

MMCAU AES{128,192,256} Performance Summary, April 21, 2011

Security Algorithm [Cycle Counts]		cm4_assyLib (tcml)	cm4_assyLib (flash)	cm4_nocau (flash)
aes128	setkey	273	309	460
128	encrypt	270	281	3862
128	decrypt	280	288	4005
aes192	setkey	287	355	478
128	encrypt	311	321	4664
128	decrypt	322	330	4834
aes256	setkey	312	401	616
128	encrypt	348	357	5462
128	decrypt	361	368	5654

Notes: CM4 uses GNU C compiler with -O3 optimization

CM4 configuration is 100 MHz core with 25 MHz flash
(except text-in-ram)

All measurements are running with text-in-flash except
cm4 (tcml)

Calculated Mbits/MHz		cm4_assyLib (tcml)	cm4_assyLib (flash)	cm4_nocau (flash)
aes128	setkey			
128	encrypt	0.474	0.456	0.033
128	decrypt	0.457	0.444	0.032
aes192	setkey			
128	encrypt	0.412	0.399	0.027
128	decrypt	0.398	0.388	0.026
aes256	setkey			
128	encrypt	0.368	0.359	0.023
128	decrypt	0.355	0.348	0.023

Absolute Mbps		cm4_assyLib (tcml)	cm4_assyLib (flash)	cm4_nocau (flash)
		100	100	100 MHz
aes128	avg(e+d)	46.56	45.00	3.26
aes192	avg(e+d)	40.45	39.33	2.70
aes256	avg(e+d)	36.12	35.32	2.30

Notes: The Absolute Mbps is calculated using the average of the encrypt and decrypt times, that is, avg(e+d)