Results of the FIPS-140-2 Tests and Other Statistical Tests Done on Files Encrypted Using IP3

1 Testing of the Prototype

1.1 Statistical Tests

Various statistical tests have been performed to assess the cryptographic capabilities of the present enhanced prototype. Three different kinds of statistical tests where performed, and the respective results are discussed below.

1.1.1 FIPS 140-2 Tests of Randomness

The FIPS 140-2 tests are the statistical tests[1] of the US National Institute of Standards and Technology (NIST) for evaluating encryptions and random number generators. It includes four statistical tests of randomness: the frequency (monobit) test, the poker test, the runs test, and the long runs test. Details of these tests can be found in the current literature. We have run our prototype in the files of the Calgary corpus and the Canterbury corpus. The results are shown in Tables 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10. Observe that the prototype passes *the four tests on all the files* of the aforementioned corpuses. The results of the tests demonstrate the random-like properties of the output of IP3 – based on the most stringent industry standards.

1.1.2 Markovian Tests

This test consists of measuring the independence of the bits in the output that are k positions apart. The measure is the estimated probability of 0 given 0 and the probability of 1 given 1 (the complementary probabilities are consequently derived). The probability of 0 given 0 is estimated

[1]The first FIPS 140-2 Draft was signed on May 25, 2001. These tests are more *restrictive* than those of the FIPS 140-1. Although the FIPS 140-2 have become the standard tests since only May 25, 2002, we have opted to use *these* test to show the power of DODE* and our enhanced prototype.

by counting the number of zeros in the output, say at position n, for which the bit at position $n-k$ is also a 0, divided by the total number of zeros. The probability of 1 given 1 is defined analogously. The prototype was tested on all the files of the Calgary corpus and the Canterbury corpus. The results obtained are shown in Tables 11 and 12 respectively.

The second and third columns of these tables contain $\hat{f}_{0|0}$ and $\hat{f}_{1|1}$, which are the probability of 0 given 0, and the probability of 1 given 1 in the output respectively. The fourth column contains the value of the Chi-square statistic for $\hat{f}_{a_i|a_j}$, where a_i, a_j are either 0 or 1, and the number of degrees of freedom is unity. The last column reports the confidence level at which the independence hypothesis is true. Observe that for *all* the files of the Calgary corpus and the Canterbury corpus the output random variables are *independent*, with a level of confidence *above 98%*. Similar results were also obtained for bits that are 2, 3, 4, and 5 positions apart.

1.1.3 Key/Output Test of Independence

This test measures the degree of dependence between the key and the output. The measure analyzed is the estimated probability of change in the output when the key is modified by *a single bit*. This measure, $\hat{p}$, is obtained by dividing the number of bits *changed* in the output by the output size. It is accepted that the closer the estimated probability of change to 0.5, the more difficult it is for the system to be broken by an eavesdropper.

We have conducted the key/output test in our prototype for the files of the Calgary corpus and the Canterbury corpus. The estimated probabilities of change obtained in all the files are shown in Tables 13 and 14 respectively. Observe that the value of $\hat{p}$ is very close to 0.5 for all the files.

File name	$n_{1\min}$	$< n_1 <$	$n_{1\max}$
bib	9,725	10,088	10,275
book1	9,725	9,977	10,275
book2	9,725	9,983	10,275
geo	9,725	9,964	10,275
news	9,725	9,981	10,275
obj1	9,725	10,144	10,275
obj2	9,725	10,059	10,275
paper1	9,725	9,938	10,275
progc	9,725	10,040	10,275
progl	9,725	9,930	10,275
progp	9,725	9,974	10,275
trans	9,725	10,054	10,275

Table 1: Monobit test on files of the Calgary corpus.

File name	$n_{1\min}$	$< n_1 <$	$n_{1\max}$
alice29.txt	9,725	9,938	10,275
asyoulik.txt	9,725	10,045	10,275
cp.html	9,725	9,967	10,275
fields.c	9,725	9,921	10,275
grammar.lsp	9,725	10,033	10,275
kennedy.xls	9,725	9,948	10,275
lcet10.txt	9,725	9,956	10,275
plrabn12.txt	9,725	10,092	10,275
ptt5	9,725	10,005	10,275
sum	9,725	9,825	10,275
xargs.1	9,725	9,933	10,275

Table 2: Monobit test on files of the Canterbury corpus.

File name	$X_{3\min}$	$< X_3 <$	$X_{3\max}$
bib	2.16	15.42	46.17
book1	2.16	26.45	46.17
book2	2.16	20.89	46.17
geo	2.16	15.24	46.17
news	2.16	13.20	46.17
obj1	2.16	9.91	46.17
obj2	2.16	13.20	46.17
paper1	2.16	27.95	46.17
progc	2.16	10.21	46.17
progl	2.16	19.03	46.17
progp	2.16	11.56	46.17
trans	2.16	25.56	46.17

Table 3: Poker test on files of the Calgary corpus, where $m = 4$.

File name	$X_{3\min}$	$< X_3 <$	$X_{3\max}$
alice29.txt	2.16	15.53	46.17
asyoulik.txt	2.16	12.08	46.17
cp.html	2.16	24.74	46.17
fields.c	2.16	15.65	46.17
grammar.lsp	2.16	8.67	46.17
kennedy.xls	2.16	5.71	46.17
lcet10.txt	2.16	15.96	46.17
plrabn12.txt	2.16	12.74	46.17
ptt5	2.16	18.53	46.17
sum	2.16	25.79	46.17
xargs.1	2.16	14.65	46.17

Table 4: Poker test on files of the Canterbury corpus, where $m = 4$.

File name	ℓ_{run}	$B_i/G_{i\text{min}}$	$< G_i$	$B_i <$	$B_i/G_{i\text{max}}$
bib	1	2,315	2,532	2,477	2,685
	2	1,114	1,293	1,299	1,386
	3	527	643	666	723
	4	240	287	289	384
	5	103	145	164	209
	6	103	141	146	209
book1	1	2,315	2,590	2,592	2,685
	2	1,114	1,237	1,277	1,386
	3	527	649	616	723
	4	240	312	293	384
	5	103	147	150	209
	6	103	148	155	209
book2	1	2,315	2,496	2,476	2,685
	2	1,114	1,238	1,288	1,386
	3	527	652	611	723
	4	240	308	321	384
	5	103	167	157	209
	6	103	145	152	209
geo	1	2,315	2,555	2,619	2,685
	2	1,114	1,288	1,248	1,386
	3	527	632	609	723
	4	240	317	304	384
	5	103	154	155	209
	6	103	139	149	209
news	1	2,315	2,486	2,525	2,685
	2	1,114	1,271	1,256	1,386
	3	527	661	624	723
	4	240	313	326	384
	5	103	161	156	209
	6	103	138	142	209
obj1	1	2,315	2,504	2,421	2,685
	2	1,114	1,252	1,234	1,386
	3	527	599	660	723
	4	240	308	315	384
	5	103	141	155	209
	6	103	158	176	209

Table 5: Runs test on files of the Calgary corpus.

File name	ℓ_{run}	$B_i/G_{i\min}$	$< G_i$	$B_i <$	$B_i/G_{i\max}$
obj2	1	2,315	2,472	2,471	2,685
	2	1,114	1,234	1,251	1,386
	3	527	618	585	723
	4	240	360	318	384
	5	103	140	164	209
	6	103	144	178	209
paper1	1	2,315	2,500	2,506	2,685
	2	1,114	1,280	1,258	1,386
	3	527	559	647	723
	4	240	340	294	384
	5	103	181	155	209
	6	103	147	147	209
progc	1	2,315	2,463	2,430	2,685
	2	1,114	1,237	1,245	1,386
	3	527	614	641	723
	4	240	334	327	384
	5	103	147	137	209
	6	103	154	168	209
progl	1	2,315	2,401	2,447	2,685
	2	1,114	1,198	1,229	1,386
	3	527	668	600	723
	4	240	338	315	384
	5	103	154	170	209
	6	103	166	163	209
progp	1	2,315	2,541	2,557	2,685
	2	1,114	1,246	1,276	1,386
	3	527	651	626	723
	4	240	315	287	384
	5	103	166	148	209
	6	103	133	158	209
trans	1	2,315	2,522	2,498	2,685
	2	1,114	1,268	1,240	1,386
	3	527	581	653	723
	4	240	331	320	384
	5	103	165	137	209
	6	103	144	163	209

Table 6: Runs test on files of the Calgary corpus.

File name	ℓ_{run}	$B_i/G_{i\min}$	$< G_i$	$B_i <$	$B_i/G_{i\max}$
alice29.txt	1	2,315	2,482	2,495	2,685
	2	1,114	1,217	1,228	1,386
	3	527	630	620	723
	4	240	305	300	384
	5	103	161	164	209
	6	103	170	158	209
asyoulik.txt	1	2,315	2,551	2,490	2,685
	2	1,114	1,203	1,209	1,386
	3	527	593	662	723
	4	240	309	307	384
	5	103	180	164	209
	6	103	152	156	209
cp.html	1	2,315	2,520	2,422	2,685
	2	1,114	1,171	1,306	1,386
	3	527	619	624	723
	4	240	327	311	384
	5	103	163	158	209
	6	103	169	147	209
fields.c	1	2,315	2,522	2,530	2,685
	2	1,114	1,209	1,214	1,386
	3	527	622	624	723
	4	240	319	325	384
	5	103	146	164	209
	6	103	179	139	209
grammar.lsp	1	2,315	2,566	2,515	2,685
	2	1,114	1,215	1,251	1,386
	3	527	637	612	723
	4	240	282	316	384
	5	103	130	151	209
	6	103	183	167	209
kennedy.xls	1	2,315	2,498	2,517	2,685
	2	1,114	1,245	1,245	1,386
	3	527	643	647	723
	4	240	315	289	384
	5	103	145	164	209
	6	103	163	147	209

Table 7: Runs test on files of the Canterbury corpus.

File name	ℓ_{run}	$B_i/G_{i\min}$	$< G_i$	$B_i <$	$B_i/G_{i\max}$
lcet10.txt	1	2,315	2,446	2,480	2,685
	2	1,114	1,279	1,251	1,386
	3	527	598	621	723
	4	240	306	306	384
	5	103	187	156	209
	6	103	155	156	209
plrabn12.txt	1	2,315	2,534	2,505	2,685
	2	1,114	1,240	1,242	1,386
	3	527	599	606	723
	4	240	321	300	384
	5	103	168	168	209
	6	103	137	178	209
ptt5	1	2,315	2,502	2,442	2,685
	2	1,114	1,185	1,265	1,386
	3	527	605	622	723
	4	240	359	321	384
	5	103	148	158	209
	6	103	164	154	209
sum	1	2,315	2,540	2,583	2,685
	2	1,114	1,206	1,223	1,386
	3	527	596	619	723
	4	240	337	308	384
	5	103	162	143	209
	6	103	178	143	209
xargs.1	1	2,315	2,447	2,517	2,685
	2	1,114	1,239	1,186	1,386
	3	527	649	641	723
	4	240	327	309	384
	5	103	150	168	209
	6	103	160	151	209

Table 8: Runs test on files of the Canterbury corpus.

File name	Max. run length	Runs ≥ 26
bib	18	0
book1	14	0
book2	14	0
geo	13	0
news	12	0
obj1	12	0
obj2	13	0
paper1	16	0
progc	14	0
progl	13	0
progp	16	0
trans	13	0

Table 9: Long runs test on files of the Calgary corpus.

File name	Max. run length	Runs ≥ 26
alice29.txt	14	0
asyoulik.txt	13	0
cp.html	16	0
fields.c	13	0
grammar.lsp	-	
kennedy.xls	12	0
lcet10.txt	16	0
plrabn12.txt	14	0
ptt5	14	0
sum	23	0
xargs.1	13	0

Table 10: Long run test on files of the Canterbury corpus.

File name	$\hat{f}_{0\|0}$	$\hat{f}_{1\|1}$	$d(\hat{\mathcal{F}}\,\mathcal{F}^*)$	χ^2	$P(\chi^2, 1)$
bib	0.498605	0.501850	0.00001074	0.00002148	99.63
book1	0.499809	0.499924	0.00000008	0.00000017	99.97
book2	0.500428	0.499971	0.00000037	0.00000073	99.93
geo	0.498950	0.500117	0.00000223	0.00000447	99.83
news	0.499583	0.500206	0.00000043	0.00000086	99.93
obj1	0.500562	0.502928	0.00001778	0.00003556	99.52
obj2	0.500526	0.500533	0.00000112	0.00000224	99.88
paper1	0.498496	0.498524	0.00000888	0.00001777	99.66
progc	0.500559	0.502490	0.00001303	0.00002605	99.59
progl	0.500949	0.502410	0.00001342	0.00002683	99.59
progp	0.498114	0.498904	0.00000951	0.00001903	99.65
trans	0.499271	0.498310	0.00000677	0.00001355	99.71

Table 11: First order Markovian Chi-square test of independence for the output of the prototype executed on files of the Calgary corpus.

File name	$\hat{f}_{0\|0}$	$\hat{f}_{1\|1}$	$d(\hat{\mathcal{F}}\,\mathcal{F}^*)$	χ^2	$P(\chi^2, 1)$
alice29.txt	0.498967	0.499199	0.00000342	0.00000683	99.79
asyoulik.txt	0.500073	0.500496	0.00000050	0.00000101	99.92
cp.html	0.501431	0.501390	0.00000796	0.00001592	99.68
fields.c	0.504239	0.497348	0.00005000	0.00003632	99.52
grammar.lsp	0.496727	0.498602	0.00002533	0.00005066	99.43
kennedy.xls	0.500649	0.500249	0.00000097	0.00000193	99.89
lcet10.txt	0.500234	0.499746	0.00000024	0.00000047	99.95
plrabn12.txt	0.499319	0.500018	0.00000093	0.00000186	99.89
ptt5	0.499553	0.500409	0.00000073	0.00000147	99.90
xargs.1	0.504894	0.502496	0.00006036	0.00012072	99.12

Table 12: First order Markovian Chi-square test of independence for the output of the prototype executed on files of the Canterbury corpus.

File name	$\hat{p}$
bib	0.49715
book1	0.49585
book2	0.49745
geo	0.4987
news	0.50095
obj1	0.50215
obj2	0.4994
paper1	0.49835
progc	0.50315
progl	0.50065
progp	0.4962
trans	0.4996

Table 13: Statistical independence test between the key and the output performed by modifying the *key* in a single bit on files of the Calgary corpus, where $\hat{p}$ is the estimated prob. of change.

File name	$\hat{p}$
alice29.txt	0.50485
asyoulik.txt	0.4981
cp.html	0.50515
fields.c	0.49515
grammar.lsp	0.50025
kennedy.xls	0.49925
lcet10.txt	0.50025
plrabn12.txt	0.5015
ptt5	0.50135
sum	0.50025
xargs.1	0.49835

Table 14: Statistical independence test between the key and the output performed by modifying the *key* in a single bit on files of the Canterbury corpus, where $\hat{p}$ is the estimated prob. of change.