Nielsen





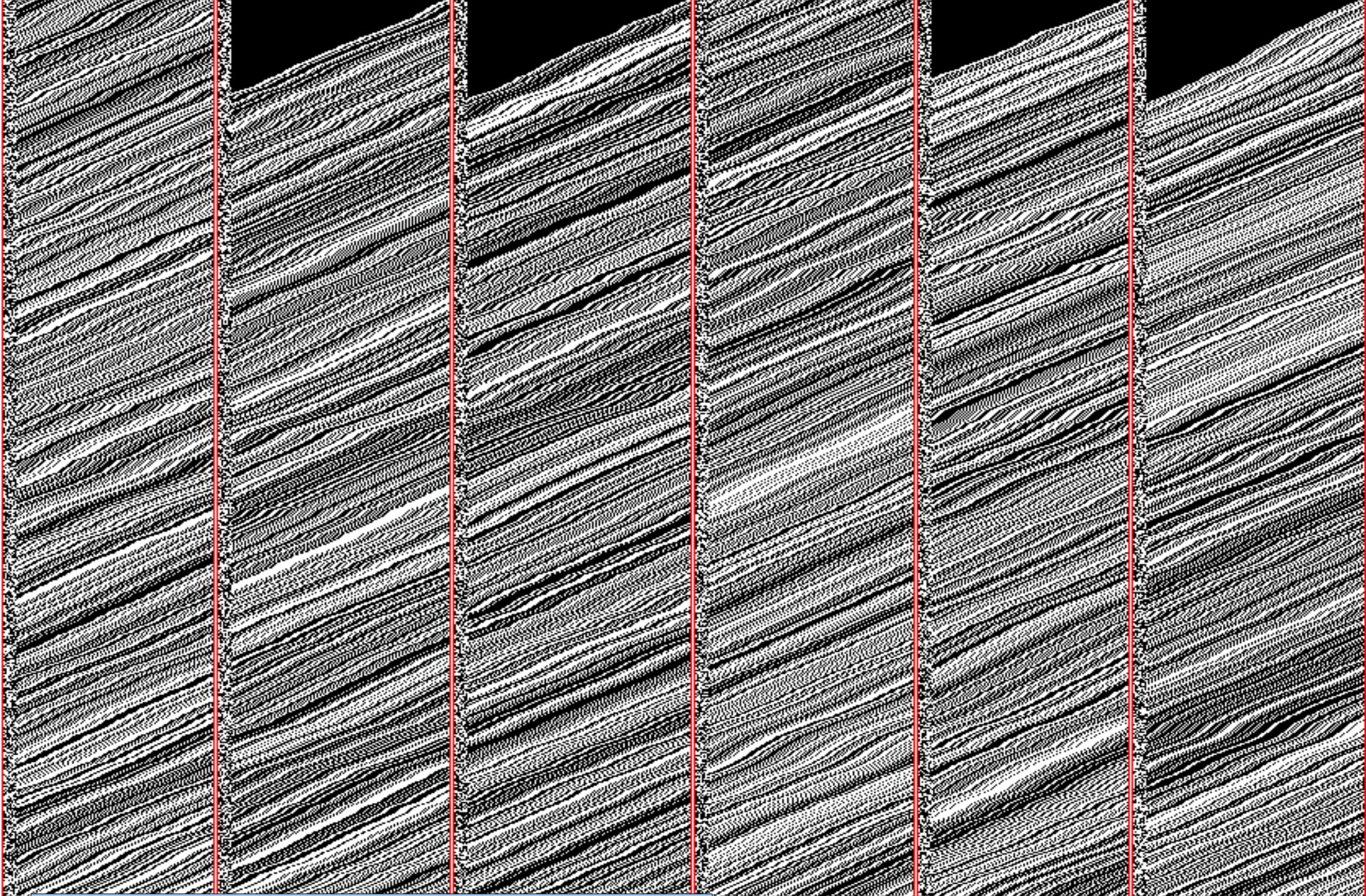
Each CSR is stepped in sequence, where stepping a CSR causes either the next or the previous CSR to be stepped. This has two big advantages:

- 1) Each CSR is stepped anywhere from 1-3 times in a data dependent way.
- 2) Despite this, Ponoc still maintains near deterministic execution time.



Six rounds of the Ponic NLF are performed. This makes every bit dependent on every other bit.

(Which is probably maybe perhaps just possibly what you want in such a function.)



Ponic("Nobody expects the spammish repetition!")
Note that the leftmost column of each CSR is noisy.

Csr 0

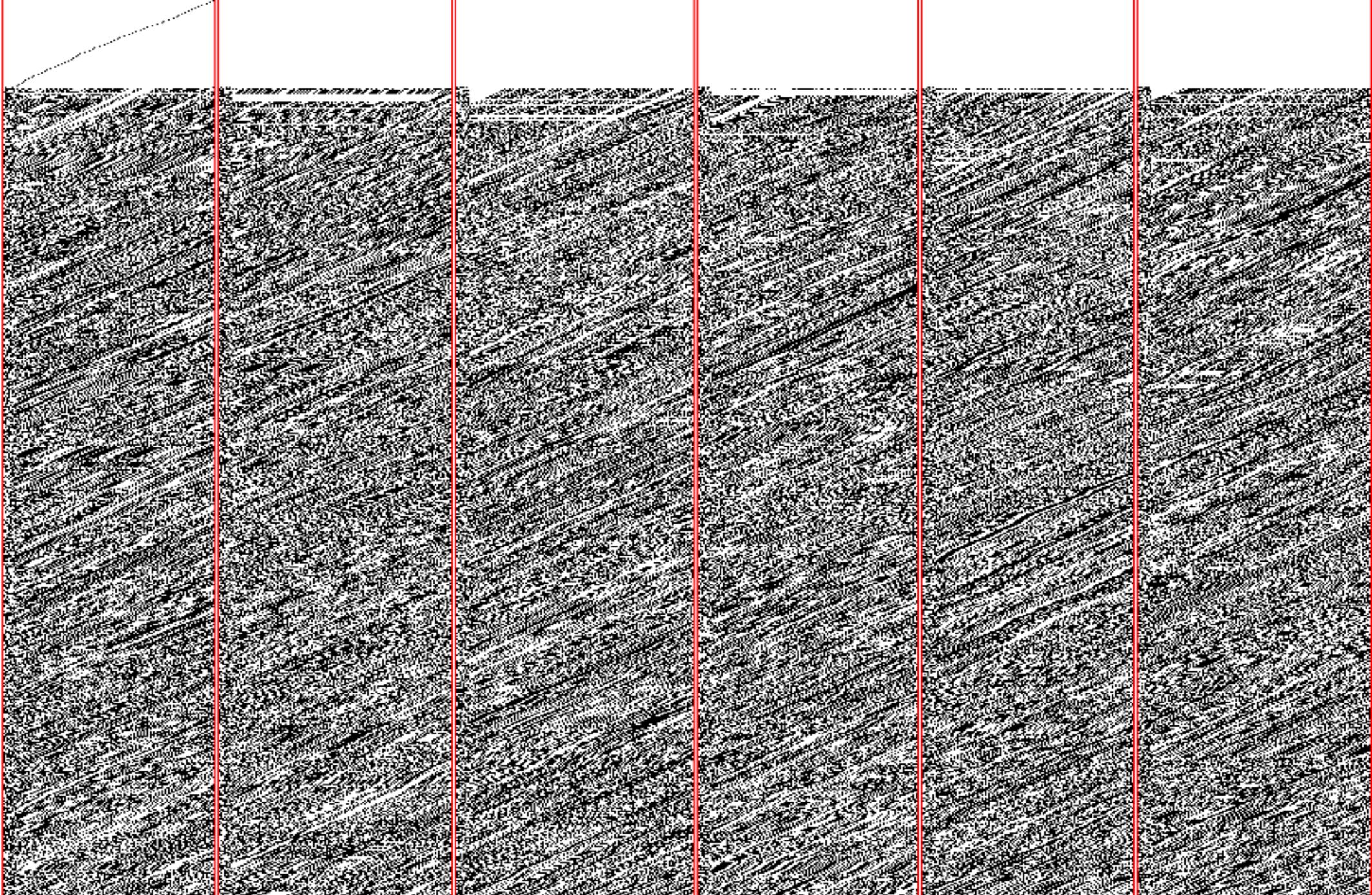
Csr 1

Csr 2

Csr 3

Csr 4

Csr 5



$\text{Ponic}(m) \oplus \text{Ponic}(m \oplus 1)$

- 1) Things diffuse very quickly once the bit enters the CSR.
- 2) The differing bit "wobbles" due to the clocking scheme.

Csr 0

Csr 1

Csr 2

Csr 3

Csr 4

Csr 5

Ponic Performance:

Initial published performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	7,000-7,500
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	3,000-3,500
Optimized-8bit	Estimate	Estimate	Estimate	~24,000
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	700,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	600,000 cycles

More accurate, and optimized performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	1,600
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	800
Optimized-8bit	Estimate	Estimate	Estimate	???
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	280,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	240,000 cycles

Disclaimer: Even those second numbers are not very reliable.

They are gotten from my new optimized numbers of 4,000 cycles per byte, but then I found that my computer is actually running at 800MHz, not 2GHz, so I divided by 2.5 to correct, but then I forgot to give gcc the -O3 switch, so then I retested, etc... In short, these numbers are processed a bit, and may not be very accurate. But the 7,000cpb is certainly an accurate upper bound.

Ponic Performance: (with AES instruction)

Initial published performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	7,000-7,500
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	3,000-3,500
Optimized-8bit	Estimate	Estimate	Estimate	~24,000
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	700,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	600,000 cycles

More accurate, and optimized performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	1,600
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	800
Optimized-8bit	Estimate	Estimate	Estimate	???
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	280,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	240,000 cycles

Disclaimer: Even those second numbers are not very reliable.

They are gotten from my new optimized numbers of 4,000 cycles per byte, but then I found that my computer is actually running at 800MHz, not 2GHz, so I divided by 2.5 to correct, but then I forgot to give gcc the -O3 switch, so then I retested, etc... In short, these numbers are processed a bit, and may not be very accurate. But the 7,000cpb is certainly an accurate upper bound.

Ponic Performance: (with time travel)

Initial published performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	7,000-7,500
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	3,000-3,500
Optimized-8bit	Estimate	Estimate	Estimate	~24,000
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	700,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	600,000 cycles

More accurate, and optimized performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	1,600
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	800
Optimized-8bit	Estimate	Estimate	Estimate	???
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	280,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	240,000 cycles

Disclaimer: Even those second numbers are not very reliable.

They are gotten from my new optimized numbers of 4,000 cycles per byte, but then I found that my computer is actually running at 800MHz, not 2GHz, so I divided by 2.5 to correct, but then I forgot to give gcc the -O3 switch, so then I retested, etc... In short, these numbers are processed a bit, and may not be very accurate. But the 7,000cpb is certainly an accurate upper bound.

Ponic Performance: (with a side order of Gröstl)

Initial published performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	7,000-7,500
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	3,000-3,500
Optimized-8bit	Estimate	Estimate	Estimate	~24,000
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	700,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	600,000 cycles

More accurate, and optimized performance:

Performance:	Processor	Operating System	Compiler	Cycles/Byte
Optimized-32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	1,600
Optimized-64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	800
Optimized-8bit	Estimate	Estimate	Estimate	???
Setup for 32bit	Athlon 2x 2.0GHz	Ubuntu 8.04	Gcc 4.2.3	280,000 cycles
Setup for 64bit	Athlon 1.5GHz	Ubuntu 8.04	Gcc 4.2.3	240,000 cycles

Disclaimer: Even those second numbers are not very reliable.

They are gotten from my new optimized numbers of 4,000 cycles per byte, but then I found that my computer is actually running at 800MHz, not 2GHz, so I divided by 2.5 to correct, but then I forgot to give gcc the -O3 switch, so then I retested, etc... In short, these numbers are processed a bit, and may not be very accurate. But the 7,000cpb is certainly an accurate upper bound.

Questions?