

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: 185342964abfcfd1357a58e3caf9e61d9. 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	Salsa20/8 1.88 251	Salsa20/8 2.86 251	Salsa20/8 2.24 251	Salsa20/8 2.06 251	Salsa20/8 10.79 251	Salsa20/8 11.47
HC-128 128	CryptMTv3 256	Rabbit 2.95 128	Rabbit 2.80 256	Salsa20/12 256	Salsa20/12 12.67 256	Salsa20/12 13.35
Rabbit 128	Salsa20/12 256	Salsa20/12 3.53 256	Salsa20/12 3.01 128	Rabbit 3.04 256	CryptMTv3 13.93 256	CryptMTv3 14.75
Salsa20/12 256	Rabbit 2.54 128	TRIVIUM 3.66	TRIVIUM 4.11	Salsa20/20 256	LEX v2 4.24 128	Salsa20/20 15.74 256
CryptMTv3 256	TRIVIUM 2.71	TRIVIUM 4.75	TRIVIUM 4.55	Salsa20/20 256	Salsa20/20 16.19 128	LEX v2 19.87
Sosemanuk 226	Salsa20/20 256	NLS v2 4.88 128	NLS v2 4.57	SNOW 2.0 256	Rabbit 5.19 128	TRIVIUM 17.68 20.39
HC-256 256	SNOW 2.0 256	SNOW 2.0 5.57	SNOW 2.0 4.65	CryptMTv3 256	AES-128 5.21 128	SNOW 2.0 18.60 256
TRIVIUM 3.66	NLS v2 128	Sosemanuk 6.65 226	NLS v2 4.72 128	TRIVIUM 5.39	TRIVIUM 19.57 128	AES-128 26.75
Salsa20/20 256	Sosemanuk 226	CryptMTv3 256	Sosemanuk 4.99 226	SNOW 2.0 256	Rabbit 5.77 128	SNOW 2.0 22.44 128
NLS v2 128	LEX v2 128	LEX v2 7.26 128	LEX v2 6.24 128	NLS v2 226	Sosemanuk 6.95 226	AES-256 23.99 256
SNOW 2.0 256	Dragon 256	RC4 9.30	RC4 10.15	AES-128 128	NLS v2 12.79 128	NLS v2 24.19 128
LEX v2 128	HC-128 128	AES-128 10.83 128	AES-128 12.72	RC4 13.74	AES-256 256	Sosemanuk 24.68 226
Dragon 256	RC4 7.33	HC-128 13.91 128	HC-128 15.59 256	AES-256 256	Dragon 17.95 256	Dragon 49.85 256
RC4 7.47	AES-128 128	AES-256 14.39	AES-256 17.88	Dragon 256	RC4 20.54	RC4 144.92
AES-128 128	HC-256 256	Dragon 256	HC-128 18.80 128	HC-128 36.63 128	HC-128 498.93 128	HC-128 499.79
AES-256 256	AES-256 256	HC-256 256	HC-256 34.18 256	HC-256 82.76 256	HC-256 1145.68 256	HC-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
Salsa20/12 256	9.75	Salsa20/12 256	13.09	Salsa20/12 256	10.63	Salsa20/12 256
TRIVIUM 9.81		TRIVIUM 13.76		TRIVIUM 11.17		TRIVIUM 12.92
HC-128 128	11.02	LEX v2 128	17.72	LEX v2 128	14.50	LEX v2 128
LEX v2 128	12.59	Salsa20/20 256	19.26	NLS v2 128	16.97	Salsa20/20 256
NLS v2 128	15.18	Dragon	Salsa20/20 256	17.05	NLS v2 128	AES-128 128
Salsa20/20 256	16.07	Sosemanuk 226	23.68	SNOW 2.0 256	25.07	SNOW 2.0 256
HC-256 256	16.08	NLS v2 128	24.12	Sosemanuk 226	28.29	Sosemanuk 226
Dragon 256	17.70	SNOW 2.0 256	26.23	AES-128 128	36.82	AES-128 128
Sosemanuk 226	21.11	HC-128 128	Rabbit 128	Rabbit 128	37.42	Rabbit 128
SNOW 2.0 256	22.46	Rabbit 128	HC-128 128	AES-128 128	53.77	SNOW 2.0 256
CryptMTv3 256	26.79	AES-128 128	RC4 256	CryptMTv3 256	57.24	CryptMTv3 256
Rabbit 128	35.03	HC-256 256	AES-256 256	RC4 256	60.94	RC4 256
AES-128 128	35.83	RC4 256	CryptMTv3 256	HC-128 128	60.98	RC4 256
RC4 44.17		CryptMTv3 256	HC-256 256	Dragon 256	61.79	RC4 256
AES-256 256	60.18	AES-256 256	Dragon 256	HC-256 256	140.97	HC-128 128
					150.39	1613.00
					329.97	1618.20
					4579.75	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 <small>226</small>	Sosemanuk 7.26 <small>256</small>	SNOW 2.0 5.62 <small>251</small>	Salsa20/8 5.64 <small>251</small>	LEX v2 23.99 <small>128</small>	LEX v2 31.73 <small>128</small>
SNOW 2.0 256	4.85 <small>251</small>	Salsa20/8 7.34 <small>128</small>	NLS v2 6.07 <small>256</small>	SNOW 2.0 6.52 <small>128</small>	AES-128 26.28 <small>251</small>	Salsa20/8 33.03 <small>251</small>
Salsa20/8 251	4.91 <small>256</small>	SNOW 2.0 7.69 <small>251</small>	Salsa20/8 6.86 <small>128</small>	NLS v2 7.13 <small>128</small>	NLS v2 29.77 <small>128</small>	TRIVIUM 34.00 <small>128</small>
HC-256 256	5.20 <small>226</small>	TRIVIUM 8.29 <small>226</small>	Sosemanuk 6.86 <small>256</small>	Salsa20/12 7.67 <small>251</small>	Salsa20/8 30.38 <small>128</small>	AES-128 34.02 <small>256</small>
Sosemanuk 226	5.31 <small>256</small>	Salsa20/12 8.94 <small>128</small>	TRIVIUM 7.07 <small>128</small>	TRIVIUM 8.17 <small>128</small>	Rabbit 31.16 <small>256</small>	SNOW 2.0 37.44 <small>256</small>
NLS v2 128	5.59 <small>128</small>	NLS v2 9.89 <small>128</small>	LEX v2 8.28 <small>226</small>	Sosemanuk 8.38 <small>256</small>	TRIVIUM 31.22 <small>256</small>	Salsa20/12 38.74 <small>256</small>
CryptMTv3 256	5.77 <small>128</small>	LEX v2 10.23 <small>256</small>	Salsa20/12 9.15 <small>128</small>	LEX v2 9.19 <small>226</small>	Sosemanuk 32.54 <small>256</small>	CryptMTv3 44.30 <small>256</small>
TRIVIUM 6.28	CryptMTv3 12.40 <small>256</small>	Rabbit 10.90 <small>128</small>	Rabbit 11.70 <small>128</small>	SNOW 2.0 33.57 <small>256</small>	NLS v2 47.55 <small>128</small>	
Salsa20/12 256	7.12 <small>128</small>	Rabbit 13.01 <small>256</small>	CryptMTv3 11.98 <small>256</small>	Salsa20/20 12.64 <small>256</small>	Salsa20/12 36.09 <small>128</small>	Rabbit 49.19 <small>128</small>
LEX v2 128	Salsa20/20 13.03 <small>256</small>	Salsa20/20 13.85 <small>256</small>	CryptMTv3 13.18 <small>256</small>	AES-256 38.76 <small>256</small>	Salsa20/20 49.96 <small>256</small>	
Dragon 256	9.93 <small>256</small>	Dragon 14.01 <small>128</small>	AES-128 17.09 <small>128</small>	AES-128 17.33 <small>256</small>	CryptMTv3 41.75 <small>256</small>	AES-256 53.85 <small>256</small>
Rabbit 128	RC4 10.30	HC-128 16.13 <small>128</small>	AES-256 24.77 <small>256</small>	AES-256 24.67 <small>256</small>	Salsa20/20 47.31 <small>226</small>	Sosemanuk 58.59 <small>226</small>
Salsa20/20 256	10.66 <small>128</small>	HC-128 17.17 <small>256</small>	Dragon 26.39 <small>256</small>	Dragon 28.40 <small>256</small>	Dragon 72.52 <small>256</small>	Dragon 77.59 <small>256</small>
RC4 11.98	AES-128 20.03 <small>128</small>	AES-256 26.49 <small>256</small>	RC4 52.06 <small>128</small>	RC4 587.04 <small>128</small>	RC4 590.81 <small>128</small>	
AES-128 128	16.82 <small>256</small>	HC-256 24.31 <small>256</small>	RC4 27.35 <small>128</small>	HC-128 57.81 <small>128</small>	HC-128 833.20 <small>128</small>	HC-128 836.39 <small>128</small>
AES-256 256	24.39 <small>256</small>	AES-256 28.96 <small>256</small>	HC-256 60.67 <small>256</small>	HC-256 150.43 <small>256</small>	HC-256 2099.48 <small>256</small>	HC-256 2102.03 <small>256</small>

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 256 4.56	Salsa20/12 256 5.04	LEX v2 128 14.51	Salsa20/20 256 18.78
Sosemanuk 226 4.06	TRIVIUM 226 5.42	NLS v2 128 4.65	TRIVIUM 256 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 256 22.97
HC-256 256 4.28	LEX v2 128 7.00	SNOW 2.0 256 5.40	LEX v2 128 6.29	TRIVIUM 256 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 256 23.59	RC4 128 38.23	RC4 128 357.69	RC4 128 360.56
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	Rabbit 3.49 ₁₂₈	Rabbit 5.35 ₁₂₈	Rabbit 4.47 ₁₂₈	Rabbit 4.90 ₂₅₁	Salsa20/8 19.09 ₂₅₁	Salsa20/8 20.96
Rabbit 128	SNOW 2.0 3.94 ₂₅₆	SNOW 2.0 6.16 ₂₅₆	SNOW 2.0 5.39 ₂₅₁	Salsa20/8 5.54 ₂₅₁	LEX v1 20.45 ₁₂₈	Salsa20/12 24.63 ₂₅₆
SNOW 2.0 256	Salsa20/8 4.72 ₂₅₁	NLS v2 6.34 ₁₂₈	NLS v2 5.62 ₂₅₆	SNOW 2.0 6.12 ₂₅₆	Salsa20/12 22.88 ₂₅₆	CryptMTv3 25.51 ₂₅₆
CryptMTv3 256	TRIVIUM 4.77	Salsa20/8 6.56 ₂₅₁	Salsa20/8 5.63 ₁₂₈	NLS v2 6.82 ₂₅₆	CryptMTv3 23.37 ₁₂₈	AES-128 28.60
HC-256 256	Sosemanuk 4.99 ₂₂₆	TRIVIUM 6.61	TRIVIUM 6.16	TRIVIUM 7.12 ₁₂₈	Rabbit 23.45 ₁₂₈	TRIVIUM 31.03
NLS v2 128	CryptMTv3 5.13 ₂₅₆	Salsa20/12 7.98 ₂₅₆	Salsa20/12 7.86 ₂₅₆	Salsa20/12 7.71 ₁₂₈	AES-128 23.69 ₁₂₈	LEX v1 31.44
Salsa20/8 251	Salsa20/12 5.30 ₂₅₆	Sosemanuk 8.48 ₂₂₆	Sosemanuk 8.56 ₂₅₆	CryptMTv3 8.66 ₁₂₈	NLS v2 28.29 ₂₅₆	Salsa20/20 31.87
TRIVIUM 5.52	NLS v2 8.58 ₁₂₈	CryptMTv3 8.71 ₂₅₆	Sosemanuk 10.01 ₂₂₆	TRIVIUM 29.03 ₂₅₆	SNOW 2.0 32.57	
Sosemanuk 226	LEX v1 5.60 ₁₂₈	LEX v1 11.89 ₁₂₈	LEX v1 10.02 ₁₂₈	LEX v1 10.84 ₂₅₆	SNOW 2.0 29.71 ₁₂₈	Rabbit 37.45
Salsa20/12 256	Salsa20/20 7.44 ₂₅₆	Salsa20/20 12.74 ₂₅₆	Salsa20/20 12.26 ₂₅₆	Salsa20/20 11.97 ₂₅₆	Salsa20/20 30.14 ₁₂₈	NLS v2 43.42
LEX v1 128	HC-128 9.51 ₁₂₈	AES-128 15.46 ₁₂₈	AES-128 16.17 ₁₂₈	AES-128 16.30 ₂₂₆	Sosemanuk 34.28 ₂₅₆	AES-256 50.79
Salsa20/20 256	Dragon 11.70 ₂₅₆	RC4 15.58	RC4 21.84 ₂₅₆	AES-256 25.30 ₂₅₆	AES-256 35.19 ₂₂₆	Sosemanuk 63.18
RC4 12.65	RC4 15.81 ₁₂₈	HC-128 23.84 ₂₅₆	HC-128 32.40 ₂₅₆	Dragon 36.40 ₂₅₆	Dragon 83.41 ₂₅₆	Dragon 88.23
Dragon 256	AES-128 13.38 ₁₂₈	AES-256 18.04 ₂₅₆	AES-256 25.16 ₂₅₆	RC4 36.40 ₂₅₆	RC4 356.42 ₁₂₈	RC4 359.64
AES-128 128	HC-256 15.96 ₂₅₆	Dragon 22.50 ₂₅₆	Dragon 29.99 ₁₂₈	HC-128 56.27 ₁₂₈	HC-128 767.88 ₁₂₈	HC-128 770.03
AES-256 256	AES-256 24.98 ₂₅₆	HC-256 28.79 ₂₅₆	HC-256 50.96 ₂₅₆	HC-256 124.39 ₂₅₆	HC-256 1727.68 ₂₅₆	HC-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 <small>226</small>	Sosemanuk <small>256</small>	SNOW 2.0 <small>6.19</small> <small>251</small>	Salsa20/8 <small>6.95</small> <small>128</small>	LEX v2 <small>24.53</small> <small>128</small>	LEX v2 <small>32.87</small>
SNOW 2.0 256	5.19 <small>256</small>	SNOW 2.0 <small>7.89</small> <small>128</small>	NLS v2 <small>6.66</small> <small>256</small>	SNOW 2.0 <small>7.29</small> <small>128</small>	Rabbit <small>26.78</small> <small>251</small>	Salsa20/8 <small>34.80</small>
CryptMTv3 256	5.57 <small>251</small>	Salsa20/8 <small>8.24</small> <small>251</small>	Salsa20/8 <small>7.42</small> <small>128</small>	NLS v2 <small>8.90</small> <small>128</small>	AES-128 <small>29.92</small> <small>128</small>	AES-128 <small>37.73</small>
NLS v2 128	5.64 <small>256</small>	Salsa20/12 <small>10.30</small> <small>128</small>	Rabbit <small>8.50</small> <small>256</small>	Salsa20/12 <small>8.98</small> <small>251</small>	Salsa20/8 <small>31.88</small> <small>256</small>	Salsa20/12 <small>40.31</small>
Sosemanuk 226	5.72 <small>128</small>	Rabbit <small>10.44</small> <small>226</small>	Sosemanuk <small>9.39</small> <small>128</small>	Rabbit <small>9.12</small> <small>256</small>	Salsa20/12 <small>37.39</small> <small>128</small>	Rabbit <small>41.30</small>
Salsa20/8 251	5.79 <small>251</small>	TRIVIUM <small>11.10</small>	TRIVIUM <small>10.11</small> <small>226</small>	Sosemanuk <small>11.16</small> <small>226</small>	Sosemanuk <small>38.54</small> <small>256</small>	CryptMTv3 <small>45.81</small>
HC-256 256	6.26 <small>256</small>	CryptMTv3 <small>12.45</small> <small>256</small>	Salsa20/12 <small>10.12</small> <small>256</small>	TRIVIUM <small>11.81</small> <small>256</small>	CryptMTv3 <small>42.61</small> <small>256</small>	SNOW 2.0 <small>48.44</small>
Salsa20/12 256	7.76 <small>128</small>	NLS v2 <small>12.87</small> <small>128</small>	LEX v2 <small>11.18</small> <small>128</small>	LEX v2 <small>12.28</small> <small>256</small>	SNOW 2.0 <small>42.91</small> <small>256</small>	Salsa20/20 <small>50.93</small>
Rabbit 128	8.02 <small>128</small>	LEX v2 <small>13.23</small> <small>256</small>	CryptMTv3 <small>12.83</small> <small>256</small>	CryptMTv3 <small>13.09</small> <small>256</small>	AES-256 <small>43.07</small> <small>256</small>	TRIVIUM <small>51.21</small>
TRIVIUM 9.03	9.03 <small>256</small>	Salsa20/20 <small>14.05</small> <small>256</small>	Salsa20/20 <small>14.78</small> <small>256</small>	Salsa20/20 <small>13.32</small> <small>256</small>	Salsa20/20 <small>47.94</small> <small>256</small>	AES-256 <small>58.74</small>
LEX v2 128	10.49 <small>128</small>	HC-128 <small>17.44</small> <small>128</small>	AES-128 <small>19.17</small> <small>128</small>	AES-128 <small>19.52</small> <small>128</small>	TRIVIUM <small>48.14</small> <small>128</small>	NLS v2 <small>87.26</small>
Salsa20/20 256	11.77 <small>256</small>	Dragon <small>18.17</small> <small>256</small>	AES-256 <small>28.21</small> <small>256</small>	AES-256 <small>28.64</small> <small>256</small>	NLS v2 <small>53.00</small> <small>128</small>	Sosemanuk <small>91.29</small>
Dragon 256	13.41 <small>128</small>	RC4 <small>20.23</small> <small>128</small>	HC-128 <small>28.50</small> <small>128</small>	Dragon <small>34.68</small> <small>256</small>	Dragon <small>95.21</small> <small>256</small>	Dragon <small>100.35</small>
RC4 16.44	16.44 <small>128</small>	AES-128 <small>22.02</small> <small>256</small>	Dragon <small>30.95</small> <small>256</small>	RC4 <small>55.96</small> <small>128</small>	RC4 <small>585.16</small> <small>128</small>	RC4 <small>589.22</small>
AES-128 128	18.81 <small>256</small>	HC-256 <small>24.41</small> <small>256</small>	RC4 <small>31.64</small> <small>128</small>	HC-128 <small>67.54</small> <small>128</small>	HC-128 <small>887.98</small> <small>128</small>	HC-128 <small>891.06</small>
AES-256 256	28.05 <small>256</small>	AES-256 <small>32.46</small> <small>256</small>	HC-256 <small>68.64</small> <small>256</small>	HC-256 <small>168.08</small> <small>256</small>	HC-256 <small>2345.04</small> <small>256</small>	HC-256 <small>2348.07</small>

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	Salsa20/8 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	Salsa20/12 256 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	TRIVIUM 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	TRIVIUM 26.09
NLS v2 128	SNOW 2.0 256 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	NLS v2 128 6.06	LEX 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	Salsa20/20 256 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	LEX v2 128 6.99	Sosemanuk 226 10.49	Sosemanuk 226 8.97	Sosemanuk 226 10.61	Rabbit 128 28.68	NLS v2 128 38.06
LEX v2 128	Dragon 256 7.28	Rabbit 128 12.43	Rabbit 128 10.89	Rabbit 128 11.52	SNOW 2.0 256 28.97	Rabbit 128 43.50
Salsa20/20 256	Rabbit 128 7.81	CryptMTv3 256 13.36	CryptMTv3 256 12.79	CryptMTv3 256 14.09	CryptMTv3 256 30.82	AES-256 256 48.24
CryptMTv3 256	CryptMTv3 256 8.18	RC4 256 14.06	RC4 256 17.33	AES-128 128 18.67	Sosemanuk 226 36.61	LEX v2 128 64.98
Dragon 256	RC4 128 8.39	AES-128 128 14.21	AES-128 128 18.59	RC4 256 30.02	AES-256 256 38.85	Dragon 256 75.87
RC4 9.44	HC-128 128 19.25	HC-128 128 23.80	HC-128 256 31.14	AES-256 256 31.14	Dragon 256 71.97	Sosemanuk 226 94.55
Rabbit 128	AES-128 128 10.42	AES-256 256 22.22	AES-256 256 31.00	Dragon 256 35.72	RC4 128 306.25	RC4 310.67
AES-128 128	HC-256 256 18.50	Dragon 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	AES-256 256 30.69	HC-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	Salsa20/8 5.96 <small>251</small>	7.54	TRIVIUM 6.57 <small>251</small>	Salsa20/8 6.76 <small>128</small>	LEX v2 22.11 <small>251</small>	Salsa20/8 26.06
HC-128 <small>128</small>	TRIVIUM 6.03	7.67 <small>128</small>	NLS v2 6.84	TRIVIUM 7.50 <small>251</small>	Salsa20/8 24.56 <small>128</small>	LEX v2 28.13
NLS v2 <small>128</small>	LEX v2 6.52 <small>128</small>	9.51 <small>251</small>	Salsa20/8 6.97 <small>128</small>	NLS v2 8.54 <small>256</small>	Salsa20/12 28.66 <small>256</small>	Salsa20/12 30.14
Salsa20/8 <small>251</small>	Sosemanuk 6.64 <small>226</small>	LEX v2 9.89 <small>128</small>	LEX v2 7.77 <small>128</small>	TRIVIUM 8.79 <small>256</small>	TRIVIUM 28.94 <small>256</small>	TRIVIUM 33.52
LEX v2 <small>128</small>	Salsa20/12 7.21 <small>256</small>	10.21	Salsa20/12 9.66 <small>256</small>	Salsa20/12 9.32 <small>256</small>	Salsa20/20 32.94 <small>256</small>	Salsa20/20 34.54
HC-256 <small>256</small>	SNOW 2.0 7.85 <small>256</small>	10.99	SNOW 2.0 9.91 <small>256</small>	SNOW 2.0 10.53 <small>256</small>	Rabbit 34.80 <small>128</small>	SNOW 2.0 46.99
Sosemanuk <small>226</small>	Dragon 8.47 <small>256</small>	12.27	Sosemanuk 11.94 <small>226</small>	Sosemanuk 13.46 <small>128</small>	NLS v2 41.98 <small>128</small>	Rabbit 51.95
SNOW 2.0 <small>256</small>	NLS v2 8.80 <small>128</small>	12.68	Rabbit 13.14 <small>128</small>	Rabbit 13.95 <small>128</small>	Sosemanuk 42.87 <small>226</small>	AES-128 54.67 <small>128</small>
Dragon <small>256</small>	Rabbit 8.82 <small>128</small>	15.09	Salsa20/20 14.85 <small>256</small>	Salsa20/20 14.46 <small>256</small>	SNOW 2.0 42.89 <small>128</small>	NLS v2 62.66
Salsa20/12 <small>256</small>	Salsa20/20 9.21 <small>256</small>	15.24	CryptMTv3 24.40 <small>256</small>	CryptMTv3 26.70 <small>256</small>	AES-128 49.10 <small>128</small>	CryptMTv3 70.93 <small>256</small>
Rabbit <small>128</small>	RC4 12.21	19.50	RC4 27.21 <small>128</small>	AES-128 29.86 <small>256</small>	CryptMTv3 66.40 <small>226</small>	Sosemanuk 82.63
CryptMTv3 <small>256</small>	CryptMTv3 13.38 <small>256</small>	25.31	AES-128 29.74 <small>128</small>	Dragon 45.93 <small>256</small>	AES-256 82.91 <small>256</small>	AES-256 99.18
Salsa20/20 <small>256</small>	AES-128 14.34 <small>128</small>	32.43	HC-128 35.59 <small>128</small>	RC4 46.80 <small>256</small>	Dragon 96.36 <small>256</small>	Dragon 103.73
RC4 <small>15.10</small>	HC-128 36.95 <small>256</small>	43.99	Dragon 64.93 <small>256</small>	AES-256 64.93 <small>256</small>	RC4 472.63 <small>128</small>	RC4 477.03
AES-128 <small>128</small>	HC-256 29.45 <small>256</small>	58.42	AES-256 64.91 <small>256</small>	HC-128 82.58 <small>128</small>	HC-128 1115.14 <small>128</small>	HC-128 1117.68
AES-256 <small>256</small>	AES-256 64.60 <small>256</small>	69.66	HC-256 80.54 <small>256</small>	HC-256 195.89 <small>256</small>	HC-256 2726.91 <small>256</small>	HC-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	SNOW 2.0 256	Salsa20/8 251	Salsa20/8 251	Salsa20/8 251
SNOW 2.0 256	5.18	SNOW 2.0 256	Salsa20/8 251	SNOW 2.0 256	LEX v2 128	Salsa20/12 256
HC-256 256	5.33	Salsa20/12 256	NLS v2 128	Salsa20/12 256	AES-128 128	LEX v2 128
CryptMTv3 256	5.37	Rabbit 128	Rabbit 128	Rabbit 128	Salsa20/12 256	AES-128 128
Salsa20/8 251	5.40	TRIVIUM 10.21	Salsa20/12 256	NLS v2 128	Salsa20/20 256	Salsa20/20 256
NLS v2 128	6.02	Sosemanuk 226	TRIVIUM 10.72	TRIVIUM 9.30	SNOW 2.0 256	SNOW 2.0 256
Salsa20/12 256	7.51	CryptMTv3 256	LEX v2 128	LEX v2 128	AES-256 256	CryptMTv3 256
Rabbit 128	7.54	LEX v2 128	CryptMTv3 256	CryptMTv3 256	Rabbit 128	TRIVIUM 47.40
TRIVIUM 8.29	8.29	NLS v2 128	Salsa20/20 256	Salsa20/20 256	CryptMTv3 256	Rabbit 66.37
Sosemanuk 226	9.74	Salsa20/20 256	Sosemanuk 226	Sosemanuk 226	TRIVIUM 44.54	AES-256 256
LEX v2 128	9.91	Dragon 256	AES-128 128	AES-128 128	Sosemanuk 226	Dragon 93.11
Salsa20/20 256	11.74	RC4 18.91	RC4 26.02	AES-256 256	NLS v2 128	NLS v2 128
Dragon 256	12.57	HC-128 128	AES-256 256	Dragon 256	Dragon 256	Sosemanuk 226
RC4 14.20	14.20	AES-128 128	Dragon 256	RC4 45.22	RC4 451.46	RC4 458.36
AES-128 128	16.98	HC-256 256	HC-128 128	HC-128 128	HC-128 128	HC-128 128
AES-256 256	28.41	AES-256 256	HC-256 256	HC-256 256	HC-256 256	HC-256 256
			64.34	158.26	2215.76	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	Salsa20/8 251	Salsa20/8 251	Salsa20/8 251	Salsa20/8 251	Salsa20/8 251
1.99	2.64	2.17	2.14	9.68	11.42
Salsa20/12 256	Salsa20/12 256	Salsa20/12 256	Salsa20/12 256	Salsa20/12 256	Salsa20/12 256
2.74	3.40	2.94	2.88	10.88	12.62
Salsa20/20 256	Salsa20/20 256	Salsa20/20 256	Salsa20/20 256	Salsa20/20 256	Salsa20/20 256
4.24	4.90	4.48	4.38	13.29	15.03
HC-128 128	Sosemanuk	NLS v2	SNOW 2.0	LEX v2	LEX v2
4.80	7.10	6.82	8.40	22.80	27.29
HC-256 256	SNOW 2.0	SNOW 2.0	NLS v2	AES-128	AES-128
6.17	8.24	7.74	8.73	28.21	33.33
Sosemanuk 226	LEX v2 128	LEX v2 128	LEX v2 128	SNOW 2.0 256	SNOW 2.0 256
6.17	9.27	8.19	9.17	31.82	34.52
NLS v2 128	Dragon	Sosemanuk	Sosemanuk	Sosemanuk	CryptMTv3
6.22	10.03	9.17	10.61	32.37	40.84
SNOW 2.0 256	NLS v2 128	TRIVIUM 11.16	Rabbit	Rabbit	AES-256
7.06	11.16	13.21	15.16	36.15	52.24
LEX v2 128	TRIVIUM 13.06	Rabbit 14.39	TRIVIUM 15.16	CryptMTv3 38.70	Rabbit 52.75
Dragon 256	RC4 13.95	CryptMTv3 15.10	CryptMTv3 17.00	AES-256 44.62	TRIVIUM 62.67
8.39	13.95	15.10	17.00	44.62	62.67
CryptMTv3 256	Rabbit 128	RC4 14.83	AES-128 17.42	NLS v2 18.52	NLS v2 46.05
8.92	14.83	17.42	18.52	46.05	69.29
RC4 11.16	CryptMTv3 15.98	AES-128 17.88	RC4 27.34	TRIVIUM 59.77	Dragon 70.27
TRIVIUM 11.91	HC-128 16.43	HC-128 25.40	Dragon 28.86	Dragon 66.90	Sosemanuk 77.50
Rabbit 128	AES-128 20.57	Dragon 27.14	AES-256 34.97	RC4 245.45	RC4 248.77
13.89	20.57	27.14	34.97	245.45	248.77
AES-128 128	HC-256 256	AES-256 34.98	HC-128 58.21	HC-128 779.70	HC-128 781.49
17.75	26.79	34.98	58.21	779.70	781.49
AES-256 256	AES-256 256	HC-256 54.08	HC-256 130.33	HC-256 1798.00	HC-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.