Serpent Cipher

Final Report

Cryptography

Team Rikki-Tikki-Tavi

Authors:
Nicholas Sereni
Dan Grau
Karl Berger

Prof.:
Alan Kaminsky

February 8, 2013

Contents

1 Serpent Cipher

Example citation [Figueredo and Wolf, 2009].

1.1 Background

The Serpent cipher was designed by Ross Angerson, Eli Biham, and Lars Knudsen. It was created as candidate for the Advanced Encryption Standard. Based on AES requirements, it has a 128 bit block length and a 256 bit key length. It also supports keys sizes of 128 and 192 bits.

1.2 The Algorithm

Serpent splits the 128 bit block into four 32-bit words. There are 32 rounds. Each round uses a subkey generated from the user key. The user key does not have a size requirement, but it becomes fixed at 128, 192, or 256 bits. Padding is achieved by appending a "1" followed by "0" bits. The algorithm can be summarized as:

- An initial permutation
- 32 rounds consisting of:
  - key mixing operation
  - S-boxes
  - linear transformation (replaced by a a key mixing operation in the final round)
- A final permutation

2 Original Implementation

2.1 Description

2.2 Timing Results

All timing results were measured on the CS machine, Joplin.

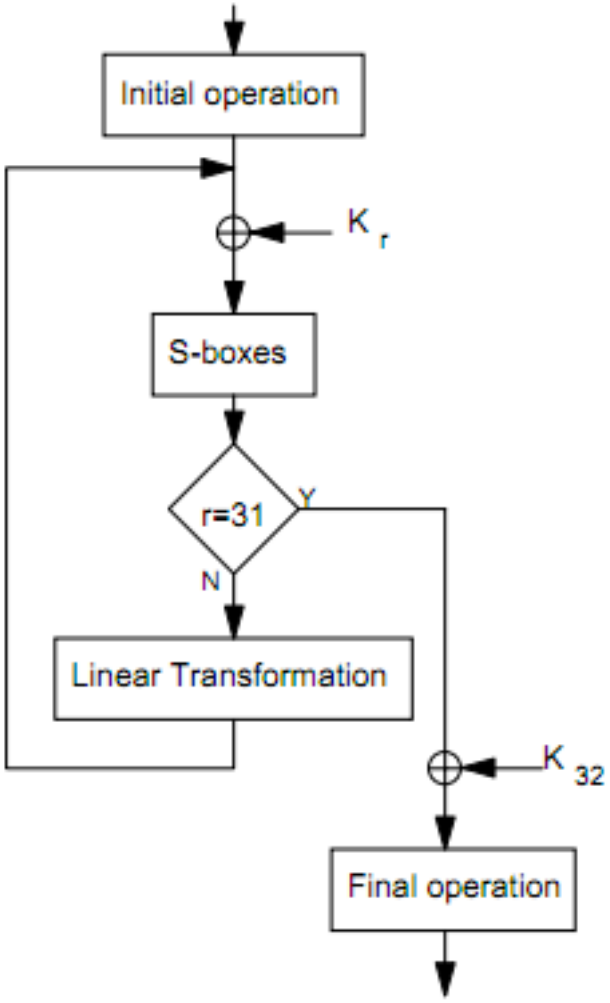

Figure 1: Block Diagram of the Encryption Process

2.2.1 Total Running Time with no JIT compiler

$ time java -Xint Serpent 1
49672ba898d98df95019180445491089
real 0m0.135s
user 0m0.040s
sys 0m0.024s

2.2.2 Source Code Line Level Profiling with Runtime over 100 Seconds

$ time java -Xint -agentlib:hprof=cpu=samples,depth=10 Serpent 100000
d3f68d0623563be822d68dde8f4ad282
Dumping CPU usage by sampling running threads ... done.
real 2m36.683s
user 2m36.774s
sys 0m0.524s

rank	self	accum	count	trace	method
1	6.77	% 6.77	% 1039	300032	Serpent.linearTransform
2	6.65	% 13.42	% 1021	300031	Serpent.initPermutation
3	6.55	% 19.97	% 1005	300050	Serpent.sBox
4	6.17	% 26.14	% 947	300029	Serpent.getRoundKey
5	5.95	% 32.09	% 913	300037	Serpent.initPermutation
6	4.46	% 36.56	% 685	300044	Serpent.sBox
7	2.16	% 38.71	% 331	300047	Serpent.getRoundKey
8	2.16	% 40.87	% 331	300069	Serpent.finalPermutation
9	2.14	% 43.01	% 329	300028	Serpent.finalPermutation
10	2.12	% 45.14	% 326	300039	Serpent.initPermutation
11	2.12	% 47.26	% 325	300054	Serpent.finalPermutation
12	1.99	% 49.25	% 306	300038	Serpent.finalPermutation
13	1.94	% 51.19	% 297	300043	Serpent.finalPermutation
14	1.92	% 53.10	% 294	300035	Serpent.initPermutation
15	1.90	% 55.00	% 292	300063	Serpent.finalPermutation
16	1.86	% 56.86	% 285	300048	Serpent.initPermutation
17	1.77	% 58.63	% 272	300061	Serpent.initPermutation
18	1.70	% 60.33	% 261	300073	Serpent.setKey
19	1.63	% 61.96	% 250	300027	Serpent.initPermutation
20	1.48	% 63.44	% 227	300026	Serpent.initPermutation
21	1.48	% 64.92	% 227	300030	Serpent.initPermutation
22	1.47	% 66.39	% 225	300112	Serpent.initPermutation
23	1.41	% 67.80	% 217	300060	Serpent.initPermutation
24	1.35	% 69.15	% 207	300046	Serpent.initPermutation
25	1.29	% 70.44	% 198	300040	Serpent.finalPermutation

26	1.15	% 71.60	% 177	300045	Serpent.initPermutation
27	1.11	% 72.70	% 170	300057	Serpent.finalPermutation
28	1.11	% 73.81	% 170	300103	Serpent.initPermutation
29	0.92	% 74.73	% 141	300034	Serpent.finalPermutation
30	0.87	% 75.60	% 134	300068	Serpent.setKey
31	0.87	% 76.48	% 134	300071	Serpent.finalPermutation
32	0.85	% 77.33	% 131	300067	Serpent.initPermutation
33	0.68	% 78.01	% 105	300049	Serpent.initPermutation
34	0.68	% 78.69	% 104	300097	Serpent.initPermutation
35	0.64	% 79.33	% 98	300070	Serpent.encrypt
36	0.63	% 79.96	% 96	300124	Serpent.finalPermutation
37	0.60	% 80.56	% 92	300084	Serpent.initPermutation
38	0.54	% 81.10	% 83	300094	Serpent.finalPermutation
39	0.53	% 81.63	% 82	300053	Serpent.initPermutation
40	0.53	% 82.16	% 82	300055	Serpent.initPermutation
41	0.52	% 82.69	% 80	300080	Serpent.initPermutation
42	0.51	% 83.20	% 79	300064	Serpent.initPermutation
43	0.51	% 83.71	% 78	300132	Serpent.initPermutation
44	0.50	% 84.21	% 77	300096	Serpent.initPermutation
45	0.50	% 84.71	% 76	300078	Serpent.initPermutation
46	0.46	% 85.17	% 71	300154	Serpent.initPermutation
47	0.43	% 85.60	% 66	300041	Serpent.initPermutation
48	0.37	% 85.97	% 57	300056	Serpent.initPermutation
49	0.37	% 86.34	% 57	300058	Serpent.initPermutation
50	0.36	% 86.70	% 55	300059	Serpent.initPermutation
51	0.31	% 87.01	% 48	300116	Serpent.setKey
52	0.31	% 87.33	% 48	300123	Serpent.getRoundKey
53	0.31	% 87.63	% 47	300169	Serpent.getRoundKey
54	0.29	% 87.92	% 44	300076	Serpent.finalPermutation
55	0.25	% 88.17	% 38	300036	Serpent.getRoundKey
56	0.24	% 88.41	% 37	300140	Serpent.getRoundKey
57	0.24	% 88.65	% 37	300164	Serpent.getRoundKey
58	0.22	% 88.87	% 34	300066	Serpent.initPermutation
59	0.20	% 89.07	% 31	300144	Serpent.encrypt

60	0.20	% 89.27	% 30	300147	Serpent.getRoundKey
61	0.19	% 89.46	% 29	300095	Serpent.finalPermutation
62	0.19	% 89.65	% 29	300126	Serpent.getRoundKey
63	0.18	% 89.83	% 28	300065	Serpent.getRoundKey
64	0.16	% 89.99	% 25	300090	Serpent.getRoundKey
65	0.16	% 90.15	% 24	300042	Serpent.getRoundKey
66	0.16	% 90.30	% 24	300136	Serpent.encrypt
67	0.15	% 90.45	% 23	300106	Serpent.getRoundKey
68	0.15	% 90.60	% 23	300130	java.nio.Bits.putIntB
69	0.14	% 90.75	% 22	300166	Serpent.getRoundKey
70	0.14	% 90.88	% 21	300214	Serpent.getRoundKey
71	0.13	% 91.01	% 20	300051	Serpent.getRoundKey
72	0.13	% 91.14	% 20	300122	Serpent.getRoundKey
73	0.13	% 91.27	% 20	300135	Serpent.getRoundKey
74	0.13	% 91.40	% 20	300221	Serpent.getRoundKey
75	0.12	% 91.53	% 19	300105	Serpent.getRoundKey
76	0.12	% 91.65	% 19	300137	Serpent.getRoundKey
77	0.12	% 91.78	% 19	300175	java.nio.Buffer.nextPutIndex
78	0.12	% 91.89	% 18	300111	Serpent.getRoundKey
79	0.12	% 92.01	% 18	300247	Serpent.getRoundKey
80	0.11	% 92.12	% 17	300127	Serpent.finalPermutation
81	0.11	% 92.23	% 17	300153	java.nio.Bits.int3
82	0.10	% 92.34	% 16	300052	Serpent.encrypt
83	0.10	% 92.44	% 16	300089	java.nio.HeapByteBuffer.putInt
84	0.10	% 92.55	% 16	300117	java.nio.Buffer.nextPutIndex
85	0.10	% 92.65	% 16	300120	Serpent.initPermutation
86	0.10	% 92.75	% 16	300234	java.nio.Bits.putInt
87	0.10	% 92.85	% 15	300142	Serpent.getRoundKey
88	0.10	% 92.95	% 15	300152	java.nio.Bits.putIntB
89	0.10	% 93.05	% 15	300193	java.nio.Bits.int3
90	0.10	% 93.14	% 15	300195	java.nio.Bits.putIntB
91	0.10	% 93.24	% 15	300227	Serpent.finalPermutation
92	0.09	% 93.33	% 14	300072	java.nio.Bits.int1
93	0.09	% 93.42	% 14	300083	Serpent.sBox

94	0.09	% 93.52	% 14	300149	Serpent.getRoundKey
95	0.08	% 93.60	% 13	300082	Serpent.initPermutation
96	0.08	% 93.69	% 13	300121	Serpent.finalPermutation
97	0.08	% 93.77	% 13	300155	Serpent.finalPermutation
98	0.08	% 93.86	% 13	300200	java.nio.Buffer.nextPutIndex
99	0.08	% 93.94	% 13	300209	Serpent.getRoundKey
100	0.08	% 94.02	% 13	300222	java.nio.Buffer.nextPutIndex
101	0.08	% 94.11	% 13	300246	Serpent.getRoundKey
102	0.08	% 94.19	% 12	300113	java.nio.Buffer.nextPutIndex
103	0.08	% 94.27	% 12	300129	Serpent.finalPermutation
104	0.08	% 94.34	% 12	300159	Serpent.linearTransform
105	0.08	% 94.42	% 12	300176	Serpent.encrypt
106	0.08	% 94.50	% 12	300196	Serpent.initPermutation
107	0.08	% 94.58	% 12	300231	java.nio.HeapByteBuffer._put
108	0.08	% 94.66	% 12	300258	java.nio.Buffer.nextPutIndex
109	0.07	% 94.73	% 11	300033	Serpent.getRoundKey
110	0.07	% 94.80	% 11	300092	java.nio.Bits.int3
111	0.07	% 94.87	% 11	300146	java.nio.Bits.putIntB
112	0.07	% 94.94	% 11	300162	Serpent.getRoundKey
113	0.07	% 95.01	% 11	300217	java.nio.HeapByteBuffer._put
114	0.07	% 95.09	% 11	300219	java.nio.HeapByteBuffer._put
115	0.07	% 95.16	% 11	300225	java.nio.Bits.putIntB
116	0.07	% 95.23	% 11	300228	Serpent.getRoundKey
117	0.07	% 95.30	% 11	300235	Serpent.getRoundKey
118	0.07	% 95.37	% 10	300081	java.nio.Bits.int2
119	0.07	% 95.43	% 10	300108	java.nio.Bits.putInt
120	0.07	% 95.50	% 10	300151	java.nio.Buffer.nextPutIndex
121	0.07	% 95.56	% 10	300165	Serpent.getRoundKey
122	0.07	% 95.63	% 10	300172	java.nio.Bits.int2
123	0.07	% 95.69	% 10	300178	Serpent.getRoundKey
124	0.07	% 95.76	% 10	300206	Serpent.getRoundKey
125	0.06	% 95.82	% 9	300075	Serpent.initPermutation
126	0.06	% 95.88	% 9	300079	java.nio.Bits.putIntB
127	0.06	% 95.93	% 9	300100	java.nio.Bits.putIntB

128	0.06	% 95.99	% 9	300107	Serpent.initPermutation
129	0.06	% 96.05	% 9	300115	java.nio.HeapByteBuffer.ix
130	0.06	% 96.11	% 9	300118	Serpent.getRoundKey
131	0.06	% 96.17	% 9	300128	java.nio.Bits.int3
132	0.06	% 96.23	% 9	300158	java.nio.HeapByteBuffer._put
133	0.06	% 96.29	% 9	300180	java.nio.HeapByteBuffer._put
134	0.06	% 96.34	% 9	300181	java.nio.Bits.int2
135	0.06	% 96.40	% 9	300184	java.nio.Bits.putIntB
136	0.06	% 96.46	% 9	300189	Serpent.initPermutation
137	0.06	% 96.52	% 9	300197	Serpent.finalPermutation
138	0.06	% 96.58	% 9	300202	Serpent.getRoundKey
139	0.06	% 96.64	% 9	300241	java.nio.HeapByteBuffer.putInt
140	0.06	% 96.70	% 9	300260	Serpent.finalPermutation
141	0.05	% 96.75	% 8	300091	Serpent.encrypt
142	0.05	% 96.80	% 8	300099	java.nio.HeapByteBuffer.putInt
143	0.05	% 96.85	% 8	300109	java.nio.Buffer.nextPutIndex
144	0.05	% 96.90	% 8	300110	Serpent.finalPermutation
145	0.05	% 96.96	% 8	300114	Serpent.initPermutation
146	0.05	% 97.01	% 8	300133	java.nio.HeapByteBuffer.ix
147	0.05	% 97.06	% 8	300138	java.nio.Bits.putIntB
148	0.05	% 97.11	% 8	300157	Serpent.blockSize
149	0.05	% 97.17	% 8	300249	java.nio.Buffer.nextPutIndex
150	0.05	% 97.22	% 8	300252	java.nio.HeapByteBuffer._put
151	0.05	% 97.26	% 7	300074	java.nio.Bits.int2
152	0.05	% 97.31	% 7	300119	Serpent.encrypt
153	0.05	% 97.35	% 7	300139	Serpent.getRoundKey
154	0.05	% 97.40	% 7	300141	Serpent.initPermutation
155	0.05	% 97.45	% 7	300145	java.nio.Bits.putIntB
156	0.05	% 97.49	% 7	300156	Serpent.getRoundKey
157	0.05	% 97.54	% 7	300167	Serpent.encrypt
158	0.05	% 97.58	% 7	300170	Serpent.linearTransform
159	0.05	% 97.63	% 7	300173	java.nio.HeapByteBuffer._put
160	0.05	% 97.67	% 7	300179	Serpent.initPermutation
161	0.05	% 97.72	% 7	300188	java.nio.HeapByteBuffer.ix

162	0.05	% 97.76	% 7	300194	java.nio.Buffer.nextPutIndex
163	0.05	% 97.81	% 7	300199	Serpent.encrypt
164	0.05	% 97.86	% 7	300210	java.nio.HeapByteBuffer.ix
165	0.05	% 97.90	% 7	300229	java.nio.Bits.putIntB
166	0.05	% 97.95	% 7	300270	Serpent.initPermutation
167	0.04	% 97.99	% 6	300093	Serpent.getRoundKey
168	0.04	% 98.03	% 6	300101	java.nio.Bits.putIntB
169	0.04	% 98.06	% 6	300177	Serpent.getRoundKey
170	0.04	% 98.10	% 6	300182	Serpent.finalPermutation
171	0.04	% 98.14	% 6	300232	Serpent.initPermutation
172	0.04	% 98.18	% 6	300253	java.nio.HeapByteBuffer._put
173	0.04	% 98.22	% 6	300271	Serpent.sBox
174	0.03	% 98.25	% 5	300131	java.nio.Bits.putIntB
175	0.03	% 98.29	% 5	300163	java.nio.HeapByteBuffer.putInt
176	0.03	% 98.32	% 5	300168	java.nio.Bits.putIntB
177	0.03	% 98.35	% 5	300186	java.nio.Bits.int0
178	0.03	% 98.38	% 5	300208	Serpent.getRoundKey
179	0.03	% 98.42	% 5	300237	java.nio.Bits.putIntB
180	0.03	% 98.45	% 5	300245	java.nio.Buffer.nextPutIndex
181	0.03	% 98.48	% 5	300251	Serpent.getRoundKey
182	0.03	% 98.51	% 5	300265	Serpent.getRoundKey
183	0.03	% 98.55	% 5	300278	Serpent.linearTransform
184	0.03	% 98.58	% 5	300284	Serpent.getRoundKey
185	0.03	% 98.61	% 4	300085	Serpent.getRoundKey
186	0.03	% 98.63	% 4	300125	Serpent.initPermutation
187	0.03	% 98.66	% 4	300148	Serpent.initPermutation
188	0.03	% 98.68	% 4	300160	Serpent.getRoundKey
189	0.03	% 98.71	% 4	300187	java.nio.Bits.int0
190	0.03	% 98.74	% 4	300205	Serpent.getRoundKey
191	0.03	% 98.76	% 4	300213	java.nio.Bits.putIntB
192	0.03	% 98.79	% 4	300230	java.nio.HeapByteBuffer._put
193	0.03	% 98.81	% 4	300240	Serpent.getRoundKey
194	0.03	% 98.84	% 4	300255	Serpent.getRoundKey
195	0.03	% 98.87	% 4	300257	Serpent.getRoundKey

196	0.03	% 98.89	% 4	300261	Serpent.initPermutation
197	0.03	% 98.92	% 4	300266	java.nio.Bits.putIntB
198	0.03	% 98.94	% 4	300281	Serpent.encrypt
199	0.03	% 98.97	% 4	300288	Serpent.getRoundKey
200	0.02	% 98.99	% 3	300062	java.nio.HeapByteBuffer._put
201	0.02	% 99.01	% 3	300077	Serpent.initPermutation
202	0.02	% 99.03	% 3	300098	java.nio.Bits.int1
203	0.02	% 99.05	% 3	300150	java.nio.HeapByteBuffer._put
204	0.02	% 99.07	% 3	300183	Serpent.getRoundKey
205	0.02	% 99.09	% 3	300203	Serpent.getRoundKey
206	0.02	% 99.11	% 3	300211	Serpent.finalPermutation
207	0.02	% 99.13	% 3	300212	java.nio.Bits.int0
208	0.02	% 99.15	% 3	300223	Serpent.initPermutation
209	0.02	% 99.17	% 3	300226	Serpent.getRoundKey
210	0.02	% 99.19	% 3	300259	Serpent.getRoundKey
211	0.02	% 99.21	% 3	300285	Serpent.getRoundKey
212	0.02	% 99.22	% 3	300295	java.nio.Bits.putInt
213	0.02	% 99.24	% 3	300296	Serpent.getRoundKey
214	0.02	% 99.26	% 3	300300	Serpent.finalPermutation
215	0.02	% 99.28	% 3	300303	java.nio.HeapByteBuffer._put
216	0.01	% 99.30	% 2	300086	Serpent.initPermutation
217	0.01	% 99.31	% 2	300102	Serpent.initPermutation
218	0.01	% 99.32	% 2	300104	java.nio.HeapByteBuffer._put
219	0.01	% 99.34	% 2	300134	Serpent.initPermutation
220	0.01	% 99.35	% 2	300143	java.nio.Buffer.nextPutIndex
221	0.01	% 99.36	% 2	300191	Serpent.initPermutation
222	0.01	% 99.37	% 2	300215	Serpent.initPermutation
223	0.01	% 99.39	% 2	300216	Serpent.initPermutation
224	0.01	% 99.40	% 2	300224	java.nio.HeapByteBuffer._put
225	0.01	% 99.41	% 2	300239	Serpent.initPermutation
226	0.01	% 99.43	% 2	300243	Serpent.initPermutation
227	0.01	% 99.44	% 2	300244	Serpent.finalPermutation
228	0.01	% 99.45	% 2	300254	Serpent.setKey
229	0.01	% 99.47	% 2	300263	Serpent.initPermutation

230	0.01	% 99.48	% 2	300264	Serpent.linearTransform
231	0.01	% 99.49	% 2	300267	Serpent.linearTransform
232	0.01	% 99.50	% 2	300269	java.nio.Bits.int1
233	0.01	% 99.52	% 2	300273	Serpent.linearTransform
234	0.01	% 99.53	% 2	300274	Serpent.initPermutation
235	0.01	% 99.54	% 2	300276	Serpent.finalPermutation
236	0.01	% 99.56	% 2	300280	Serpent.getRoundKey
237	0.01	% 99.57	% 2	300282	Serpent.initPermutation
238	0.01	% 99.58	% 2	300290	java.nio.HeapByteBuffer._put
239	0.01	% 99.60	% 2	300292	Serpent.getRoundKey
240	0.01	% 99.61	% 2	300308	Serpent.linearTransform
241	0.01	% 99.62	% 2	300317	Serpent.initPermutation

CPU SAMPLES END

2.3 Source Code

3 Conclusion

References

[Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.