Which phase-3 eSTREAM ciphers provide the best software speeds?

Daniel J. Bernstein *

Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
snuffle6@box.cr.yp.to

Abstract. This paper compares the software speeds of 128-bit 10-round AES, 256-bit 14-round AES, 256-bit CryptMT v3, 256-bit Dragon, 128-bit HC-128, 256-bit HC-256, 128-bit LEX v2, 128-bit NLS v2, 128-bit Rabbit, 256-bit RC4, 256-bit Salsa20/8, 256-bit Salsa20/12, 256-bit Salsa20/20, 256-bit SNOW 2.0, 256-bit Sosemanuk, and 80-bit TRIVIUM.

0 Introduction

Suppose a user wants to encrypt data, in software, using one of the "phase 3 software" eSTREAM ciphers: CryptMT, Dragon, HC, LEX, NLS, Rabbit, Salsa20, or Sosemanuk. Which cipher will provide the best performance?

The answer depends—more than one might expect—on the user's CPU. This paper considers the following representative set of ten CPUs:

Architecture	Manufacturer	CPU	ID	MHz	Release date
amd64	Intel	Core 2 Quad Q6600	6fb	2394	2007.07
ppc64	IBM	Cell PPE		3192	2006.11
amd64	Intel	Pentium D 930	f64	3000	2006.01
amd64	AMD	Athlon 64 X2 3800+	15,75,2	2000	2005.08
x86	Intel	Pentium M LV 718	695	1300	2004.10
x86	Intel	Pentium 4 HT 530	f41	3000	2004.06
ppc64	IBM	PowerPC G5 970FX		2000	2004.01
sparcv9	Sun	UltraSPARC III Cu		1200	2003.08
x86	Intel	Pentium 4 1.9	f12	1900	2001.08
ppc32	Motorola	PowerPC G4 7410		533	2001.01

The rest of the paper is organized into ten sections, one section for each CPU.

The answer also depends heavily on how many bytes are generated in each keystream, and on how many keystreams are generated from each key. This paper reports cycle counts per encrypted byte for six different situations:

* Permanent ID of this document: 185342964abfcd1357a58e3caf9e61d9. Date of this document: 2008.03.31. This work was supported by the National Science Foundation under grant ITR–0716498.

- "long": Encrypt one long stream.
- "agility": Encrypt many parallel streams in 256-byte blocks.
- "1500": Set up a nonce and encrypt a 1500-byte packet.
- "576": Set up a nonce and encrypt a 576-byte packet.
- "40": Set up a nonce and encrypt a 40-byte packet.
- "40k": Set up a key, set up a nonce, and encrypt a 40-byte packet.

All of these numbers are collected by the eSTREAM benchmarking framework. The raw data and the framework versions that I used are available from my web page `http://cr.yp.to/streamciphers/timings.html`, along with raw data for many more ciphers and many more computers. The official eSTREAM position appears to be that long-stream performance is most important, so I have put it first.

I have included one of the "phase 3 hardware" eSTREAM ciphers, namely TRIVIUM, because it provides good software performance, often matching or exceeding the speeds of the "software phase 3" ciphers. I have also included all of the "benchmark" eSTREAM ciphers: 10-round AES-128, 14-round AES-256, RC4, and SNOW 2.0. Note, however, that RC4 has been broken, and that TRIVIUM has only an 80-bit key.

0.1 Should some ciphers be discarded?

There are several reasons that some users will limit their choices of ciphers.

A user who wants more than 128-bit security—let's say 192-bit security—will discard HC-128, LEX, NLS, and Rabbit. (In theory LEX has a 192-bit version, but no software was submitted to eSTREAM.) The remaining choices are CryptMT, Dragon, HC-256, Salsa20/8, Salsa20/12, Salsa20/20, and Sosemanuk.

A user who wants exactly 256-bit security will also discard Salsa20/8 (a known attack costs 2^{251}) and Sosemanuk (a known attack costs 2^{226}). See my paper [1] for a much more comprehensive discussion of known attacks against eSTREAM submissions. The remaining choices are CryptMT, Dragon, HC-256, Salsa20/12, Salsa20/20, and Sosemanuk.

A user who wants timing-attack protection will need new implementations of some ciphers. Presumably there are considerable slowdowns for the variable-index constant-table lookups in Dragon, LEX, NLS, and Sosemanuk, and larger slowdowns for the variable-index variable-table lookups in HC-128 and HC-256. These implementations have not been written, let alone benchmarked, so for the moment the only remaining choices are CryptMT, Rabbit, Salsa20/8, Salsa20/12, and Salsa20/20.

A user who wants a cipher that also fits into small hardware will discard CryptMT, Dragon, HC-128, and HC-256. The remaining choices are LEX, NLS, Rabbit, Salsa20/8, Salsa20/12, Salsa20/20, and Sosemanuk.

All of the "phase 3 software" ciphers are free for non-commercial use. A user who wants a cipher that is also free for commercial use will discard CryptMT and Rabbit (although CryptMT will be made free if it appears in the final eSTREAM portfolio). The remaining choices are Dragon, HC-128, HC-256, LEX, NLS, Salsa20/8, Salsa20/12, Salsa20/20, and Sosemanuk.

1 Intel Core 2 Quad Q6600 6fb, amd64 architecture

long	agility	1500	576	40	40k
Salsa20/8 251 **1.88**	Salsa20/8 251 **2.86**	Salsa20/8 251 **2.24**	Salsa20/8 251 **2.06**	Salsa20/8 251 **10.79**	Salsa20/8 251 **11.47**
HC-128 128 **2.34**	CryptMTv3 256 **2.95**	Rabbit 128 **2.80**	Salsa20/12 256 **2.80**	Salsa20/12 256 **12.67**	Salsa20/12 256 **13.35**
Rabbit 128 **2.34**	Salsa20/12 256 **3.53**	Salsa20/12 256 **3.01**	Rabbit 128 **3.04**	CryptMTv3 256 **13.93**	CryptMTv3 256 **14.75**
Salsa20/12 256 **2.54**	Rabbit 128 **3.66**	TRIVIUM **4.11**	Salsa20/20 256 **4.24**	LEX v2 128 **15.74**	Salsa20/20 256 **16.87**
CryptMTv3 256 **2.71**	TRIVIUM **4.75**	Salsa20/20 256 **4.55**	TRIVIUM **4.81**	Salsa20/20 256 **16.19**	LEX v2 128 **19.87**
Sosemanuk 226 **3.54**	Salsa20/20 256 **4.88**	NLS v2 128 **4.57**	SNOW 2.0 256 **5.19**	Rabbit 128 **17.68**	TRIVIUM **20.39**
HC-256 256 **3.66**	SNOW 2.0 256 **5.57**	SNOW 2.0 256 **4.65**	CryptMTv3 256 **5.21**	AES-128 128 **18.60**	SNOW 2.0 256 **24.06**
TRIVIUM **3.66**	NLS v2 128 **6.65**	Sosemanuk 226 **4.72**	NLS v2 128 **5.39**	TRIVIUM **19.57**	AES-128 128 **26.75**
Salsa20/20 256 **3.91**	Sosemanuk 226 **6.66**	CryptMTv3 256 **4.99**	Sosemanuk 226 **5.77**	SNOW 2.0 256 **22.44**	Rabbit 128 **27.81**
NLS v2 128 **4.11**	LEX v2 128 **7.26**	LEX v2 128 **6.24**	LEX v2 128 **6.95**	Sosemanuk 226 **23.99**	AES-256 256 **34.74**
SNOW 2.0 256 **4.16**	Dragon 256 **9.30**	RC4 **10.15**	AES-128 128 **12.79**	NLS v2 128 **24.19**	NLS v2 128 **37.16**
LEX v2 128 **5.83**	HC-128 128 **10.83**	AES-128 128 **12.72**	RC4 **13.74**	AES-256 256 **24.68**	Sosemanuk 226 **40.81**
Dragon 256 **7.33**	RC4 **13.91**	HC-128 128 **15.59**	AES-256 256 **17.95**	Dragon 256 **49.85**	Dragon 256 **52.23**
RC4 **7.47**	AES-128 128 **14.39**	AES-256 256 **17.88**	Dragon 256 **20.54**	RC4 **144.92**	RC4 **147.58**
AES-128 128 **12.59**	HC-256 256 **16.51**	Dragon 256 **18.80**	HC-128 128 **36.63**	HC-128 128 **498.93**	HC-128 128 **499.79**
AES-256 256 **17.75**	AES-256 256 **19.87**	HC-256 256 **34.18**	HC-256 256 **82.76**	HC-256 256 **1145.68**	HC-256 256 **1146.48**

These measurements were collected on a computer named `latour` in the Coding and Cryptography Computer Cluster at Technische Universiteit Eindhoven. This computer has a four-core 2394MHz Intel Core 2 Quad Q6600 6fb processor. Measurements used one core of the processor.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

2 IBM Cell PPE, ppc64 architecture

long	agility	1500	576	40	40k
Salsa20/8 251 **6.75**	Salsa20/8 251 **10.07**	Salsa20/8 251 **7.56**	Salsa20/8 251 **7.20**	Salsa20/8 251 **41.10**	Salsa20/8 251 **43.76**
Salsa20/12 256 **9.75**	Salsa20/12 256 **13.09**	Salsa20/12 256 **10.63**	Salsa20/12 256 **10.20**	LEX v2 128 **42.92**	Salsa20/12 256 **48.46**
TRIVIUM **9.81**	TRIVIUM **13.76**	TRIVIUM **11.17**	TRIVIUM **12.92**	Salsa20/12 256 **45.80**	LEX v2 128 **53.77**
HC-128 128 **11.02**	LEX v2 128 **17.72**	LEX v2 128 **14.50**	LEX v2 128 **16.36**	Salsa20/20 256 **54.41**	Salsa20/20 256 **58.56**
LEX v2 128 **12.59**	Salsa20/20 256 **19.26**	NLS v2 128 **16.97**	Salsa20/20 256 **16.46**	TRIVIUM **55.42**	TRIVIUM **62.02**
NLS v2 128 **15.18**	Dragon 256 **23.06**	Salsa20/20 256 **17.05**	NLS v2 128 **21.28**	AES-128 128 **70.90**	AES-128 128 **80.20**
Salsa20/20 256 **16.07**	Sosemanuk 226 **23.68**	SNOW 2.0 256 **25.07**	SNOW 2.0 256 **25.99**	NLS v2 128 **81.95**	AES-256 256 **108.68**
HC-256 256 **16.08**	NLS v2 128 **24.12**	Sosemanuk 226 **28.29**	Sosemanuk 226 **32.23**	AES-256 256 **83.97**	NLS v2 128 **124.20**
Dragon 256 **17.70**	SNOW 2.0 256 **26.23**	AES-128 128 **36.82**	AES-128 128 **36.92**	Sosemanuk 226 **85.63**	SNOW 2.0 256 **131.75**
Sosemanuk 226 **21.11**	HC-128 128 **38.61**	Rabbit 128 **37.42**	Rabbit 128 **39.84**	Rabbit 128 **112.04**	Rabbit 128 **169.43**
SNOW 2.0 256 **22.46**	Rabbit 128 **40.34**	HC-128 128 **53.77**	AES-256 256 **60.57**	SNOW 2.0 256 **124.29**	CryptMTv3 256 **180.81**
CryptMTv3 256 **26.79**	AES-128 128 **41.68**	RC4 **57.24**	CryptMTv3 256 **72.65**	CryptMTv3 256 **174.56**	Sosemanuk 226 **239.92**
Rabbit 128 **35.03**	HC-256 256 **60.94**	AES-256 256 **60.67**	RC4 **77.00**	Dragon 256 **266.21**	Dragon 256 **275.56**
AES-128 128 **35.83**	RC4 **60.98**	CryptMTv3 256 **61.79**	HC-128 128 **119.48**	RC4 **522.27**	RC4 **533.53**
RC4 **44.17**	CryptMTv3 256 **67.60**	HC-256 256 **140.97**	Dragon 256 **150.39**	HC-128 128 **1613.00**	HC-128 128 **1618.20**
AES-256 256 **60.18**	AES-256 256 **90.68**	Dragon 256 **143.85**	HC-256 256 **329.97**	HC-256 256 **4579.75**	HC-256 256 **4587.27**

These measurements were collected on a computer named `nmips3` in the NMI Build and Test Lab at the University of Wisconsin at Madison. This computer is a Sony Playstation 3 with a 3192MHz Sony–Toshiba–IBM Cell processor. Measurements used one thread on one core of the processor, specifically the "PPE." The "SPE" cores were not used.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

3 Intel Pentium D 930 f64, amd64 architecture

long	agility	1500	576	40	40k
HC-128 128 **3.88**	Sosemanuk 226 **7.26**	SNOW 2.0 256 **5.62**	Salsa20/8 251 **5.64**	LEX v2 128 **23.99**	LEX v2 128 **31.73**
SNOW 2.0 256 **4.85**	Salsa20/8 251 **7.34**	NLS v2 128 **6.07**	SNOW 2.0 256 **6.52**	AES-128 128 **26.28**	Salsa20/8 251 **33.03**
Salsa20/8 251 **4.91**	SNOW 2.0 256 **7.69**	Salsa20/8 251 **6.86**	NLS v2 128 **7.13**	NLS v2 128 **29.77**	TRIVIUM **34.00**
HC-256 256 **5.20**	TRIVIUM **8.29**	Sosemanuk 226 **6.86**	Salsa20/12 256 **7.67**	Salsa20/8 251 **30.38**	AES-128 128 **34.02**
Sosemanuk 226 **5.31**	Salsa20/12 256 **8.94**	TRIVIUM **7.07**	TRIVIUM **8.17**	Rabbit 128 **31.16**	SNOW 2.0 256 **37.44**
NLS v2 128 **5.59**	NLS v2 128 **9.89**	LEX v2 128 **8.28**	Sosemanuk 226 **8.38**	TRIVIUM **31.22**	Salsa20/12 256 **38.74**
CryptMTv3 256 **5.77**	LEX v2 128 **10.23**	Salsa20/12 256 **9.15**	LEX v2 128 **9.19**	Sosemanuk 226 **32.54**	CryptMTv3 256 **44.30**
TRIVIUM **6.28**	CryptMTv3 256 **12.40**	Rabbit 128 **10.90**	Rabbit 128 **11.70**	SNOW 2.0 256 **33.57**	NLS v2 128 **47.55**
Salsa20/12 256 **7.12**	Rabbit 128 **13.01**	CryptMTv3 256 **11.98**	Salsa20/20 256 **12.64**	Salsa20/12 256 **36.09**	Rabbit 128 **49.19**
LEX v2 128 **7.54**	Salsa20/20 256 **13.03**	Salsa20/20 256 **13.85**	CryptMTv3 256 **13.18**	AES-256 256 **38.76**	Salsa20/20 256 **49.96**
Dragon 256 **9.93**	Dragon 256 **14.01**	AES-128 128 **17.09**	AES-128 128 **17.33**	CryptMTv3 256 **41.75**	AES-256 256 **53.85**
Rabbit 128 **10.30**	RC4 **16.13**	HC-128 128 **24.77**	AES-256 256 **24.67**	Salsa20/20 256 **47.31**	Sosemanuk 226 **58.59**
Salsa20/20 256 **10.66**	HC-128 128 **17.17**	Dragon 256 **26.39**	Dragon 256 **28.40**	Dragon 256 **72.52**	Dragon 256 **77.59**
RC4 **11.98**	AES-128 128 **20.03**	AES-256 256 **26.49**	RC4 **52.06**	RC4 **587.04**	RC4 **590.81**
AES-128 128 **16.82**	HC-256 256 **24.31**	RC4 **27.35**	HC-128 128 **57.81**	HC-128 128 **833.20**	HC-128 128 **836.39**
AES-256 256 **24.39**	AES-256 256 **28.96**	HC-256 256 **60.67**	HC-256 256 **150.43**	HC-256 256 **2099.48**	HC-256 256 **2102.03**

These measurements were collected on a computer named `speed` at Technische Universiteit Eindhoven. This computer has a two-core 2992MHz Intel Pentium D 930 f64 processor. Measurements used one core of the processor.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

4 AMD Athlon 64 X2 3800+ 15,75,2, amd64 architecture

long	agility	1500	576	40	40k
Rabbit 128 **2.86**	Rabbit 128 **4.62**	Rabbit 128 **3.40**	Salsa20/8 251 **3.65**	Salsa20/8 251 **10.58**	Salsa20/8 251 **12.11**
HC-128 128 **2.87**	Salsa20/8 251 **4.79**	Salsa20/8 251 **3.67**	Rabbit 128 **3.73**	Salsa20/12 256 **12.79**	Salsa20/12 256 **14.32**
Salsa20/8 251 **3.47**	Sosemanuk 226 **5.35**	TRIVIUM **4.56**	Salsa20/12 256 **5.04**	LEX v2 128 **14.51**	Salsa20/20 256 **18.78**
Sosemanuk 226 **4.06**	TRIVIUM **5.42**	NLS v2 128 **4.65**	TRIVIUM **5.29**	Salsa20/20 256 **17.25**	LEX v2 128 **19.35**
TRIVIUM **4.08**	Salsa20/12 256 **6.18**	Salsa20/12 256 **5.09**	NLS v2 128 **5.58**	AES-128 128 **19.89**	CryptMTv3 256 **22.10**
NLS v2 128 **4.26**	SNOW 2.0 256 **6.65**	Sosemanuk 226 **5.26**	SNOW 2.0 256 **5.91**	CryptMTv3 256 **20.29**	TRIVIUM **22.97**
HC-256 256 **4.28**	LEX v2 128 **7.00**	SNOW 2.0 256 **5.40**	LEX v2 128 **6.29**	TRIVIUM **21.20**	SNOW 2.0 256 **27.17**
CryptMTv3 256 **4.63**	NLS v2 128 **7.23**	LEX v2 128 **5.63**	Sosemanuk 226 **6.34**	Rabbit 128 **21.31**	AES-128 128 **29.65**
SNOW 2.0 256 **4.86**	CryptMTv3 256 **8.64**	CryptMTv3 256 **7.77**	Salsa20/20 256 **7.84**	NLS v2 128 **23.24**	Rabbit 128 **33.96**
Salsa20/12 256 **4.86**	Salsa20/20 256 **8.97**	Salsa20/20 256 **7.94**	CryptMTv3 256 **8.40**	Sosemanuk 226 **24.05**	NLS v2 128 **35.02**
LEX v2 128 **5.25**	Dragon 256 **10.02**	AES-128 128 **13.45**	AES-128 128 **13.58**	SNOW 2.0 256 **24.49**	AES-256 256 **38.43**
Salsa20/20 256 **7.64**	HC-128 128 **10.81**	HC-128 128 **18.55**	AES-256 256 **18.77**	AES-256 256 **26.19**	Sosemanuk 226 **41.91**
Dragon 256 **7.76**	AES-128 128 **16.22**	AES-256 256 **18.65**	Dragon 256 **26.08**	Dragon 256 **61.40**	Dragon 256 **64.48**
AES-128 128 **13.32**	HC-256 256 **16.43**	RC4 **23.59**	RC4 **38.23**	RC4 **357.69**	RC4 **360.56**
RC4 **14.45**	RC4 **21.47**	Dragon 256 **24.45**	HC-128 128 **43.44**	HC-128 128 **590.50**	HC-128 128 **592.51**
AES-256 256 **18.52**	AES-256 256 **23.11**	HC-256 256 **64.17**	HC-256 256 **159.78**	HC-256 256 **2247.60**	HC-256 256 **2250.18**

These measurements were collected on a computer named `mace` in the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago. This computer has a two-core 2000MHz AMD Athlon 64 X2 3800+ 15,75,2 processor. Measurements used one core of the processor.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

5 Intel Pentium M LV 718 695, x86 architecture

long	agility	1500	576	40	40k
HC-128 128 **3.49**	Rabbit 128 **5.35**	Rabbit 128 **4.47**	Rabbit 128 **4.90**	Salsa20/8 251 **19.09**	Salsa20/8 251 **20.96**
Rabbit 128 **3.94**	SNOW 2.0 256 **6.16**	SNOW 2.0 256 **5.39**	Salsa20/8 251 **5.54**	LEX v1 128 **20.45**	Salsa20/12 256 **24.63**
SNOW 2.0 256 **4.72**	Salsa20/8 251 **6.34**	NLS v2 128 **5.62**	SNOW 2.0 256 **6.12**	Salsa20/12 256 **22.88**	CryptMTv3 256 **25.51**
CryptMTv3 256 **4.77**	TRIVIUM **6.56**	Salsa20/8 251 **5.63**	NLS v2 128 **6.82**	CryptMTv3 256 **23.37**	AES-128 128 **28.60**
HC-256 256 **4.99**	Sosemanuk 226 **6.61**	TRIVIUM **6.16**	TRIVIUM **7.12**	Rabbit 128 **23.45**	TRIVIUM **31.03**
NLS v2 128 **5.13**	CryptMTv3 256 **7.98**	Salsa20/12 256 **7.86**	Salsa20/12 256 **7.71**	AES-128 128 **23.69**	LEX v1 128 **31.44**
Salsa20/8 251 **5.30**	Salsa20/12 256 **8.48**	Sosemanuk 226 **8.56**	CryptMTv3 256 **8.66**	NLS v2 128 **28.29**	Salsa20/20 256 **31.87**
TRIVIUM **5.52**	NLS v2 128 **8.58**	CryptMTv3 256 **8.71**	Sosemanuk 226 **10.01**	TRIVIUM **29.03**	SNOW 2.0 256 **32.57**
Sosemanuk 226 **5.60**	LEX v1 128 **11.89**	LEX v1 128 **10.02**	LEX v1 128 **10.84**	SNOW 2.0 256 **29.71**	Rabbit 128 **37.45**
Salsa20/12 256 **7.44**	Salsa20/20 256 **12.74**	Salsa20/20 256 **12.26**	Salsa20/20 256 **11.97**	Salsa20/20 256 **30.14**	NLS v2 128 **43.42**
LEX v1 128 **9.51**	HC-128 128 **15.46**	AES-128 128 **16.17**	AES-128 128 **16.30**	Sosemanuk 226 **34.28**	AES-256 256 **50.79**
Salsa20/20 256 **11.70**	Dragon 256 **15.58**	RC4 **21.84**	AES-256 256 **25.30**	AES-256 256 **35.19**	Sosemanuk 226 **63.18**
RC4 **12.65**	RC4 **15.81**	HC-128 128 **23.84**	Dragon 256 **32.40**	Dragon 256 **83.41**	Dragon 256 **88.23**
Dragon 256 **13.38**	AES-128 128 **18.04**	AES-256 256 **25.16**	RC4 **36.40**	RC4 **356.42**	RC4 **359.64**
AES-128 128 **15.96**	HC-256 256 **22.50**	Dragon 256 **29.99**	HC-128 128 **56.27**	HC-128 128 **767.88**	HC-128 128 **770.03**
AES-256 256 **24.98**	AES-256 256 **28.79**	HC-256 256 **50.96**	HC-256 256 **124.39**	HC-256 256 **1727.68**	HC-256 256 **1729.22**

These measurements were collected on a computer named `whisper` owned by me. This computer has a one-core 1300MHz Intel Pentium M LV 718 695 processor.

These measurements used `estreambench-20080209`. This `estreambench` version predates the first LEX v2 implementation, so LEX v1 is listed instead of LEX v2.

6 Intel Pentium 4 HT 530 f41, x86 architecture

long	agility	1500	576	40	40k
HC-128 128 **4.53**	Sosemanuk 226 **7.76**	SNOW 2.0 256 **6.19**	Salsa20/8 251 **6.95**	LEX v2 128 **24.53**	LEX v2 128 **32.87**
SNOW 2.0 256 **5.19**	SNOW 2.0 256 **7.89**	NLS v2 128 **6.66**	SNOW 2.0 256 **7.29**	Rabbit 128 **26.78**	Salsa20/8 251 **34.80**
CryptMTv3 256 **5.57**	Salsa20/8 251 **8.24**	Salsa20/8 251 **7.42**	NLS v2 128 **8.90**	AES-128 128 **29.92**	AES-128 128 **37.73**
NLS v2 128 **5.64**	Salsa20/12 256 **10.30**	Rabbit 128 **8.50**	Salsa20/12 256 **8.98**	Salsa20/8 251 **31.88**	Salsa20/12 256 **40.31**
Sosemanuk 226 **5.72**	Rabbit 128 **10.44**	Sosemanuk 226 **9.39**	Rabbit 128 **9.12**	Salsa20/12 256 **37.39**	Rabbit 128 **41.30**
Salsa20/8 251 **5.79**	TRIVIUM **11.10**	TRIVIUM **10.11**	Sosemanuk 226 **11.16**	Sosemanuk 226 **38.54**	CryptMTv3 256 **45.81**
HC-256 256 **6.26**	CryptMTv3 256 **12.45**	Salsa20/12 256 **10.12**	TRIVIUM **11.81**	CryptMTv3 256 **42.61**	SNOW 2.0 256 **48.44**
Salsa20/12 256 **7.76**	NLS v2 128 **12.87**	LEX v2 128 **11.18**	LEX v2 128 **12.28**	SNOW 2.0 256 **42.91**	Salsa20/20 256 **50.93**
Rabbit 128 **8.02**	LEX v2 128 **13.23**	CryptMTv3 256 **12.83**	CryptMTv3 256 **13.09**	AES-256 256 **43.07**	TRIVIUM **51.21**
TRIVIUM **9.03**	Salsa20/20 256 **14.05**	Salsa20/20 256 **14.78**	Salsa20/20 256 **13.32**	Salsa20/20 256 **47.94**	AES-256 256 **58.74**
LEX v2 128 **10.49**	HC-128 128 **17.44**	AES-128 128 **19.17**	AES-128 128 **19.52**	TRIVIUM **48.14**	NLS v2 128 **87.26**
Salsa20/20 256 **11.77**	Dragon 256 **18.17**	AES-256 256 **28.21**	AES-256 256 **28.64**	NLS v2 128 **53.00**	Sosemanuk 226 **91.29**
Dragon 256 **13.41**	RC4 **20.23**	HC-128 128 **28.50**	Dragon 256 **34.68**	Dragon 256 **95.21**	Dragon 256 **100.35**
RC4 **16.44**	AES-128 128 **22.02**	Dragon 256 **30.95**	RC4 **55.96**	RC4 **585.16**	RC4 **589.22**
AES-128 128 **18.81**	HC-256 256 **24.41**	RC4 **31.64**	HC-128 128 **67.54**	HC-128 128 **887.98**	HC-128 128 **891.06**
AES-256 256 **28.05**	AES-256 256 **32.46**	HC-256 256 **68.64**	HC-256 256 **168.08**	HC-256 256 **2345.04**	HC-256 256 **2348.07**

These measurements were collected on a computer named `svlin002` at Technische Universiteit Eindhoven. This computer has a one-core 2992MHz Intel Pentium 4 HT 530 f41 processor.

These measurements used `estreambench-20080326`.

7 IBM PowerPC G5 970FX, ppc64 architecture

long	agility	1500	576	40	40k
Salsa20/8 251 **3.24**	Salsa20/8 251 **5.80**	Salsa20/8 251 **3.45**	Salsa20/8 251 **3.33**	Salsa20/8 251 **11.18**	Salsa20/8 251 **11.84**
HC-128 128 **4.22**	Salsa20/12 256 **7.32**	Salsa20/12 256 **4.98**	Salsa20/12 256 **4.83**	Salsa20/12 256 **13.53**	Salsa20/12 256 **14.32**
Salsa20/12 256 **4.74**	TRIVIUM **7.62**	TRIVIUM **5.53**	TRIVIUM **6.32**	LEX v2 128 **17.95**	Salsa20/20 256 **18.97**
TRIVIUM **5.02**	Sosemanuk 226 **9.12**	NLS v2 128 **6.40**	NLS v2 128 **7.35**	Salsa20/20 256 **18.16**	TRIVIUM **26.09**
NLS v2 128 **5.93**	SNOW 2.0 256 **9.76**	SNOW 2.0 256 **7.40**	Salsa20/20 256 **7.89**	TRIVIUM **23.71**	SNOW 2.0 256 **30.91**
HC-256 256 **6.06**	NLS v2 128 **10.14**	LEX v2 128 **7.95**	SNOW 2.0 256 **8.00**	NLS v2 128 **24.43**	CryptMTv3 256 **32.39**
SNOW 2.0 256 **6.68**	Salsa20/20 256 **10.33**	Salsa20/20 256 **8.14**	LEX v2 128 **8.78**	AES-128 128 **27.96**	AES-128 128 **34.05**
Sosemanuk 226 **6.99**	LEX v2 128 **10.49**	Sosemanuk 226 **8.97**	Sosemanuk 226 **10.61**	Rabbit 128 **28.68**	NLS v2 128 **38.06**
LEX v2 128 **7.28**	Dragon 256 **12.43**	Rabbit 128 **10.89**	Rabbit 128 **11.52**	SNOW 2.0 256 **28.97**	Rabbit 128 **43.50**
Salsa20/20 256 **7.81**	Rabbit 128 **13.36**	CryptMTv3 256 **12.79**	CryptMTv3 256 **14.09**	CryptMTv3 256 **30.82**	AES-256 256 **48.24**
CryptMTv3 256 **8.18**	CryptMTv3 256 **14.06**	RC4 **17.33**	AES-128 128 **18.67**	Sosemanuk 226 **36.61**	LEX v2 128 **64.98**
Dragon 256 **8.39**	RC4 **14.21**	AES-128 128 **18.59**	RC4 **30.02**	AES-256 256 **38.85**	Dragon 256 **75.87**
RC4 **9.44**	HC-128 128 **19.25**	HC-128 128 **23.80**	AES-256 256 **31.14**	Dragon 256 **71.97**	Sosemanuk 226 **94.55**
Rabbit 128 **10.42**	AES-128 128 **22.22**	AES-256 256 **31.00**	Dragon 256 **35.72**	RC4 **306.25**	RC4 **310.67**
AES-128 128 **18.50**	HC-256 256 **28.65**	Dragon 256 **34.27**	HC-128 128 **55.20**	HC-128 128 **739.03**	HC-128 128 **740.58**
AES-256 256 **30.69**	AES-256 256 **36.30**	HC-256 256 **58.48**	HC-256 256 **141.02**	HC-256 256 **1955.50**	HC-256 256 **1957.12**

These measurements were collected on a computer named `geespaz` in the NMI Build and Test Lab at the University of Wisconsin at Madison. This computer has two 2000MHz IBM PowerPC G5 970FX processors. Measurements used one processor.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

8 Sun UltraSPARC III Cu, sparcv9 architecture

long	agility	1500	576	40	40k
TRIVIUM **5.96**	Salsa20/8 251 **7.54**	TRIVIUM **6.57**	Salsa20/8 251 **6.76**	LEX v2 128 **22.11**	Salsa20/8 251 **26.06**
HC-128 128 **6.03**	TRIVIUM **7.67**	NLS v2 128 **6.84**	TRIVIUM **7.50**	Salsa20/8 251 **24.56**	LEX v2 128 **28.13**
NLS v2 128 **6.52**	LEX v2 128 **9.51**	Salsa20/8 251 **6.97**	NLS v2 128 **8.54**	Salsa20/12 256 **28.66**	Salsa20/12 256 **30.14**
Salsa20/8 251 **6.64**	Sosemanuk 226 **9.89**	LEX v2 128 **7.77**	LEX v2 128 **8.79**	TRIVIUM **28.94**	TRIVIUM **33.52**
LEX v2 128 **7.21**	Salsa20/12 256 **10.21**	Salsa20/12 256 **9.66**	Salsa20/12 256 **9.32**	Salsa20/20 256 **32.94**	Salsa20/20 256 **34.54**
HC-256 256 **7.85**	SNOW 2.0 256 **10.99**	SNOW 2.0 256 **9.91**	SNOW 2.0 256 **10.53**	Rabbit 128 **34.80**	SNOW 2.0 256 **46.99**
Sosemanuk 226 **8.47**	Dragon 256 **12.27**	Sosemanuk 226 **11.94**	Sosemanuk 226 **13.46**	NLS v2 128 **41.98**	Rabbit 128 **51.95**
SNOW 2.0 256 **8.80**	NLS v2 128 **12.68**	Rabbit 128 **13.14**	Rabbit 128 **13.95**	Sosemanuk 226 **42.87**	AES-128 128 **54.67**
Dragon 256 **8.82**	Rabbit 128 **15.09**	Salsa20/20 256 **14.85**	Salsa20/20 256 **14.46**	SNOW 2.0 256 **42.89**	NLS v2 128 **62.66**
Salsa20/12 256 **9.21**	Salsa20/20 256 **15.24**	CryptMTv3 256 **24.40**	CryptMTv3 256 **26.70**	AES-128 128 **49.10**	CryptMTv3 256 **70.93**
Rabbit 128 **12.21**	RC4 **19.50**	RC4 **27.21**	AES-128 128 **29.86**	CryptMTv3 256 **66.40**	Sosemanuk 226 **82.63**
CryptMTv3 256 **13.38**	CryptMTv3 256 **25.31**	AES-128 128 **29.74**	Dragon 256 **45.93**	AES-256 256 **82.91**	AES-256 256 **99.18**
Salsa20/20 256 **14.34**	AES-128 128 **32.43**	HC-128 128 **35.59**	RC4 **46.80**	Dragon 256 **96.36**	Dragon 256 **103.73**
RC4 **15.10**	HC-128 128 **36.95**	Dragon 256 **43.99**	AES-256 256 **64.93**	RC4 **472.63**	RC4 **477.03**
AES-128 128 **29.45**	HC-256 256 **58.42**	AES-256 256 **64.91**	HC-128 128 **82.58**	HC-128 128 **1115.14**	HC-128 128 **1117.68**
AES-256 256 **64.60**	AES-256 256 **69.66**	HC-256 256 **80.54**	HC-256 256 **195.89**	HC-256 256 **2726.91**	HC-256 256 **2729.73**

These measurements were collected on a computer named `nmisolaris10` in the NMI Build and Test Lab at the University of Wisconsin at Madison. This computer has two 1200MHz Sun UltraSPARC III Cu processors. Measurements used one processor.

These measurements used `estreambench-20080326`. The LEX v2 measurements reflect recent speedups from Peter Schwabe.

9 Intel Pentium 4 1.9 f12, x86 architecture

long	agility	1500	576	40	40k
HC-128 128 **4.03**	Salsa20/8 251 **7.18**	SNOW 2.0 256 **6.09**	Salsa20/8 251 **5.99**	Salsa20/8 251 **21.83**	Salsa20/8 251 **24.18**
SNOW 2.0 256 **5.18**	SNOW 2.0 256 **8.13**	Salsa20/8 251 **6.38**	SNOW 2.0 256 **7.22**	LEX v2 128 **22.67**	Salsa20/12 256 **29.42**
HC-256 256 **5.33**	Salsa20/12 256 **9.31**	NLS v2 128 **7.18**	Salsa20/12 256 **8.21**	AES-128 128 **27.01**	LEX v2 128 **35.96**
CryptMTv3 256 **5.37**	Rabbit 128 **9.79**	Rabbit 128 **8.44**	Rabbit 128 **9.39**	Salsa20/12 256 **27.05**	AES-128 128 **37.23**
Salsa20/8 251 **5.40**	TRIVIUM **10.21**	Salsa20/12 256 **8.83**	NLS v2 128 **9.79**	Salsa20/20 256 **37.49**	Salsa20/20 256 **39.87**
NLS v2 128 **6.02**	Sosemanuk 226 **10.72**	TRIVIUM **9.30**	TRIVIUM **10.84**	SNOW 2.0 256 **38.14**	SNOW 2.0 256 **42.74**
Salsa20/12 256 **7.51**	CryptMTv3 256 **12.88**	LEX v2 128 **10.59**	LEX v2 128 **11.68**	AES-256 256 **39.20**	CryptMTv3 256 **45.33**
Rabbit 128 **7.54**	LEX v2 128 **13.47**	CryptMTv3 256 **12.16**	CryptMTv3 256 **12.09**	Rabbit 128 **39.41**	TRIVIUM **47.40**
TRIVIUM **8.29**	NLS v2 128 **13.52**	Salsa20/20 256 **13.82**	Salsa20/20 256 **12.67**	CryptMTv3 256 **41.75**	Rabbit 128 **66.37**
Sosemanuk 226 **9.74**	Salsa20/20 256 **13.66**	Sosemanuk 226 **14.45**	Sosemanuk 226 **16.90**	TRIVIUM **44.54**	AES-256 256 **72.03**
LEX v2 128 **9.91**	Dragon 256 **17.61**	AES-128 128 **17.19**	AES-128 128 **17.58**	Sosemanuk 226 **57.27**	Dragon 256 **93.11**
Salsa20/20 256 **11.74**	RC4 **18.91**	RC4 **26.02**	AES-256 256 **29.50**	NLS v2 128 **61.95**	NLS v2 128 **96.21**
Dragon 256 **12.57**	HC-128 128 **19.28**	AES-256 256 **28.24**	Dragon 256 **31.22**	Dragon 256 **84.89**	Sosemanuk 226 **127.73**
RC4 **14.20**	AES-128 128 **20.20**	Dragon 256 **29.21**	RC4 **45.22**	RC4 **451.46**	RC4 **458.36**
AES-128 128 **16.98**	HC-256 256 **26.57**	HC-128 128 **45.25**	HC-128 128 **110.25**	HC-128 128 **1570.07**	HC-128 128 **1572.65**
AES-256 256 **28.41**	AES-256 256 **33.28**	HC-256 256 **64.34**	HC-256 256 **158.26**	HC-256 256 **2215.76**	HC-256 256 **2218.11**

These measurements were collected on a computer named `fireball` in the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago. This computer has one 1900MHz Intel Pentium 4 1.9 f12 processor.

These measurements used `estreambench-20080326`.

10 Motorola PowerPC G4 7410, ppc32 architecture

long	agility	1500	576	40	40k
Salsa20/8 251 **1.99**	Salsa20/8 251 **2.64**	Salsa20/8 251 **2.17**	Salsa20/8 251 **2.14**	Salsa20/8 251 **9.68**	Salsa20/8 251 **11.42**
Salsa20/12 256 **2.74**	Salsa20/12 256 **3.40**	Salsa20/12 256 **2.94**	Salsa20/12 256 **2.88**	Salsa20/12 256 **10.88**	Salsa20/12 256 **12.62**
Salsa20/20 256 **4.24**	Salsa20/20 256 **4.90**	Salsa20/20 256 **4.48**	Salsa20/20 256 **4.38**	Salsa20/20 256 **13.29**	Salsa20/20 256 **15.03**
HC-128 128 **4.80**	Sosemanuk 226 **7.10**	NLS v2 128 **6.82**	SNOW 2.0 256 **8.40**	LEX v2 128 **22.80**	LEX v2 128 **27.29**
HC-256 256 **6.17**	SNOW 2.0 256 **8.24**	SNOW 2.0 256 **7.74**	NLS v2 128 **8.73**	AES-128 128 **28.21**	AES-128 128 **33.33**
Sosemanuk 226 **6.17**	LEX v2 128 **9.27**	LEX v2 128 **8.19**	LEX v2 128 **9.17**	SNOW 2.0 256 **31.82**	SNOW 2.0 256 **34.52**
NLS v2 128 **6.22**	Dragon 256 **10.03**	Sosemanuk 226 **9.17**	Sosemanuk 226 **10.61**	Sosemanuk 226 **32.37**	CryptMTv3 256 **40.84**
SNOW 2.0 256 **7.06**	NLS v2 128 **11.16**	TRIVIUM **13.21**	Rabbit 128 **15.16**	Rabbit 128 **36.15**	AES-256 256 **52.24**
LEX v2 128 **7.62**	TRIVIUM **13.06**	Rabbit 128 **14.39**	TRIVIUM **15.16**	CryptMTv3 256 **38.70**	Rabbit 128 **52.75**
Dragon 256 **8.39**	RC4 **13.95**	CryptMTv3 256 **15.10**	CryptMTv3 256 **17.00**	AES-256 256 **44.62**	TRIVIUM **62.67**
CryptMTv3 256 **8.92**	Rabbit 128 **14.83**	RC4 **17.42**	AES-128 128 **18.52**	NLS v2 128 **46.05**	NLS v2 128 **69.29**
RC4 **11.16**	CryptMTv3 256 **15.98**	AES-128 128 **17.88**	RC4 **27.34**	TRIVIUM **59.77**	Dragon 256 **70.27**
TRIVIUM **11.91**	HC-128 128 **16.43**	HC-128 128 **25.40**	Dragon 256 **28.86**	Dragon 256 **66.90**	Sosemanuk 226 **77.50**
Rabbit 128 **13.89**	AES-128 128 **20.57**	Dragon 256 **27.14**	AES-256 256 **34.97**	RC4 **245.45**	RC4 **248.77**
AES-128 128 **17.75**	HC-256 256 **26.79**	AES-256 256 **34.98**	HC-128 128 **58.21**	HC-128 128 **779.70**	HC-128 128 **781.49**
AES-256 256 **34.80**	AES-256 256 **37.62**	HC-256 256 **54.08**	HC-256 256 **130.33**	HC-256 256 **1798.00**	HC-256 256 **1800.19**

These measurements were collected on a computer named `gggg` in the Center for Research and Instruction in Technologies for Electronic Security (RITES) at the University of Illinois at Chicago. This computer has two 533MHz Motorola PowerPC G4 7410 processors. Measurements used one processor.

These measurements used `estreambench-20080326`. The LEX v2 and AES-128 measurements reflect recent speedups from Peter Schwabe.

References

1. Daniel J. Bernstein, *Which eSTREAM ciphers have been broken?*, eSTREAM report 2008/010 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §0.1.