Date: Wed, 24 May 2000 17:34:03 +0100 (BST)
From: Sean Murphy <sean@dcs.rhbnc.ac.uk>
X-Sender: sean@platon.cs.rhbnc.ac.uk
To: AESround2@nist.gov
Subject: AES paper

We wish to submit the attached postscript file as an AES Round 2 comment. It contains a document discussed in the NESSIE project comments about the AES.

Sean Murphy

Differential Distributions for Twofish S-Boxes

Sean Murphy

Information Security Group,
Royal Holloway, University of London
Egham, Surrey TW20 0EX, U.K.

Abstract

This paper gives some results concerning the the probability distribtuins for simultaneous differentials across the same Twofish S-Box.

1 A Single Differential for an S-Box

Consider a Twofish S-Box [1] S-Box. For a given Twofish S-box (16-bit) subkey k, this defines a function $S_k : Z_2^8 \rightarrow Z_2^8$. The differential count for S_k for input difference a and output difference b ($a \rightarrow b$) is defined by

$$N_k(a,b) = \#\{x \in Z_2^8 | S_k(x) \oplus S_k(x \oplus a) \oplus b = 0\} \qquad [a, b \in Z_2^8].$$

The probability of the differential $a \rightarrow b$ is given by $2^{-8} N_k(a,b)$. Clearly, $N_k(a,0) = N_k(0,b) = 0$ for $a, b \neq 0$ with $N_k(0,0) = 2^8$. We consider $N_k(a,b)$ when $a, b \neq 0$.

Consider the quotient space $U_a = Z_2^8/\{0, a\}$, and define $W_x \in U_a$ to be the coset $\{x, x \oplus a\}$. We can now define $F : U_a \rightarrow Z_2^8$ by

$$F(W_x) = S_k(x) \oplus S_k(x \oplus a) \oplus b.$$

It is reasonable to regard F as a random function mapping uniformly into an 8-bit space, so the indicator function I_{W_x} for the event $F(W_x) = 0$ takes the value 1 with probability 2^{-8} and 0 with probability $1 - 2^{-8}$. Furthermore, to a very good approximation, I_{W_x} are independent random variables. Thus, summing over all 2^7 elements of U_a, we obtain

$$\sum_{W_x \in U_a} I_{W_x} \sim Bin(2^7, 2^{-8}) \approx Poi(1/2).$$

However, $N_k(a,b) = 2\sum_{W_x \in U_a} I_{W_x}$. Thus, if X is a $2 \cdot Poi(1/2)$ random variable, so

$$P(X = 2n) = \frac{e^{-\frac{1}{2}}\frac{1}{2}^n}{n!}, \qquad P(X = 2n+1) = 0, \qquad [n \geq 0],$$

then $N_k(a,b)$ has approximately the same distribution as X.

We have seen that for a fixed S-Box subkey k, $N_k(a,b)$ takes the value $2n$ with probability $P(X = 2n)$. However, we can regard $N_k(a,b)$ and $N_{k'}(a,b)$ as independent for $k \neq k'$. Thus, equivalently, we can say that $N_k(a,b)$ takes the value $2n$ for a proportion of $P(X = 2n)$ of the 2^{16} S-Box subkeys k. Probabilities for X are tabulated in the Appendix, and are in very close agreement with simulated distributions for $N_k(a,b)$.

2 Multiple Differentials for the same S-Box

To conduct a differential cryptanalysis of Twofish, we require a number of differentials $a_1 \to b_1, \cdots, a_l \to b_l$ to hold across an S-Box with the same S-Box subkey k. As $N_k(a_i, b_i)$ are essentially independent, the total count for all these differentials simultaneously is given by

$$M_k(a,b) = \prod_{i=1}^{l} N_k(a_i, b_i).$$

If $X_1, \cdots, X_l$ are independent $2 \cdot Poi(1/2)$ random variables (as discussed in the previous Section), then $M_k(a,b)$ has approximately the same distribution as $Y_l = \prod_{i=1}^{l} X_i$. Note that Y_l is 2^l times the product of l independent $Poi(1/2)$ random variables. As above, we can say that $M_k(a,b)$ takes the value $2^l n$ for a proportion of $P(Y_l = 2^l n)$ of the 2^{16} S-Box subkeys k. Probabilities for Y_l $(l = 2, \cdots, 5)$ are tabulated in the Appendix, and are in very close agreement with simulated distributions for $M_k(a,b)$. It is interesting to note that these distributions have many modes (ie. they do not decay monotonically). this is because the distributions are a product of a discrete (non-negative integer-valued) distribution.

In analysing Twofish, we may use exactly the same differential across the same S-Box simultaneously. Thus we may require the differentials $a_1 \to b_1, \cdots, a_{l-2} \to b_{l-2}$ to hold simultaneously with $a_{l-1} \to b_{l-1}$ *twice* across an S-Box with the same S-Box subkey k. The distribution is slightly different from that described above and is given by

$$M_k^*(a,b) = N_k^2(a_{l-1}, b_{l-1} \prod_{i=1}^{l-2} N_k(a_i, b_i).$$

As above, if $X_1, \cdots, X_{l-1}$ are independent $2 \cdot Poi(1/2)$ random variables (as discussed in the previous Section), then $M_k^*(a,b)$ has approximately the same distribution as $Y_l^* = X_l^2 \prod_{i=1}^{l-2} X_i$. Note that Y_l^* is 2^l times the product of $(l-2)$ independent $Poi(1/2)$ random variables and an independent squared $Poi(1/2)$ random variables. The values of Y_l^* are tabulated in the Appendix for $l = 2, \cdots, 5$. It is interesting to note the discrepancy between Y_l and Y_l^*. For example, the former distribution has expected value 1 and the latter 3. The latter distribution offers greater assistance to the cryptanalyst.

3 Conclusions

In this paper, we have given a theoretical derivation for the probabilities of several differentials to hold across a Twofish S-Box under the same S-Box subkey. Such differentials have been used in the analysis of Twofish [2]. We have also tabulated these results. These results can be used to calculate the proportion of S-Box subkeys for which a differential holds with a certain probability. This represents a step in the production of tools to assess the key-dependent S-Boxes of Twofish. It is possible to imagine the use of these tables as part of much more sophisticated tools.

References

[1] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. *Twofish: A 128-Bit Block Cipher*, AES Submission, 1999. `http://www.counterpane.com/twofish-paper.html`,

[2] S. Murphy and M.J.B. Robshaw *Key Dependent S-Boxes, Differential Cryptanalysis and Twofish*, submitted as an AES comment, 2000. `http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm`.

Appendix

Single Differential
Double Poisson
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion Subkeys	Expected Subkeys	Cumulative Subkeys	Cumulative Subkeys
0	$0 \cdot 2^{-7}$	0.606531	39749	1.000000	65536
2	$1 \cdot 2^{-7}$	0.303265	19874	0.393469	25786
4	$2 \cdot 2^{-7}$	0.075816	4968	0.090204	5911
6	$3 \cdot 2^{-7}$	0.012636	828	0.014388	942
8	$4 \cdot 2^{-7}$	0.001580	103	0.001752	114
10	$5 \cdot 2^{-7}$	0.000158	10	0.000172	11
12	$6 \cdot 2^{-7}$	0.000013	0	0.000014	0
14	$7 \cdot 2^{-7}$	0.000001	0	0.000001	0
16	$8 \cdot 2^{-7}$	0.000000	0	0.000000	0

2 Differentials
2-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-14}$	0.845182	55389	1.000000	65536
4	$1 \cdot 2^{-14}$	0.091970	6027	0.154818	10146
8	$2 \cdot 2^{-14}$	0.045985	3013	0.062848	4118
12	$3 \cdot 2^{-14}$	0.007664	502	0.016863	1105
16	$4 \cdot 2^{-14}$	0.006706	439	0.009199	602
20	$5 \cdot 2^{-14}$	0.000096	6	0.002493	163
24	$6 \cdot 2^{-14}$	0.001924	126	0.002397	157
28	$7 \cdot 2^{-14}$	0.000001	0	0.000473	31
32	$8 \cdot 2^{-14}$	0.000240	15	0.000473	30
36	$9 \cdot 2^{-14}$	0.000160	10	0.000233	15
40	$10 \cdot 2^{-14}$	0.000024	1	0.000074	4
44	$11 \cdot 2^{-14}$	0.000000	0	0.000050	3
48	$12 \cdot 2^{-14}$	0.000042	2	0.000050	3
52	$13 \cdot 2^{-14}$	0.000000	0	0.000008	0
56	$14 \cdot 2^{-14}$	0.000000	0	0.000008	0
60	$15 \cdot 2^{-14}$	0.000004	0	0.000008	0
64	$16 \cdot 2^{-14}$	0.000002	0	0.000004	0

3 Differentials
3-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-21}$	0.939084	61543	1.000000	65536
8	$1 \cdot 2^{-21}$	0.027891	1827	0.060916	3992
16	$2 \cdot 2^{-21}$	0.020918	1370	0.033025	2164
24	$3 \cdot 2^{-21}$	0.003486	228	0.012107	793
32	$4 \cdot 2^{-21}$	0.005665	371	0.008620	564
40	$5 \cdot 2^{-21}$	0.000044	2	0.002955	193
48	$6 \cdot 2^{-21}$	0.001747	114	0.002911	190
56	$7 \cdot 2^{-21}$	0.000000	0	0.001164	76
64	$8 \cdot 2^{-21}$	0.000654	42	0.001164	76
72	$9 \cdot 2^{-21}$	0.000145	9	0.000510	33
80	$10 \cdot 2^{-21}$	0.000022	1	0.000365	23
88	$11 \cdot 2^{-21}$	0.000000	0	0.000343	22
96	$12 \cdot 2^{-21}$	0.000256	16	0.000343	22
104	$13 \cdot 2^{-21}$	0.000000	0	0.000087	5
112	$14 \cdot 2^{-21}$	0.000000	0	0.000087	5
120	$15 \cdot 2^{-21}$	0.000004	0	0.000087	5
128	$16 \cdot 2^{-21}$	0.000030	1	0.000084	5
136	$17 \cdot 2^{-21}$	0.000000	0	0.000054	3
144	$18 \cdot 2^{-21}$	0.000037	2	0.000054	3
152	$19 \cdot 2^{-21}$	0.000000	0	0.000017	1
160	$20 \cdot 2^{-21}$	0.000003	0	0.000017	1
168	$21 \cdot 2^{-21}$	0.000000	0	0.000014	0
176	$22 \cdot 2^{-21}$	0.000000	0	0.000014	0
184	$23 \cdot 2^{-21}$	0.000000	0	0.000014	0
192	$24 \cdot 2^{-21}$	0.000009	0	0.000014	0
200	$25 \cdot 2^{-21}$	0.000000	0	0.000005	0
208	$26 \cdot 2^{-21}$	0.000000	0	0.000005	0
216	$27 \cdot 2^{-21}$	0.000002	0	0.000005	0
224	$28 \cdot 2^{-21}$	0.000000	0	0.000003	0
232	$29 \cdot 2^{-21}$	0.000000	0	0.000003	0
240	$30 \cdot 2^{-21}$	0.000001	0	0.000003	0
248	$31 \cdot 2^{-21}$	0.000000	0	0.000002	0
256	$32 \cdot 2^{-21}$	0.000001	0	0.000002	0
264	$33 \cdot 2^{-21}$	0.000000	0	0.000001	0
272	$34 \cdot 2^{-21}$	0.000000	0	0.000001	0
280	$35 \cdot 2^{-21}$	0.000000	0	0.000001	0
288	$36 \cdot 2^{-21}$	0.000001	0	0.000001	0

4 Differentials
4-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-28}$	0.976031	63965	1.000000	65536
16	$1 \cdot 2^{-28}$	0.008458	554	0.023969	1570
32	$2 \cdot 2^{-28}$	0.008458	554	0.015510	1016
48	$3 \cdot 2^{-28}$	0.001410	92	0.007052	462
64	$4 \cdot 2^{-28}$	0.003348	219	0.005642	369
80	$5 \cdot 2^{-28}$	0.000018	1	0.002294	150
96	$6 \cdot 2^{-28}$	0.001059	69	0.002276	149
112	$7 \cdot 2^{-28}$	0.000000	0	0.001218	79
128	$8 \cdot 2^{-28}$	0.000661	43	0.001218	79
144	$9 \cdot 2^{-28}$	0.000088	5	0.000557	36
160	$10 \cdot 2^{-28}$	0.000013	0	0.000469	30
176	$11 \cdot 2^{-28}$	0.000000	0	0.000455	29
192	$12 \cdot 2^{-28}$	0.000287	18	0.000455	29
208	$13 \cdot 2^{-28}$	0.000000	0	0.000168	11
224	$14 \cdot 2^{-28}$	0.000000	0	0.000168	11
240	$15 \cdot 2^{-28}$	0.000002	0	0.000168	11
256	$16 \cdot 2^{-28}$	0.000067	4	0.000166	10
272	$17 \cdot 2^{-28}$	0.000000	0	0.000098	6
288	$18 \cdot 2^{-28}$	0.000044	2	0.000098	6
304	$19 \cdot 2^{-28}$	0.000000	0	0.000054	3
320	$20 \cdot 2^{-28}$	0.000004	0	0.000054	3
336	$21 \cdot 2^{-28}$	0.000000	0	0.000050	3
352	$22 \cdot 2^{-28}$	0.000000	0	0.000050	3
368	$23 \cdot 2^{-28}$	0.000000	0	0.000050	3
384	$24 \cdot 2^{-28}$	0.000033	2	0.000050	3
400	$25 \cdot 2^{-28}$	0.000000	0	0.000017	1
416	$26 \cdot 2^{-28}$	0.000000	0	0.000017	1
432	$27 \cdot 2^{-28}$	0.000002	0	0.000017	1
448	$28 \cdot 2^{-28}$	0.000000	0	0.000015	0
464	$29 \cdot 2^{-28}$	0.000000	0	0.000015	0
480	$30 \cdot 2^{-28}$	0.000001	0	0.000015	0
496	$31 \cdot 2^{-28}$	0.000000	0	0.000014	0
512	$32 \cdot 2^{-28}$	0.000003	0	0.000014	0
528	$33 \cdot 2^{-28}$	0.000000	0	0.000010	0
544	$34 \cdot 2^{-28}$	0.000000	0	0.000010	0
560	$35 \cdot 2^{-28}$	0.000000	0	0.000010	0
576	$36 \cdot 2^{-28}$	0.000007	0	0.000010	0

5 Differentials
5-fold Double Poisson Product
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-35}$	0.990569	64917	1.000000	65536
32	$1 \cdot 2^{-35}$	0.002565	168	0.009431	618
64	$2 \cdot 2^{-35}$	0.003206	210	0.006866	449
96	$3 \cdot 2^{-35}$	0.000534	35	0.003660	239
128	$4 \cdot 2^{-35}$	0.001670	109	0.003125	204
160	$5 \cdot 2^{-35}$	0.000007	0	0.001455	95
192	$6 \cdot 2^{-35}$	0.000535	35	0.001449	94
224	$7 \cdot 2^{-35}$	0.000000	0	0.000914	59
256	$8 \cdot 2^{-35}$	0.000468	30	0.000914	59
288	$9 \cdot 2^{-35}$	0.000045	2	0.000446	29
320	$10 \cdot 2^{-35}$	0.000007	0	0.000402	26
352	$11 \cdot 2^{-35}$	0.000000	0	0.000395	25
384	$12 \cdot 2^{-35}$	0.000212	13	0.000395	25
416	$13 \cdot 2^{-35}$	0.000000	0	0.000183	11
448	$14 \cdot 2^{-35}$	0.000000	0	0.000183	11
480	$15 \cdot 2^{-35}$	0.000001	0	0.000183	11
512	$16 \cdot 2^{-35}$	0.000076	4	0.000182	11
544	$17 \cdot 2^{-35}$	0.000000	0	0.000106	6
576	$18 \cdot 2^{-35}$	0.000033	2	0.000106	6
608	$19 \cdot 2^{-35}$	0.000000	0	0.000072	4
640	$20 \cdot 2^{-35}$	0.000003	0	0.000072	4
672	$21 \cdot 2^{-35}$	0.000000	0	0.000070	4
704	$22 \cdot 2^{-35}$	0.000000	0	0.000070	4
736	$23 \cdot 2^{-35}$	0.000000	0	0.000070	4
768	$24 \cdot 2^{-35}$	0.000042	2	0.000070	4
800	$25 \cdot 2^{-35}$	0.000000	0	0.000028	1
832	$26 \cdot 2^{-35}$	0.000000	0	0.000028	1
864	$27 \cdot 2^{-35}$	0.000002	0	0.000028	1
896	$28 \cdot 2^{-35}$	0.000000	0	0.000026	1
928	$29 \cdot 2^{-35}$	0.000000	0	0.000026	1
960	$30 \cdot 2^{-35}$	0.000001	0	0.000026	1
992	$31 \cdot 2^{-35}$	0.000000	0	0.000025	1
1024	$32 \cdot 2^{-35}$	0.000007	0	0.000025	1
1056	$33 \cdot 2^{-35}$	0.000000	0	0.000018	1
1088	$34 \cdot 2^{-35}$	0.000000	0	0.000018	1
1120	$35 \cdot 2^{-35}$	0.000000	0	0.000018	1
1152	$36 \cdot 2^{-35}$	0.000009	0	0.000018	1

2 Differentials (Including One Repeated)
Squared Double Poison
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-14}$	0.606531	39749	1.000000	65536
4	$1 \cdot 2^{-14}$	0.303265	19874	0.393469	25786
8	$2 \cdot 2^{-14}$	0.000000	0	0.090204	5911
12	$3 \cdot 2^{-14}$	0.000000	0	0.090204	5911
16	$4 \cdot 2^{-14}$	0.075816	4968	0.090204	5911
20	$5 \cdot 2^{-14}$	0.000000	0	0.014388	942
24	$6 \cdot 2^{-14}$	0.000000	0	0.014388	942
28	$7 \cdot 2^{-14}$	0.000000	0	0.014388	942
32	$8 \cdot 2^{-14}$	0.000000	0	0.014388	942
36	$9 \cdot 2^{-14}$	0.012636	828	0.014388	942
40	$10 \cdot 2^{-14}$	0.000000	0	0.001752	114
44	$11 \cdot 2^{-14}$	0.000000	0	0.001752	114
48	$12 \cdot 2^{-14}$	0.000000	0	0.001752	114
52	$13 \cdot 2^{-14}$	0.000000	0	0.001752	114
56	$14 \cdot 2^{-14}$	0.000000	0	0.001752	114
60	$15 \cdot 2^{-14}$	0.000000	0	0.001752	114
64	$16 \cdot 2^{-14}$	0.001580	103	0.001752	114
68	$17 \cdot 2^{-14}$	0.000000	0	0.000172	11
72	$18 \cdot 2^{-14}$	0.000000	0	0.000172	11
76	$19 \cdot 2^{-14}$	0.000000	0	0.000172	11
80	$20 \cdot 2^{-14}$	0.000000	0	0.000172	11
84	$21 \cdot 2^{-14}$	0.000000	0	0.000172	11
88	$22 \cdot 2^{-14}$	0.000000	0	0.000172	11
92	$23 \cdot 2^{-14}$	0.000000	0	0.000172	11
96	$24 \cdot 2^{-14}$	0.000000	0	0.000172	11
100	$25 \cdot 2^{-14}$	0.000158	10	0.000172	11
104	$26 \cdot 2^{-14}$	0.000000	0	0.000014	0
108	$27 \cdot 2^{-14}$	0.000000	0	0.000014	0
112	$28 \cdot 2^{-14}$	0.000000	0	0.000014	0
116	$29 \cdot 2^{-14}$	0.000000	0	0.000014	0
120	$30 \cdot 2^{-14}$	0.000000	0	0.000014	0
124	$31 \cdot 2^{-14}$	0.000000	0	0.000014	0
128	$32 \cdot 2^{-14}$	0.000000	0	0.000014	0
132	$33 \cdot 2^{-14}$	0.000000	0	0.000014	0
136	$34 \cdot 2^{-14}$	0.000000	0	0.000014	0
140	$35 \cdot 2^{-14}$	0.000000	0	0.000014	0
144	$36 \cdot 2^{-14}$	0.000013	0	0.000014	0

3 Differentials (Including One Repeated)
Product of Double Poisson & Squared Double Poison
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-21}$	0.845182	55389	1.000000	65536
8	$1 \cdot 2^{-21}$	0.091970	6027	0.154818	10146
16	$2 \cdot 2^{-21}$	0.022992	1506	0.062848	4118
24	$3 \cdot 2^{-21}$	0.003832	251	0.039856	2611
32	$4 \cdot 2^{-21}$	0.023471	1538	0.036024	2360
40	$5 \cdot 2^{-21}$	0.000048	3	0.012552	822
48	$6 \cdot 2^{-21}$	0.000004	0	0.012504	819
56	$7 \cdot 2^{-21}$	0.000000	0	0.012500	819
64	$8 \cdot 2^{-21}$	0.005748	376	0.012500	819
72	$9 \cdot 2^{-21}$	0.003832	251	0.006752	442
80	$10 \cdot 2^{-21}$	0.000000	0	0.002920	191
88	$11 \cdot 2^{-21}$	0.000000	0	0.002920	191
96	$12 \cdot 2^{-21}$	0.000958	62	0.002920	191
104	$13 \cdot 2^{-21}$	0.000000	0	0.001962	128
112	$14 \cdot 2^{-21}$	0.000000	0	0.001962	128
120	$15 \cdot 2^{-21}$	0.000000	0	0.001962	128
128	$16 \cdot 2^{-21}$	0.000599	39	0.001962	128
136	$17 \cdot 2^{-21}$	0.000000	0	0.001363	89
144	$18 \cdot 2^{-21}$	0.000958	62	0.001363	89
152	$19 \cdot 2^{-21}$	0.000000	0	0.000405	26
160	$20 \cdot 2^{-21}$	0.000012	0	0.000405	26
168	$21 \cdot 2^{-21}$	0.000000	0	0.000393	25
176	$22 \cdot 2^{-21}$	0.000000	0	0.000393	25
184	$23 \cdot 2^{-21}$	0.000000	0	0.000393	25
192	$24 \cdot 2^{-21}$	0.000001	0	0.000393	25
200	$25 \cdot 2^{-21}$	0.000048	3	0.000392	25
208	$26 \cdot 2^{-21}$	0.000000	0	0.000344	22
216	$27 \cdot 2^{-21}$	0.000160	10	0.000344	22
224	$28 \cdot 2^{-21}$	0.000000	0	0.000185	12
232	$29 \cdot 2^{-21}$	0.000000	0	0.000185	12
240	$30 \cdot 2^{-21}$	0.000000	0	0.000185	12
248	$31 \cdot 2^{-21}$	0.000000	0	0.000185	12
256	$32 \cdot 2^{-21}$	0.000120	7	0.000185	12
264	$33 \cdot 2^{-21}$	0.000000	0	0.000065	4
272	$34 \cdot 2^{-21}$	0.000000	0	0.000065	4
280	$35 \cdot 2^{-21}$	0.000000	0	0.000065	4
288	$36 \cdot 2^{-21}$	0.000024	1	0.000065	4

4 Differentials (Including One Repeated)
Product of 2-fold Double Poisson & Squared Double Poison
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-28}$	0.939081	61543	1.000000	65536
16	$1 \cdot 2^{-28}$	0.027891	1827	0.060919	3992
32	$2 \cdot 2^{-28}$	0.013946	913	0.033027	2164
48	$3 \cdot 2^{-28}$	0.002324	152	0.019082	1250
64	$4 \cdot 2^{-28}$	0.009007	590	0.016757	1098
80	$5 \cdot 2^{-28}$	0.000029	1	0.007751	507
96	$6 \cdot 2^{-28}$	0.000583	38	0.007722	506
112	$7 \cdot 2^{-28}$	0.000000	0	0.007138	467
128	$8 \cdot 2^{-28}$	0.003559	233	0.007138	467
144	$9 \cdot 2^{-28}$	0.001211	79	0.003579	234
160	$10 \cdot 2^{-28}$	0.000007	0	0.002369	155
176	$11 \cdot 2^{-28}$	0.000000	0	0.002361	154
192	$12 \cdot 2^{-28}$	0.000594	38	0.002361	154
208	$13 \cdot 2^{-28}$	0.000000	0	0.001768	115
224	$14 \cdot 2^{-28}$	0.000000	0	0.001768	115
240	$15 \cdot 2^{-28}$	0.000001	0	0.001768	115
256	$16 \cdot 2^{-28}$	0.000654	42	0.001766	115
272	$17 \cdot 2^{-28}$	0.000000	0	0.001112	72
288	$18 \cdot 2^{-28}$	0.000581	38	0.001112	72
304	$19 \cdot 2^{-28}$	0.000000	0	0.000531	34
320	$20 \cdot 2^{-28}$	0.000007	0	0.000531	34
336	$21 \cdot 2^{-28}$	0.000000	0	0.000523	34
352	$22 \cdot 2^{-28}$	0.000000	0	0.000523	34
368	$23 \cdot 2^{-28}$	0.000000	0	0.000523	34
384	$24 \cdot 2^{-28}$	0.000146	9	0.000523	34
400	$25 \cdot 2^{-28}$	0.000015	0	0.000377	24
416	$26 \cdot 2^{-28}$	0.000000	0	0.000363	23
432	$27 \cdot 2^{-28}$	0.000097	6	0.000363	23
448	$28 \cdot 2^{-28}$	0.000000	0	0.000266	17
464	$29 \cdot 2^{-28}$	0.000000	0	0.000266	17
480	$30 \cdot 2^{-28}$	0.000000	0	0.000266	17
496	$31 \cdot 2^{-28}$	0.000000	0	0.000266	17
512	$32 \cdot 2^{-28}$	0.000091	5	0.000266	17
528	$33 \cdot 2^{-28}$	0.000000	0	0.000175	11
544	$34 \cdot 2^{-28}$	0.000000	0	0.000175	11
560	$35 \cdot 2^{-28}$	0.000000	0	0.000175	11
576	$36 \cdot 2^{-28}$	0.000098	6	0.000175	11

5 Differentials (Including One Repeated)
Product of 3-fold Double Poisson & Squared Double Poison
Parameter $\frac{1}{2}$

Differential Count	Differential Probability	Proportion of Subkeys	Expected No of 2^{16} Subkeys	Cumulative Proportion Subkeys	Cumulative No of 2^{16} Subkeys
0	$0 \cdot 2^{-35}$	0.976021	63964	1.000000	65536
32	$1 \cdot 2^{-35}$	0.008458	554	0.023979	1571
64	$2 \cdot 2^{-35}$	0.006344	415	0.015521	1017
96	$3 \cdot 2^{-35}$	0.001057	69	0.009177	601
128	$4 \cdot 2^{-35}$	0.003833	251	0.008120	532
160	$5 \cdot 2^{-35}$	0.000013	0	0.004287	280
192	$6 \cdot 2^{-35}$	0.000530	34	0.004274	280
224	$7 \cdot 2^{-35}$	0.000000	0	0.003744	245
256	$8 \cdot 2^{-35}$	0.001784	116	0.003744	245
288	$9 \cdot 2^{-35}$	0.000396	25	0.001960	128
320	$10 \cdot 2^{-35}$	0.000007	0	0.001563	102
352	$11 \cdot 2^{-35}$	0.000000	0	0.001557	102
384	$12 \cdot 2^{-35}$	0.000342	22	0.001557	102
416	$13 \cdot 2^{-35}$	0.000000	0	0.001215	79
448	$14 \cdot 2^{-35}$	0.000000	0	0.001215	79
480	$15 \cdot 2^{-35}$	0.000001	0	0.001215	79
512	$16 \cdot 2^{-35}$	0.000483	31	0.001214	79
544	$17 \cdot 2^{-35}$	0.000000	0	0.000731	47
576	$18 \cdot 2^{-35}$	0.000275	18	0.000731	47
608	$19 \cdot 2^{-35}$	0.000000	0	0.000456	29
640	$20 \cdot 2^{-35}$	0.000004	0	0.000456	29
672	$21 \cdot 2^{-35}$	0.000000	0	0.000451	29
704	$22 \cdot 2^{-35}$	0.000000	0	0.000451	29
736	$23 \cdot 2^{-35}$	0.000000	0	0.000451	29
768	$24 \cdot 2^{-35}$	0.000135	8	0.000451	29
800	$25 \cdot 2^{-35}$	0.000004	0	0.000316	20
832	$26 \cdot 2^{-35}$	0.000000	0	0.000312	20
864	$27 \cdot 2^{-35}$	0.000045	2	0.000312	20
896	$28 \cdot 2^{-35}$	0.000000	0	0.000267	17
928	$29 \cdot 2^{-35}$	0.000000	0	0.000267	17
960	$30 \cdot 2^{-35}$	0.000000	0	0.000267	17
992	$31 \cdot 2^{-35}$	0.000000	0	0.000267	17
1024	$32 \cdot 2^{-35}$	0.000083	5	0.000267	17
1056	$33 \cdot 2^{-35}$	0.000000	0	0.000184	12
1088	$34 \cdot 2^{-35}$	0.000000	0	0.000184	12
1120	$35 \cdot 2^{-35}$	0.000000	0	0.000184	12
1152	$36 \cdot 2^{-35}$	0.000083	5	0.000184	12