Table 1: Performance of Camellia (updated on October 31, 2008)
Software Performance

Processor	Language	Key Size	Speed			RAM Usage(*1)		ROM Usage				Reference/Notes
			Key scheduling	Encryption Decryption		Key scheduling	Enc./Dec.	Total Size	Key scheduling	Enc./Dec.	Table	
		[bits]	[cycles]	[cycles]	[Mbps]	[bytes]	[bytes]	[bytes]	[bytes]	[bytes]	[bytes]	
Pentium II (Win95, 300MHz *3)	ANSI C	128	263	577	66.6	44	64	9,461	1,600	3,733	4,128	1st NESSIE Workshop (Nov. 2000)
Pentium III (FreeBSD, 700MHz *4)	Assembly	128	1,570	308	290.9	288	20	15,012	6,788	0	8,224	1st NESSIE Workshop (Nov. 2000)
		128	160	371	241.5	28	36	11,420	1,046	2,150	8,224	
		192	222	494	181.4	28	36	13,032	1,469	3,323	8,240	
		256	226	494	181.4	28	36	13,048	1,485	3,323	8,240	
Pentium III (Linux, 600MHz *5)	ANSI C	128	285	560	137.1	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	390	720	106.7	-	-	-	-	-	-	
		256	401	736	104.3	-	-	-	-	-	-	
Pentium III (Win2000, 850MHz *6)	ANSI C	128	298	592	183.8	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	426	768	141.7	-	-	-	-	-	-	
		256	435	768	141.7	-	-	-	-	-	-	
Pentium III (Win98 SE, 650MHz *7)	Assembly	128	-	326	255.2	-	-	29,285	-	-	-	CRYPTREC Report 2002
		128	(Enc) 467 (*2)		0.72 μ sec	-	-	20,110	-	-	-	
		128	(Dec) 474 (*2)		0.73 μ sec	-	-	20,236	-	-	-	
Pentium III (Win2000, 1GHz *8)	Java	128	9,091	793	161.4	-	-	-	-	-	-	Not published
Pentium 4 (Linux, 1.7GHz *9)	ANSI C	128	453	1,008	215.9	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	546	1,376	158.1	-	-	-	-	-	-	
		256	555	1,376	158.1	-	-	-	-	-	-	
Pentium 4 (WinXP, 3.2GHz *10)	ANSI C	128	2,309	2,798	146.4	-	-	-	-	-	-	Reference Code of this HP
		192	3,315	3,708	110.5	-	-	-	-	-	-	
		256	3,276	3,757	109.0	-	-	-	-	-	-	
		128	658	981	417.5	-	-	-	-	-	-	OSS Code of this HP (Old version)
		192	931	1,278	320.5	-	-	-	-	-	-	
		256	1,007	1,250	327.7	-	-	-	-	-	-	
		128	913	900	455.1	-	-	-	-	-	-	
		192	1,280	1,168	350.7	-	-	-	-	-	-	
		256	1,289	1,165	351.6	-	-	-	-	-	-	
Pentium 4 (WinXP, 3.2GHz *10)	Java	128	-	966	424.0	-	-	-	-	-	-	Not published
		128	-	1,552	264.0	-	-	-	-	-	-	OSS Code of this HP (Old version)
Pentium 4 (WinXP, 3.2GHz *10)	Assembly	128	-	361	1,134.6	-	-	-	-	-	-	Reported by S.Oda, et al. [NTT] SCIS 2006 (Jan. 2006)
Pentium 4 HT (WinXP, 3.6GHz *11)	Assembly	128	-	457 (*19)	1,008.3	-	-	-	-	-	-	Reported by M. Matsui [Mitsubishi] FSE 2006 (Mar. 2006)
		128	-	415 (*20)	1,110.4	-	-	-	-	-	-	
Core2 Duo E6400 (WinXP, 2.13GHz *21)	Assembly	128	-	208 (*19)	1,310.8	-	-	-	-	-	-	Reported by M. Matsui, et al. [Mitsubishi] FSE 2006 (Mar. 2006)
		128	-	135 (*20)	2,019.6	-	-	-	-	-	-	
Core2 Duo E8400 (Fedora, 3.16GHz *26)	ANSI C	128	415	505	801.0	-	-	-	-	-	-	OSS Code of this HP
		192	568	655	617.5	-	-	-	-	-	-	
		256	561	655	617.5	-	-	-	-	-	-	
	Java	128	566	698	579.5							OSS Code of this HP (with 64-bit registers)
		128	679	1,248	324.1			small size				
		192	907	869	465.5							
		192	1,068	1,599	253			small size				
		256	935	869	465.5							
		256	1,115	1,599	253			small size				
		128	1,519	1,949	207.5							OSS Code of this HP (with 32-bit registers)
		128	1,627	2,288	176.8			small size				
		192	2,050	2,108	191.9							
		192	2,174	2,638	153.3			small size				
		256	2,073	2,117	191.1							
		256	2,193	2,658	152.2			small size				
AMD Athlon 64 3500+ (WinXP, 2.2GHz *12)	Assembly	128	-	175 (*19)	1,609.1	-	-	-	-	-	-	Reported by M. Matsui [Mitsubishi] FSE 2006 (Mar. 2006)
		128	-	243 (*20)	1,158.8	-	-	-	-	-	-	

Processor	Language	Key Size	Speed			RAM Usage(*1)		ROM Usage				Reference/Notes
			Key scheduling	Encryption Decryption		Key scheduling	Enc./Dec.	Total Size	Key scheduling	Enc./Dec.	Table	
		[bits]	[cycles]	[cycles]	[Mbps]	[bytes]	[bytes]	[bytes]	[bytes]	[bytes]	[bytes]	
AMD Athlon 64 3500+ (WinXP, 2.2GHz *23)	Java	128	3,344	3,518	80.0	-	-	19,250 (*24)	-	-	-	OSS Code of this HP (without optimized)
		192	3,870	3,606	78.1	-	-		-	-	-	
		256	3,870	3,606	78.1	-	-		-	-	-	
		128	3,518	4,046	69.6	-	-	8,708 (*24)	-	-	-	
		192	3,958	4,398	64.0	-	-		-	-	-	
		256	4,046	4,398	64.0	-	-		-	-	-	
AMD Athlon 1700 (Linux, 1467MHz *13)	ANSI C	128	235	512	366.8	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	346	640	293.4	-	-	-	-	-	-	
		256	361	672	279.4	-	-	-	-	-	-	
AMD Opteron 270 (Vista, 2GHz *22)	ANSI C	128	-	800	320	-	-	-	-	-	-	Reported by K. Oikawa, et al. [Iwate Prefectural University] SCIS 2008 (Jan. 2008)
AMD Phenom 9850 (FreeBSD, 2507MHz *25)	ANSI C	128	355	470	682.9	-	-	-	-	-	-	OSS Code of this HP
		192	541	610	526.2	-	-	-	-	-	-	
		256	512	603	532.3	-	-	-	-	-	-	
Alpha 21264 (Tru64, 667MHz *14)	Assembly	128	158	326	261.9	48	48	21,040	1,600	2,928	16,512	1st NESSIE Workshop (Nov. 2000)
		128	118	339	251.8	48	48	20,736	1,132	3,076	16,528	
		192	176	445	191.9	48	48	22,196	1,668	4,000	16,528	
		256	176	445	191.9	48	48	22,204	1,676	4,000	16,528	
Alpha 21264 (Tru64, 463MHz *15)	Assembly	128	-	282	210.2	-	-	31,552	-	-	-	CRYPTREC Report 2002
		128	(Enc) 448 (*2)		0.97 μ sec	-	-	25,792	-	-	-	
		128	(Dec) 435 (*2)		0.94 μ sec	-	-	25,792	-	-	-	
Alpha 21264A (OSF1, 667MHz *16)	ANSI C	128	320	560	152.5	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	407	752	113.5	-	-	-	-	-	-	
		256	453	752	113.5	-	-	-	-	-	-	
UltraSPARCIIi (Sol, 400MHz *17)	Assembly	128	-	355	144.2	-	-	15,240	-	-	-	CRYPTREC Report 2002
		128	403 (*2)		1.01 μ sec	-	-	23,992	-	-	-	
Sun/Sparc V9 (Sun OS5.8, 400MHz *18)	ANSI C	128	306	768	66.7	-	-	-	-	-	-	NESSIE Report (Feb. 2003)
		192	518	960	53.3	-	-	-	-	-	-	
		256	514	960	53.3	-	-	-	-	-	-	

(*1) The figure includes stack area, and excludes text area and key area.
(*2) The figure includes key generation and one block encryption. This is achieved by using the on-the-fly key generation.
(*3) IBM PC/AT compatible PC, Intel Pentium II (300MHz), 512KB L2 cache, Windows95, 160MB main memory.
(*4) IBM PC/AT compatible PC, Intel Pentium III (700MHz), 256KB on-die L2 cache, FreeBSD 4.0R, 128MB main memory.
(*5) IBM PC/AT compatible PC, Intel Pentium III (600MHz), 256KB on-die L2 cache, Linux 2.4.17, 256MB main memory.
(*6) IBM PC/AT compatible PC, Intel Pentium III (850MHz), 256KB on-die L2 cache, Windows2000.
(*7) IBM PC/AT compatible PC, Intel Pentium III (650MHz), 256KB on-die L2 cache, Windows98 SE, 64MB main memory.
(*8) IBM PC/AT compatible PC, Intel Pentium III (1GHz), 256KB on-die L2 cache, Windows2000, 512MB main memory
(*9) IBM PC/AT compatible PC, Intel Pentium 4 (1.7GHz), Linux 2.4.12
(*10) IBM PC/AT compatible PC, Intel Pentium 4 (3.2GHz), 512KB on-die L2 cache, WindowsXP SP2, 2GB main memory, Hyper-threading off.
(*11) IBM PC/AT compatible PC, Intel Pentium 4 HT Prescott (3.6GHz), WindowsXP 64bit Edition, 1GB main memory
(*12) IBM PC/AT compatible PC, AMD Athlon 64 3500+ Winchester (2.2GHz), WindowsXP 64bit Edition, 1GB main memory
(*13) IBM PC/AT compatible PC, AMD Athlon 1700 (1467MHz), Linux 2.4.18.
(*14) Alpha 21264 (667MHz), Tru64 UNIX 4.0F, 2GB main memory.
(*15) Alpha 21264 (463MHz), Tru64 UNIX V5.1, 512MB main memory.
(*16) Alpha EF6.7 (21264A) (667MHz), OSF1 V4.0, V5.1.
(*17) Ultra SPARC IIi (400MHz), Solaris 7, 256MB main memory.
(*18) Sun/Sparc V9 (400MHz), SunOS 5.8.
(*19) In two-block parallel encryption.
(*20) Using bitslice technique.
(*21) IBM PC/AT compatible PC, Intel Core2 Duo E6400 (2.13GHz), WindowsXP 64bit Edition, 1GB main memory
(*22) IBM PC/AT compatible PC, AMD Opteron 270 (2GHz), Windows Vista Business Edition, Microsoft .NET Framework 2.0
(*23) IBM PC/AT compatible PC, AMD Athlon 64 3500+ Winchester (2.2GHz), FreeBSD-current amd64, 2GB main memory
(*24) Class file size
(*25) IBM PC/AT compatible PC, AMD Phenom 9850 (2507.63 MHz), FreeBSD-current amd64, 4GB main memory
(*26) IBM PC/AT compatible PC, Intel Core2 Duo E8400 (3.16GHz), Fedora9 x86_64, 4GB main memory

Table 2: Performance of Camellia (updated on October 31, 2008)
Software Performance for Smart Card and Embedded Systems

Processor	Language	Key Size [bits]	Speed		RAM Usage(*1)		ROM Usage					Reference/Notes
			Key scheduling [cycles]	Encryption Decryption [cycles]	Key scheduling [bytes]	Enc./Dec. [bytes]	Total Size [bytes]	Key scheduling [bytes]	Enc./Dec. [bytes]	Table [bytes]	Sharing Size (*5) [bytes]	
8051 (*6)	Assembly	128	10217 (*1) 10.22msec		0	32 (*2)	990	0	702	288	0	1st NESSIE Workshop (Nov. 2000)
Z80 (*7)	Assembly	128	5,146 1.03msec	28,382 5.68msec	44 (*3)	62 (*3)	1,698	358	1,183	288	-131	Not published
		128	(Enc) 35,951 (*1) 7.19msec		0	60 (*3)	1,268	-	1,023	-	-797	Not published
			(Dec) 37,553 (*1) 7.51msec		0	60 (*3)		-	1,042	-		
H8/3113 (*8)	Assembly	128	2,380 0.95msec	4,100 1.64msec	208 (*4)	0	-	-	-	-	-	Reported by Chung-Huang Yang [National Kaohsiung First Univ. of Sci. and Tech.] Updated Version of SCIS2001
MC68HC705B16 (*9)	Assembly	128	7,500 3.57msec	9,900 4.71msec	208 (*4)	0	-	-	-	-	-	
MC68HC908AB32(*10)	Assembly	128	5,679 0.71msec	8,430 1.05msec	208 (*4)	0	-	-	-	-	-	Reported by Chung-Huang Yang
SLE66CLX320P (*11)	Assembly	128	6,144 0.41msec	17,920 1.19msec	248 (*3)		1,279	-	-	-	-	Not published
		128	(Enc) 24,064 (*1) 1.60msec		56 (*3)		1,311	-	-	-	-	Not published
			(Dec) 24,576 (*1) 1.64msec		56 (*3)			-	-	-	-	
SLE66CLX320P (*12)	Assembly	128	6,229 0.41msec	18,244 1.22msec	248 (*3)		1,279	-	-	-	-	Not published
		128	(Enc) 24,077 (*1) 1.61msec		56 (*3)		1,311	-	-	-	-	Not published
			(Dec) 24,989 (*1) 1.67msec		56 (*3)			-	-	-	-	Not published
AE45X (*13)	Assembly	128	(Enc) 7,510 (*1) 1.11msec		56 (*3)		-	-	-	-	-	Not published
			(Dec) 8,032 (*1) 1.18msec		56 (*3)			-	-	-	-	
M32Rx/D (*14)	Assembly	128	642 6.42µsec	1,236 12.36µsec	44 (*2)	44 (*2)	8,684	1,392	3,164	4,128	0	1st NESSIE Workshop (Nov. 2000)

(*1) The figure includes key generation and one block encryption. This is achieved by using the on-the-fly key generation.
(*2) The figure includes stack area, and excludes text area and key area.
(*3) The figure includes stack area, text area and key area.
(*4) The figure shows the size of round keys.
(*5) Some ROM size may be reduced, since some functions can be shared among key generation, encryption and decryption.
(*6) Intel 8051 (12MHz; 1cycle=12oscillator periods) simulator on Unix.
(*7) Z80 (5MHz) simulator on Windows.
(*8) Hitachi H8/3113 (5MHz; 1cycle=2oscillator periods) on Hitachi's E6000 Emulator.
(*9) Motorola 6805 series MC68HC705B16 (2.1MHz) on Motorola's In-Circuit Simulator Kits.
(*10) Motorola 6805 series MC68HC908AB32 (8MHz) on Motorola's In-Circuit Simulator Kits.
(*11) Infineon SLE66CLX320P (15MHz)
(*12) Infineon SLE66CLX320P (15MHz) simulator
(*13) Mitsubishi 32-bit microcomputer M32Rx/D (100MHz) on MSA2310 evaluation board.
(*14) Renesas AE45X (6.78MHz) simulator

Table 3: Performance of Camellia (updated on October 31, 2008)
Hardware Performance

Type	Archi-tecture	Design Library	Key Size [bits]	Speed				Area Size				Efficiency	Reference/Notes
				Key Se tup time [nsec]	Max. delay [nsec]	Latency [cycles]	Throughput [Mbps]	Unit	Total (*1) [unit]	Key sched. (*2) [unit]	Enc./Dec. (*3) [unit]	Throughput/Area [kbps/unit]	
ASIC	Unrolled	Mitsubishi 0.35 μm	128	24.36	109.35	1	1170.55	gate	272,820	55.91	216.91	4.29	1st NESSIE Workshop (Nov. 2000)
		Mitsubishi 0.18 μm	128	40.00	40.00	1	3200.00		35,510	-	-	90.12	Not published
		Mitsubishi 0.18 μm	128	45.96	45.96	1	2785.00		24,490	-	-	113.72	Not published
	Loop	Mitsubishi 0.35 μm	128	110.20	27.67	21	220.28	gate	11,350	4.98	6.37	19.41	ISEC200-73 (Sep. 2000)
		Mitsubishi 0.35 μm	128	117.04	28.73	21	212.16		9,660	5.75	3.91	21.96	1st NESSIE Workshop (Nov. 2000)
		Mitsubishi 0.18 μm	128	144.88	36.22	21	168.28		8,510	-	-	19.77	Not published
		Mitsubishi 0.18 μm	128	25.92	6.48	21	940.62		27,460	-	-	34.25	Not published
		Mitsubishi 0.18 μm	128	28.20	7.05	21	864.57		21,450	-	-	40.31	Not published
		Mitsubishi 0.18 μm	128	23.20	5.80	21	1050.90		11,872	-	-	88.52	Not published
		Mitsubishi 0.18 μm	128	137.24	34.31	21	177.65		8,123	-	-	21.87	Not published
		Mitsubishi 0.18 μm	128	12.96	3.24	21	1881.25		44,299	-	-	42.47	Not published
		Mitsubishi 0.18 μm	128	-	32.83	40	97.47		6,856	-	-	14.22	ISEC201-133 (Mar. 2002)
		Mitsubishi 0.18 μm	128	-	44.71	40	71.57		6,372	-	-	11.23	ISEC201-133 (Mar. 2002)
		0.25 μm	256	-	5.46	-	837.00		39,350	22.76	16.33	21.27	CRYPTREC Report 2000
		0.25 μm	256	-	11.51	-	397.00		23,120	13.3	9.67	17.17	CRYPTREC Report 2000
		IBM 0.11 μm	128	-	8.72	44	333.65		7,875	-	-	42.37	Reported by A.Satoh, et al. [IBM Research] ISC 2002 (Oct. 2002)
		IBM 0.11 μm	128	-	8.82	18	806.26		13.712	-	-	58.8	
		IBM 0.11 μm	128	-	4.21	18	1689.10		23,382	-	-	72.24	
		IBM 0.13 μm	128	-	8.93	44	325.76		6,511	-	-	50.03	Reported by A.Satoh, et al. [IBM Research] ISC 2003 (Oct. 2003)
		IBM 0.13 μm	128	-	3.05	22	1907.61		20,788	-	-	91.76	
		IBM 0.13 μm	128	-	3.30	18	2154.88		29,809	-	-	72.29	
		IBM 0.18 μm	128	-	14.22	44	204.57		6,264	-	-	32.66	
		IBM 0.18 μm	128	-	6.00	22	969.72		14,166	-	-	68.45	
		IBM 0.18 μm	128	-	5.00	18	1422.22		31,069	-	-	45.78	
		IBM 0.18 μm	128	-	8.80	23	632.40		11,900	-	-	53.14	Reported by T. Sugawara, et al. [Tohoku University, IBM Research] IT2006-104 (Mar. 2007)
		IBM 0.18 μm	128	-	5.31	23	1048.10		21,500	-	-	48.75	
		IBM 0.18 μm	128	-	9.81	23	567.30		9,100	-	-	62.34	
		IBM 0.18 μm	128	-	6.82	23	816.00		16,500	-	-	49.45	
FPGA	Loop	Xilinx XC4000XL	128	362.83	78.82	21	77.34	CLB	1,296	-	-	59.68	1st NESSIE Workshop (Nov. 2000)
		Xilinx VirtexE	128	135.03	30.56	21	199.46	Slice	1,816	-	-	109.83	ISEC2001-53 (Sep. 2001)
		Xilinx VirtexE	128	126.00	28.80	21	211.90		1,816	-	-	116.69	ISEC2001-53 (Sep. 2001)
		Xilinx VirtexE	128	127.04	26.80	21	227.42		1,780	-	-	127.76	ISEC2001-53 (Sep. 2001)
		Xilinx VirtexE	128	-	22.62	44	128.58		908	-	-	141.61	Reported by A.Satoh, et al. [IBM Research] ISC 2003 (Oct. 2003)
		Xilinx VirtexE	128	-	16.04	22	362.82		1,745	-	-	207.92	
		Xilinx VirtexE	128	-	18.08	18	393.24		2,833	-	-	138.81	
		Xilinx Virtex1000E	128	-	33.47	40	95.60		1,396	-	-	68.48	ISEC2001-133 (Mar. 2002)
		Xilinx Virtex1000E	128	-	27.25	21	95.60		1,678	-	-	56.97	Reported by T.Sorimachi, et al. [Mitsubishi] SCIS 2003 (Jan. 2003)
		Xilinx Virtex1000E	128	-	30.90	40	103.57		1,389	-	-	74.56	
		Xilinx Virtex1000E	128	-	31.04	40	103.10		1,358	-	-	75.92	
		Xilinx Virtex1000E	128	-	40.14	40	79.73		1,124	-	-	70.93	
	Unrolled	Xilinx VirtexE	128	97.70	318.50	1	401.89		9,426	-	-	42.64	ISEC2001-53 (Sep. 2001)
		Xilinx Virtex1000E	128	-	340.97	1	375.40		8,976	-	-	41.82	Reported by T.Sorimachi, et al. [Mitsubishi] SCIS 2003 (Jan. 2003)
		Xilinx Virtex3200E	128	-	346.87	1	369.01		8,957	-	-	41.2	
	Pipeline	Xilinx VirtexE	128	83.25	18.96	20	6749.99		9,692	-	-	696.45	ISEC2001-53 (Sep. 2001)
		Xilinx Virtex3200E	128	-	0.05	96	25440.00		19.482	-	-	1,305.82	IEICE2004 A-7-7 (Sep. 2004)
		Xilinx XC2V4000	128	-	-	-	16300.00	Slice (BRAMS)	5,368 (88)	-	-	-	Reported by D. Denning, et al. FPL 04 (Aug. 2004)
	SubPipeline	Xilinx XC2V4000	128	-	-	-	17400.00		7,837 (88)	-	-	-	Reported by D. Denning, et al. FPL 04 (Aug. 2004)
		Xilinx XC2Vp50	128	-	-	-	33250.00		11,287 (88)	-	-	-	Reported by D. Denning, et al. PRIME 2005 (Jul. 2005)

(*1) The figure includes key scheduling circuit, encryption/decryption circuit, controller, output register, subkey register and buffers for fan-out adjustment.
(*2) The figure includes subkey register.
(*3) The figure includes output register.

Table 4: Performance of Camellia (updated on October 31, 2008)
Hardware Performance for AES and Camellia 2-in-1 architecture

Type	Archi-tecture	Design Library	Key Size [bits]	Speed				Area Size				Efficiency	Reference/Notes
				Key Se tup time [nsec]	Max. delay [nsec]	Latency [cycles]	Throughput [Mbps]	Unit	Total (*1) [unit]	Key sched. (*2) [unit]	Enc./Dec. (*3) [unit]	Throughput/Area [kbps/unit]	
ASIC	Loop	IBM 0.13 μ m	128	-	8.80	(AES) 31 (Camellia) 22	(AES) 469.22 (Camellia) 661.18	gate	14,918	-	-	-	Reported by A.Satoh, et al. [IBM Research] CHES 2003 (Sep. 2003)
		IBM 0.13 μ m	128	-	5.20	(AES) 31 (Camellia) 22	(AES) 794.05 (Camellia) 1118.89		24,424	-	-	-	

(*1) The figure includes key scheduling circuit, encryption/decryption circuit, controller, output register, subkey register and buffers for fan-out adjustment.
(*2) The figure includes subkey register.
(*3) The figure includes output register.