1 Block 1 of 8

Table 1-1: Differential Path - block 1

Using $\delta m_{11} = +2^{20}$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	01001110 01111011 10000101 00101101	32
-2	0-00+-11 0-100-10 0++100-+ 0++10111	32
-1	++010+00 -+100-10 0++1011- +0-11111	32
0	0-100+01 1-11-+11 0++11001 -0-00100	32
1	+0...+-. 1-+.++.- ....1 -.-.1+.0	16
2	1+...-+. 1.-.1..- .10^..!1 ..-^00.1	18
3	0+.0^-1. -1-011.- ^11+..^- 1.++01.+	25
4	11.1++1. -.01.... +0.0..-1 ..10+1.+	19
5	010-01.0 +00.0000 0-010001 000--00.	29
6	1-1+1+01 +1.01111 ++1+11++ 11.00-10	30
7	.0.+.0.- .1....-- 1+.-..+0 .-.11--.	17
8	.1...0.1 0-....00 100-..0+ 1+..0.-.	17
9	.0.10..1 .-....1+ .-1...++ 0+..101.	16
10	.10.0011 0.0000.0 01+00!1. +.00+.01	25
11	0010+11+ 10111111 1+0.11-0 111110+0	31
12	1-0.-1+1 0101..01 00+.00+1 001.100-	27
13	00+10-0- --+0^^+- 000^1+0- -1+.0-++	31
14	11000+-- -------- +.+----- +--1+---	31
15	+01-0100 0-1-10-0 -.1010-1 0+10100+	31
16	1001-11+ 01010001 +.000000 000+100-	31
17	1.10...0 .1.0..-. 1.1...+. .0.-..10	14
18	..+.^..- ...1.... +.-...+. ...1..+0	10
19	^^.....- .0.+..^. +....0-. ...-....	10
20	..^....0 01...0.. 0.^..1-. .0...0^.	12
21	..0....1 1-.^.1.. ^....-0. .1.^.1..	12
22	..1..... +....+.. ......^. .+...-..	6
23	..+.0... .^...... 0....^..	5
24	....1... ^....^.. 1...0... .^...^.0	8
25	..^.-... .... -...1...	4
26	....0.... ....-... ......0+	4
27	....^... ...1.... ^....... ......1+	5
28	....+.... ....^... ......+-	4
29	....0.... 0	2
30	....-.... ....^1	3
31	....-....	1
32	....	0
33	....!....	1
$34-60$	....	0
61	....	
62	.+......	
63	.+......	
64	.+......	

Table 1-2: Block 1 found using path in Table 1-1

$$
\begin{aligned}
M_1 &= \texttt{A4 74 25 81 8D C8 4F 86 73 6E 90 72 28 BB E8 77} \\
&\quad \texttt{02 03 85 8D 8C F1 83 7A FF 5E 6C 22 13 03 6A F3} \\
&\quad \texttt{D9 5C 77 E9 C2 23 7D 60 8C C4 A9 FB 97 30 7B BF} \\
&\quad \texttt{98 28 61 2F 15 99 E2 61 5B CC DE DA 59 30 53 2F} \\
&= \{\ \texttt{812574a4}_{16},\ \texttt{864fc88d}_{16},\ \texttt{72906e73}_{16},\ \texttt{77e8bb28}_{16}, \\
&\quad\ \texttt{8d850302}_{16},\ \texttt{7a83f18c}_{16},\ \texttt{226c5eff}_{16},\ \texttt{f36a0313}_{16}, \\
&\quad\ \texttt{e9775cd9}_{16},\ \texttt{607d23c2}_{16},\ \texttt{fba9c48c}_{16},\ \texttt{bf7b3097}_{16}, \\
&\quad\ \texttt{2f612898}_{16},\ \texttt{61e29915}_{16},\ \texttt{dadecc5b}_{16},\ \texttt{2f533059}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M_1' &= \texttt{A4 74 25 81 8D C8 4F 86 73 6E 90 72 28 BB E8 77} \\
&\quad \texttt{02 03 85 8D 8C F1 83 7A FF 5E 6C 22 13 03 6A F3} \\
&\quad \texttt{D9 5C 77 E9 C2 23 7D 60 8C C4 A9 FB 97 30 8B BF} \\
&\quad \texttt{98 28 61 2F 15 99 E2 61 5B CC DE DA 59 30 53 2F} \\
&= \{\ \texttt{812574a4}_{16},\ \texttt{864fc88d}_{16},\ \texttt{72906e73}_{16},\ \texttt{77e8bb28}_{16}, \\
&\quad\ \texttt{8d850302}_{16},\ \texttt{7a83f18c}_{16},\ \texttt{226c5eff}_{16},\ \texttt{f36a0313}_{16}, \\
&\quad\ \texttt{e9775cd9}_{16},\ \texttt{607d23c2}_{16},\ \texttt{fba9c48c}_{16},\ \texttt{bf8b3097}_{16}, \\
&\quad\ \texttt{2f612898}_{16},\ \texttt{61e29915}_{16},\ \texttt{dadecc5b}_{16},\ \texttt{2f533059}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_2 &= \texttt{E745A147086391F0910F3B97AE85BE73} \\
&= \{\texttt{47a145e7}_{16}, \texttt{f0916308}_{16}, \texttt{973b0f91}_{16}, \texttt{73be85ae}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV_2' &= \texttt{E745A14768C24DF4F16EF79A0EE57A77} \\
&= \{\texttt{47a145e7}_{16}, \texttt{f44dc268}_{16}, \texttt{9af76ef1}_{16}, \texttt{777ae50e}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_2 &= \{0, \delta b_2, \delta b_2, \delta b_2\} \\
\delta b_2 &= -2^5 - 2^7 - 2^{13} + 2^{15} - 2^{18} - 2^{22} + 2^{26}
\end{aligned}
$$

2 Block 2 of 8

Table 2-1: Differential Path - block 2

Using $\delta m_{11} = -2^{16}$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	01000111 10100001 01000101 11100111	32
-2	01110+11 -+111-10 1++00101 -0-01110	32
-1	1001+-1- ++11-+11 0++0111- 1++10001	32
0	11110+00 -+0-++01 +1-0001- 0++01000	32
1	0.+.11.- ++1--+.. 0+1...1- .++.....	18
2	0.+0+0.1 -.+.-... 1+0..!+. ..-.....	15
3	+1+10+.+ 10+1-0.. 0++...11 .00.....	20
4	1.+.--.+ 1.+0.... .+1...-. ..+0.^..	14
5	1.11-10. -0.-0000 01-000-0 00110+00	29
6	110.0110 -11+1111 1-+111+1 11--1011	31
7	+0111-.. -..-.1.. --+.0.-. ..00.0..	17
8	001.+-.. +.!-.+.. +...+.-. ..-+....	14
9	+00.1-.. 0..+.1.. -10.0... ..-+...0	15
10	++100-0. 00.+.-00 -.000000 !1+.00.0	26
11	-0110+10 010-0-11 -001.111 ^111110-	31
12	1000+000 101+1-^0 -.+0.00^ ++10010+	30
13	----00-- ++---+-+ +^+11--- 0-0++++-	32
14	110--+++ ++++1000 +---1100 -+++++++	32
15	1110+100 +++0101+ +010+110 010111-0	32
16	..1+1101 1++1...1 1001-.0. 110000-0	25
17	!.1.1.1. 100..+.0 1...1.1. ..-..100	16
18	..-^..-. .^+..+.1 ....1.-. ..-...10	12
19	....+..-.- ....-... .0+....+	7
20	.0^...^. ..0.1-.. .0....^. .1+..0..	11
21	.1....0. ..^.1-.^ .1..^... .+0..1.^	12
22	.+....1. ....-1.. .-...... ..^..-..	7
23	......-. 0...10.. ....0... .^......	6
24	.^.0.... 1...0... .^..1... 0....^..	8
25	......^. +....... ....+... 1.......	4
26	..0-.... ....0 .... +.......	4
27	..1-.... ^......1 ....^...	5
28	..-+.... ....- .... ^.......	4
29	...0.... ....0	2
30	..^1.... ....+	3
31	....+	1
32	....	0
33	....!	1
$34 - 60$	....	0
61	....	
62	.....-..	
63	.....-..	
64	.....-..	

Table 2-2: Block 2 found using path in Table 2-1

$$
\begin{aligned}
M_2 &= \texttt{B3 DD 11 72 78 E4 94 40 14 33 63 0E 74 61 C1 DC} \\
&\quad \texttt{9B 80 1B 2E 55 20 15 A5 13 FF 7A E7 97 3E F4 4B} \\
&\quad \texttt{83 52 E4 E0 49 79 B3 1E B6 00 65 4D 51 F4 A4 81} \\
&\quad \texttt{CE BE 3F 0B D0 99 D1 30 D1 45 6F AB E0 4A 3E 98} \\
&= \{\ \texttt{7211ddb3}_{16},\ \texttt{4094e478}_{16},\ \texttt{0e633314}_{16},\ \texttt{dcc16174}_{16}, \\
&\quad\ \texttt{2e1b809b}_{16},\ \texttt{a5152055}_{16},\ \texttt{e77aff13}_{16},\ \texttt{4bf43e97}_{16}, \\
&\quad\ \texttt{e0e45283}_{16},\ \texttt{1eb37949}_{16},\ \texttt{4d6500b6}_{16},\ \texttt{81a4f451}_{16}, \\
&\quad\ \texttt{0b3fbece}_{16},\ \texttt{30d199d0}_{16},\ \texttt{ab6f45d1}_{16},\ \texttt{983e4ae0}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M_2' &= \texttt{B3 DD 11 72 78 E4 94 40 14 33 63 0E 74 61 C1 DC} \\
&\quad \texttt{9B 80 1B 2E 55 20 15 A5 13 FF 7A E7 97 3E F4 4B} \\
&\quad \texttt{83 52 E4 E0 49 79 B3 1E B6 00 65 4D 51 F4 A3 81} \\
&\quad \texttt{CE BE 3F 0B D0 99 D1 30 D1 45 6F AB E0 4A 3E 98} \\
&= \{\ \texttt{7211ddb3}_{16},\ \texttt{4094e478}_{16},\ \texttt{0e633314}_{16},\ \texttt{dcc16174}_{16}, \\
&\quad\ \texttt{2e1b809b}_{16},\ \texttt{a5152055}_{16},\ \texttt{e77aff13}_{16},\ \texttt{4bf43e97}_{16}, \\
&\quad\ \texttt{e0e45283}_{16},\ \texttt{1eb37949}_{16},\ \texttt{4d6500b6}_{16},\ \texttt{81a3f451}_{16}, \\
&\quad\ \texttt{0b3fbece}_{16},\ \texttt{30d199d0}_{16},\ \texttt{ab6f45d1}_{16},\ \texttt{983e4ae0}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_3 &= \texttt{6900F0DD0821F13B2AF6DF5D3521BFC7} \\
&= \{\texttt{ddf00069}_{16}, \texttt{3bf12108}_{16}, \texttt{5ddff62a}_{16}, \texttt{c7bf2135}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV_3' &= \texttt{6900F0DD6880AD3B8A559C5D95807BC7} \\
&= \{\texttt{ddf00069}_{16}, \texttt{3bad8068}_{16}, \texttt{5d9c558a}_{16}, \texttt{c77b8095}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_3 &= \{0, \delta b_3, \delta b_3, \delta b_3\} \\
\delta b_3 &= -2^5 - 2^7 - 2^{13} + 2^{15} - 2^{18} - 2^{22}
\end{aligned}
$$

3 Block 3 of 8

Table 3-1: Differential Path - block 3

Using $\delta m_{11} = +2^{12}$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	11011101 11110000 00000000 01101001	32
-2	11000111 -+111-11 +0-0000- +0-10101	32
-1	01011101 1-0111-- -1-101-+ +0-01010	32
0	00111011 1-1-++01 +0-0000- 0++01000	32
1	.......- .+.-01-- 1---..10 --+.1...	17
2	0..!...0 .+..0-0- -1.+0..- +0-.-...	17
3	01.....1 .-.0-1+. +00+0..- -+1.0...	18
4	+0.^.... .-..1--1 +...+... 0-+.1...	14
5	110+000^ 0.00+1+. 0001-001 00-0.010	29
6	+110110+ 111110-0 -1111111 00-10111	32
7	-..+..-0 ....00-1 +..01... -.-...-.	14
8	-1!1..-0 .....1-. +..-.... 1..^..0.	13
9	10.1..+0 ..0..+-. ...+.0.. 1!1+0.0.	16
10	0.0.00+0 .01.00.0 100-0100 ..011..^	23
11	1110111+ 01-01-01 011+1-11 0101-01+	32
12	001.110- 10110-11 01001+.0 11+0-110	30
13	-++^+++1 -++++-+ -----+^1 +--10--1	32
14	010+1100 111+---- +-0+11-+ +++++++.	31
15	11+0110+ +000-111 010--011 -110-01.	31
16	..+00.0- ..01-001 00.0..01 +100110.	23
17	..00..11 ^.1.0.0. .-.0^... 1.1.1.+.	15
18	..10..+^ ..+.1.1. .-.1.... 1.+...+.	12
19	...-.... ......-. .+.+.... +....0-.	7
20	.0...0^. ..^...0. 1+...0.. ..^..1-.	11
21	.1.^.1.. ..0...1. 1+.^.1.. ^....-0.	12
22	.+...-.. ..1..... +1...+.. ......^.	7
23	....+.0... 10...... 0....^..	6
24	.^...^.0 ....1... 0....^.. 1...0...	8
25	....^.-... .... -...1...	4
26	......0+ ....0.... ....-...	4
27	......1+ ....^... ...1.... ^.......	5
28	......+- ....+.... ....^...	4
29	.......0 ....0....	2
30	......^1 ....-....	3
31	....-....	1
32	....	0
33	....!....	1
$34-60$	....	0
61	....	
62	....+......	
63	....+......	
64	....+......	

Table 3-2: Block 3 found using path in Table 3-1

$$
\begin{aligned}
M_3 &= \texttt{85 C8 C4 FB 29 7B 86 B5 77 52 CD 64 19 80 9F E3} \\
&\quad \texttt{7E 62 86 F0 77 32 D1 E0 69 A5 B4 E5 66 70 B8 BB} \\
&\quad \texttt{BA E5 C2 11 74 2A 13 1D 05 71 1C F1 FE 22 AF 93} \\
&\quad \texttt{3F 1E EF 22 47 62 E3 AA DA C1 7C 40 E4 48 CA 41} \\
&= \{\ \texttt{fbc4c885}_{16},\ \texttt{b5867b29}_{16},\ \texttt{64cd5277}_{16},\ \texttt{e39f8019}_{16}, \\
&\quad\ \texttt{f086627e}_{16},\ \texttt{e0d13277}_{16},\ \texttt{e5b4a569}_{16},\ \texttt{bbb87066}_{16}, \\
&\quad\ \texttt{11c2e5ba}_{16},\ \texttt{1d132a74}_{16},\ \texttt{f11c7105}_{16},\ \texttt{93af22fe}_{16}, \\
&\quad\ \texttt{22ef1e3f}_{16},\ \texttt{aae36247}_{16},\ \texttt{407cc1da}_{16},\ \texttt{41ca48e4}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M'_3 &= \texttt{85 C8 C4 FB 29 7B 86 B5 77 52 CD 64 19 80 9F E3} \\
&\quad \texttt{7E 62 86 F0 77 32 D1 E0 69 A5 B4 E5 66 70 B8 BB} \\
&\quad \texttt{BA E5 C2 11 74 2A 13 1D 05 71 1C F1 FE 32 AF 93} \\
&\quad \texttt{3F 1E EF 22 47 62 E3 AA DA C1 7C 40 E4 48 CA 41} \\
&= \{\ \texttt{fbc4c885}_{16},\ \texttt{b5867b29}_{16},\ \texttt{64cd5277}_{16},\ \texttt{e39f8019}_{16}, \\
&\quad\ \texttt{f086627e}_{16},\ \texttt{e0d13277}_{16},\ \texttt{e5b4a569}_{16},\ \texttt{bbb87066}_{16}, \\
&\quad\ \texttt{11c2e5ba}_{16},\ \texttt{1d132a74}_{16},\ \texttt{f11c7105}_{16},\ \texttt{93af32fe}_{16}, \\
&\quad\ \texttt{22ef1e3f}_{16},\ \texttt{aae36247}_{16},\ \texttt{407cc1da}_{16},\ \texttt{41ca48e4}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_4 &= \texttt{6F48D9E5383E55D0FC43ED4D20ABF6F8} \\
&= \{\texttt{e5d9486f}_{16}, \texttt{d0553e38}_{16}, \texttt{4ded43fc}_{16}, \texttt{f8f6ab20}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV'_4 &= \texttt{6F48D9E5989D51D05CA3E94D800AF3F8} \\
&= \{\texttt{e5d9486f}_{16}, \texttt{d0519d98}_{16}, \texttt{4de9a35c}_{16}, \texttt{f8f30a80}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_4 &= \{0, \delta b_4, \delta b_4, \delta b_4\} \\
\delta b_4 &= -2^5 - 2^7 - 2^{13} + 2^{15} - 2^{18}
\end{aligned}
$$

4 Block 4 of 8

Table 4-1: Differential Path - block 4

Using $\delta m_{11} = +2^8$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	11100101 11011001 01001000 01101111	32
-2	11111000 11110-1+ -0-0101- +0-00000	32
-1	01001101 11101-01 +-+00011 -1-11100	32
0	11010000 01010-01 +0-111-+ +0-11000	32
1	.0..0.-0 ....-+.. .+1+..01 -1-...0.	15
2	..!.+.0- ....10.. 0+0+..00 --+0..0.	17
3	!...0.++ .0.010.. .+.+...- +-10..+.	16
4	....11++ .1!0...^ .-.+...1 -.0-..-.	15
5	0010.0.+ 0+.+00.- 010-0000 -0.-00-0	27
6	11110+1- 0+0-1101 101-1111 .10+11+1	31
7	10+..1.0 +..+..00 ..1-.... 10.+..1.	15
8	110..-.0 +1.+..+1 ..0...1. .-....0.	14
9	-1-..+.. 1.....+. ..-01.01 .-.0.^..	14
10	-010.+0. 11^0...0 .01.00+0 0-..0-00	23
11	00+10110 -1+10001 011001++ 1.011011	31
12	+0101100 1-100110 01+0+111 1011011.	31
13	-1-1---- 0--++--1 --++-100 00+----.	31
14	0-++10+- -+++++++ +1-11-++ ++0++10.	31
15	1-110010 00-.-001 011-10-1 -01101-.	30
16	0110..+1 011^111+ 1.1+.0+1 10+00.1.	26
17	.1.....+ ..1.1... ...+..1. 1.+1..1.	10
18	..0...^1 ..-....^ ...1..0. ..01..+.	10
19	.00....- ......1. ...-.0.. ..^-....	8
20	.1+..0.. ..^..... ....01.. .0....^.	8
21	0+1..1.^ ......+. ...^1+.. .1.^....	11
22	..0..+.. ......+. ....+... .+......	5
23	+^...... ......-. 0...1^.. ....0...	7
24	+....^.. ...0..0. 1...0... .^..1...	8
25	-....... ......1. -....... ....-...	4
26	-....... ..0+.... ....0	4
27	1....... ..1+.... ^......1 ....^...	6
28	0....... ..+-.... ....+	4
29	....0.... ....0	2
30	....^1.... ....-	3
31	....-	1
32	....	0
33	....!	1
$34 - 60$	....	0
61	....	
62	....+..	
63	....+..	
64	....+..	

Table 4-2: Block 4 found using path in Table 4-1

$$
\begin{aligned}
M_4 &= \texttt{A8 79 A0 3D 3C F6 65 F2 39 C7 F3 FE 82 B3 84 E8} \\
&\quad \texttt{35 E7 C9 E8 BD EE 30 C2 68 A2 12 12 84 78 9D F4} \\
&\quad \texttt{2F 44 90 6F 19 B7 90 26 46 44 36 E1 DA 64 FA 0C} \\
&\quad \texttt{53 A3 77 FA 0D 2B 01 2B 7D DC 28 55 DA E5 B5 51} \\
&= \{\ \texttt{3da079a8}_{16},\ \texttt{f265f63c}_{16},\ \texttt{fef3c739}_{16},\ \texttt{e884b382}_{16}, \\
&\quad\ \texttt{e8c9e735}_{16},\ \texttt{c230eebd}_{16},\ \texttt{1212a268}_{16},\ \texttt{f49d7884}_{16}, \\
&\quad\ \texttt{6f90442f}_{16},\ \texttt{2690b719}_{16},\ \texttt{e1364446}_{16},\ \texttt{0cfa64da}_{16}, \\
&\quad\ \texttt{fa77a353}_{16},\ \texttt{2b012b0d}_{16},\ \texttt{5528dc7d}_{16},\ \texttt{51b5e5da}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M'_4 &= \texttt{A8 79 A0 3D 3C F6 65 F2 39 C7 F3 FE 82 B3 84 E8} \\
&\quad \texttt{35 E7 C9 E8 BD EE 30 C2 68 A2 12 12 84 78 9D F4} \\
&\quad \texttt{2F 44 90 6F 19 B7 90 26 46 44 36 E1 DA 65 FA 0C} \\
&\quad \texttt{53 A3 77 FA 0D 2B 01 2B 7D DC 28 55 DA E5 B5 51} \\
&= \{\ \texttt{3da079a8}_{16},\ \texttt{f265f63c}_{16},\ \texttt{fef3c739}_{16},\ \texttt{e884b382}_{16}, \\
&\quad\ \texttt{e8c9e735}_{16},\ \texttt{c230eebd}_{16},\ \texttt{1212a268}_{16},\ \texttt{f49d7884}_{16}, \\
&\quad\ \texttt{6f90442f}_{16},\ \texttt{2690b719}_{16},\ \texttt{e1364446}_{16},\ \texttt{0cfa65da}_{16}, \\
&\quad\ \texttt{fa77a353}_{16},\ \texttt{2b012b0d}_{16},\ \texttt{5528dc7d}_{16},\ \texttt{51b5e5da}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_5 &= \texttt{80D9AE060626A79399F4E05A0E7F318F} \\
&= \{\texttt{06aed980}_{16}, \texttt{93a72606}_{16}, \texttt{5ae0f499}_{16}, \texttt{8f317f0e}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV'_5 &= \texttt{80D9AE066685A793F953E15A6EDE318F} \\
&= \{\texttt{06aed980}_{16}, \texttt{93a78566}_{16}, \texttt{5ae153f9}_{16}, \texttt{8f31de6e}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_5 &= \{0, \delta b_5, \delta b_5, \delta b_5\} \\
\delta b_5 &= -2^5 - 2^7 - 2^{13} + 2^{15}
\end{aligned}
$$

5 Block 5 of 8

Table 5-1: Differential Path - block 5

Using $\delta m_{11} = -2^5$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	00000110 10101110 11011001 10000000	32
-2	10001111 00110001 +1-1111- 0++01110	32
-1	01011010 1110000+ -1-10-++ 1++11001	32
0	10010011 10100111 +0-001-+ 0++00110	32
1	0....0.. +..-.1.1 -.0+.1-+ 1++.....	15
2	00.!.+.. -..0.-.. -.+-.... -0-.....	13
3	+1..^1.. 1..1.-.. -.1+..00 +-+.....	15
4	00..+1^. 0....-.! +.1-.... +-+.....	14
5	10000.-0 -0000+0. 10.00000 0++00.00	28
6	+1111001 -1111110 01001111 +0+11011	32
7	+.....10 .....00. ..0..0.- +1+..00.	13
8	-00....1 0..!..+. .^-....0 .-0..-0.	14
9	110....+ .0....+. .+0....0 011..--.	14
10	0.+0100+ 0000^0.0 0010...0 .1.!01+0	25
11	10+10111 1+11-101 11.10000 00001++1	31
12	0000+00- .++10101 0+00101+ 000101-1	31
13	-+011--- .--+---- --10+--- +----+1-	31
14	10---1-- .0111011 -+++++++ --------	31
15	11000101 .+01110- 010+000+ 0-..-1+0	29
16	0-001.10 .0.0.1.. 111+1111 10^^100-	26
17	.-1..-.. .11..1.^ ...0...+ .0.!-.--	14
18	^+...-.. ..0..-.. ...1...0 ....-..0	9
19	.0..0+.. ..+..... ....- 0...+.^-	9
20	.0..1+.. .....^.. ....+ 1...+..0	8
21	....+0.. 0.^..... .0.....1 +...1..1	9
22	...0.0.. 1.....- .1.....- ....-...	6
23	....^... -.....- .-.0.... ^......0	6
24	..0+.... 0.....0. ...1...^ ..0.^..1	9
25	..1+.... 1.....- .^.+.... ..1....+	7
26	..+-.... .....0-. ..-..... ..+.....	5
27	...0.... .....1-. ...^.... ..0....^	6
28	..^1.... .....-+. ..-..... ..-.....	5
29	..-..... ......0. ..-..... ..0.....	2
30	..-..... .....^1. ..-..... ..+.....	3
31	..-..... ..-..... ..-..... ..+.....	1
32	..-..... ..-..... ..-..... ..-.....	0
33	..-..... ..-..... ..-..... ..!.....	1
$34 - 60$	..-..... ..-..... ..-..... ..-.....	0
61	..-..... ..-..... ..-..... ..-.....	
62	..-..... ..-..... -.-..... ..-.....	
63	..-..... ..-..... -.-..... ..-.....	
64	..-..... ..-..... -.-..... ..-.....	

Table 5-2: Block 5 found using path in Table 5-1

$$
\begin{aligned}
M_5 &= \texttt{51 E2 80 34 11 21 20 B5 E7 9E C5 F2 6A 9F 69 DA} \\
&\quad \texttt{85 D7 4E F6 A9 7A 0B 11 64 EF A2 5F B1 AE 26 BA} \\
&\quad \texttt{45 1C CD A7 A2 E7 84 33 9C 44 7D 56 25 49 A6 0B} \\
&\quad \texttt{F0 67 62 94 BF 58 0C 91 9E C4 57 02 5D 3C 78 60} \\
&= \{\ \texttt{3480e251}_{16},\ \texttt{b5202111}_{16},\ \texttt{f2c59ee7}_{16},\ \texttt{da699f6a}_{16}, \\
&\quad\ \texttt{f64ed785}_{16},\ \texttt{110b7aa9}_{16},\ \texttt{5fa2ef64}_{16},\ \texttt{ba26aeb1}_{16}, \\
&\quad\ \texttt{a7cd1c45}_{16},\ \texttt{3384e7a2}_{16},\ \texttt{567d449c}_{16},\ \texttt{0ba64925}_{16}, \\
&\quad\ \texttt{946267f0}_{16},\ \texttt{910c58bf}_{16},\ \texttt{0257c49e}_{16},\ \texttt{60783c5d}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M'_5 &= \texttt{51 E2 80 34 11 21 20 B5 E7 9E C5 F2 6A 9F 69 DA} \\
&\quad \texttt{85 D7 4E F6 A9 7A 0B 11 64 EF A2 5F B1 AE 26 BA} \\
&\quad \texttt{45 1C CD A7 A2 E7 84 33 9C 44 7D 56 05 49 A6 0B} \\
&\quad \texttt{F0 67 62 94 BF 58 0C 91 9E C4 57 02 5D 3C 78 60} \\
&= \{\ \texttt{3480e251}_{16},\ \texttt{b5202111}_{16},\ \texttt{f2c59ee7}_{16},\ \texttt{da699f6a}_{16}, \\
&\quad\ \texttt{f64ed785}_{16},\ \texttt{110b7aa9}_{16},\ \texttt{5fa2ef64}_{16},\ \texttt{ba26aeb1}_{16}, \\
&\quad\ \texttt{a7cd1c45}_{16},\ \texttt{3384e7a2}_{16},\ \texttt{567d449c}_{16},\ \texttt{0ba64905}_{16}, \\
&\quad\ \texttt{946267f0}_{16},\ \texttt{910c58bf}_{16},\ \texttt{0257c49e}_{16},\ \texttt{60783c5d}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_6 &= \texttt{73A70AC09AC9B2233ECC7BE4C30C6488} \\
&= \{\texttt{c00aa773}_{16}, \texttt{23b2c99a}_{16}, \texttt{e47bcc3e}_{16}, \texttt{88640cc3}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV'_6 &= \texttt{73A70AC0FAA8B2239EAB7BE423EC6388} \\
&= \{\texttt{c00aa773}_{16}, \texttt{23b2a8fa}_{16}, \texttt{e47bab9e}_{16}, \texttt{8863ec23}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_6 &= \{0, \delta b_6, \delta b_6, \delta b_6\} \\
\delta b_6 &= -2^5 - 2^7 - 2^{13}
\end{aligned}
$$

6 Block 6 of 8

Table 6-1: Differential Path - block 6

Using $\delta m_{11} = +2^3$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	11000000 00001010 10100111 01110011	32
-2	10001000 01100-++ +++01100 --+00011	32
-1	11100100 01111011 1-+01-++ +0-11110	32
0	00100011 10110010 1-+0100- 1++11010	32
1	.1..0-+. +..+..0. .....00- 0++.10..	15
2	00..-0+. +..-..+. .11..1.. .-1.+0..	15
3	1-1.-1.1 ...-..+. ^.1..0.0 .1-.0+..	16
4	1+....11 0.!..... +^+..... .++.1-1.	14
5	0-00101+ 10.00^00 0+000000 0++0-100	31
6	1011110+ 01011-11 10101111 1.0100-1	31
7	101...+0 -....0.. .1.-.... .1-.11+.	14
8	0.+...10 +.!..0.. .-.+.... ..00+0+.	14
9	0.+.!.1- -.0..... .0.1...0 ..-.++..	13
10	10-0.001 -00.^000 0-.0.001 ..01.-00	25
11	11-10100 -1-0-111 1000011+ 00010-11	32
12	00+000-1 10-11111 1-00000+ 101-0100	32
13	0000++-1 0-0+++++ +1+++0-- -+++0-++	32
14	+------+ -----111 0+------ 1------0	32
15	1111111- 1+101011 00011-.0 110-1010	31
16	+01-0101 0100+..0 .00011^- .011001.	27
17	...0...+ .1..0..1 .....1.. ...-.--.	9
18	^..+...+ ....0..- ...0...^ 0..-....	9
19	...+..01 ....-... .... 10.1.^^.	9
20	...0.01- ..0....^ ...+.... +1.0..0.	11
21	...1..-. ..1.^... ...+.0.. 1-....1.	9
22	.....-0^ ..+..... 0..-.... 0.....+.	8
23	.0...-1. .... 1..-.+.. .^......	7
24	.1...+.. ..^..... -..1.+.. ......^.	7
25	.-...+.. .... 0..0.-..	5
26	.....+.. .... 0....0.. ....0...	4
27	.^...1.. .... 1....1.. ...01...	6
28	.....0.. .... +.....0. ...1-...	4
29	....-1...	2
30	.... ^....... ...1-...	3
31	....-+...	2
32	....0....	0
33	....!!...	2
$34 - 60$	....	0
61	....	
62	....+.....	
63	....+.....	
64	....+.....	

Table 6-2: Block 6 found using path in Table 6-1

$$
\begin{aligned}
M_6 &= \texttt{B9 82 96 C0 AB 9F E5 B1 D3 53 88 2E 26 C1 F7 21} \\
&\quad \texttt{B4 18 99 D9 72 B5 A1 D5 05 0B 68 45 36 44 80 10} \\
&\quad \texttt{AF 8C 7A FF 7C E8 EA CC B9 B1 FB BD C9 29 D4 F5} \\
&\quad \texttt{D4 99 FB 81 29 24 DF 30 2C B3 C4 50 23 38 62 97} \\
&= \{\ \texttt{c09682b9}_{16},\ \texttt{b1e59fab}_{16},\ \texttt{2e8853d3}_{16},\ \texttt{21f7c126}_{16}, \\
&\quad\ \texttt{d99918b4}_{16},\ \texttt{d5a1b572}_{16},\ \texttt{45680b05}_{16},\ \texttt{10804436}_{16}, \\
&\quad\ \texttt{ff7a8caf}_{16},\ \texttt{cceae87c}_{16},\ \texttt{bdfbb1b9}_{16},\ \texttt{f5d429c9}_{16}, \\
&\quad\ \texttt{81fb99d4}_{16},\ \texttt{30df2429}_{16},\ \texttt{50c4b32c}_{16},\ \texttt{97623823}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M'_6 &= \texttt{B9 82 96 C0 AB 9F E5 B1 D3 53 88 2E 26 C1 F7 21} \\
&\quad \texttt{B4 18 99 D9 72 B5 A1 D5 05 0B 68 45 36 44 80 10} \\
&\quad \texttt{AF 8C 7A FF 7C E8 EA CC B9 B1 FB BD D1 29 D4 F5} \\
&\quad \texttt{D4 99 FB 81 29 24 DF 30 2C B3 C4 50 23 38 62 97} \\
&= \{\ \texttt{c09682b9}_{16},\ \texttt{b1e59fab}_{16},\ \texttt{2e8853d3}_{16},\ \texttt{21f7c126}_{16}, \\
&\quad\ \texttt{d99918b4}_{16},\ \texttt{d5a1b572}_{16},\ \texttt{45680b05}_{16},\ \texttt{10804436}_{16}, \\
&\quad\ \texttt{ff7a8caf}_{16},\ \texttt{cceae87c}_{16},\ \texttt{bdfbb1b9}_{16},\ \texttt{f5d429d1}_{16}, \\
&\quad\ \texttt{81fb99d4}_{16},\ \texttt{30df2429}_{16},\ \texttt{50c4b32c}_{16},\ \texttt{97623823}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_7 &= \texttt{DE56FC8A3A0A1FEBBE6E537DB6629AC4} \\
&= \{\texttt{8afc56de}_{16}, \texttt{eb1f0a3a}_{16}, \texttt{7d536ebe}_{16}, \texttt{c49a62b6}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV'_7 &= \texttt{DE56FC8A9A091FEB1E6E537D16629AC4} \\
&= \{\texttt{8afc56de}_{16}, \texttt{eb1f099a}_{16}, \texttt{7d536e1e}_{16}, \texttt{c49a6216}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
\delta IHV_7 &= \{0, \delta b_7, \delta b_7, \delta b_7\} \\
\delta b_7 &= -2^5 - 2^7
\end{aligned}
$$

7 Block 7 of 8

Table 7-1: Differential Path - block 7

Using $\delta m_{11} = +2^{29}$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	10001010 11111100 01010110 11011110	32
-2	11000100 10011010 01100010 -0-10110	32
-1	01111101 01010011 01101110 -0-11110	32
0	11101011 00011111 000010-+ +0-11010	32
1	..0..0.. ....11.. 0-0-..01 -1-.....	13
2	.1.!0+.. ....1+.. -0++..00 --+.....	15
3	.1!.01.. .0..+-.. 1-0-.... --+.....	14
4	!-..-1.. .0..+-!. +1++.... .+......	13
5	!-00-.00 ^-001-.0 101+0000 1+000000	30
6	!+11-011 ++11--01 1.+-1111 1.111111	30
7	!1..-... 00.^--.! -.01.... .1^.^...	15
8	!1..+... 10!-.... -.0-.0.. ..+0+..0	15
9	..!.1... ...010.. -..+.0.. .!001^.0	14
10	00.!-010 00.1..10 .00+!+.0 .01+1-1-	25
11	110.-111 1100^011 01110+01 001-000+	31
12	.11^00+1 0010+1+^ 00^1111. 1-0-0+-0	30
13	^1+----0 1-0+0+0- +++++++1 +--+-++0	32
14	--1110-+ +++++0+1 00000010 +--0---.	31
15	1+1+1-1- 011-1+10 0000000- 011-.10.	30
16	01...00+ 10111+1. ..+..1.. 100-^01.	21
17	.0.^.+.1 .1.^.+.. ..-..1.^ .0.0..0.	13
18	.......1 .+...+.. ..1..+.. .1.1..1.	8
19	0....^.+ ....0-.. ..-..... .-....-.	8
20	1...0... .^..1-.. 0....^.. .1.....0	9
21	+...1..^ ...0-0.. 1.^..... .0....^0	11
22	....+... ...1.^.. +.....+. .1.....+	6
23	^......0 ..0-^... 1.....+. .+.0....	8
24	....^..1 ..10.... 0.....0. ...1...^	8
25	.......- ..-+.... ....^.-....	5
26	..0..... ...-.... .....0+.	4
27	..1....^ ..^1.... .....1+. ...^....	7
28	..+..... ...0.... .....+-.	4
29	..0..... ....0.	2
30	..-..... ....^1.	3
31	..-.....	1
32	....	0
33	..!.....	1
$34-60$	....	0
61	....	
62	.... +.......	
63	.... +.......	
64	.... +.......	

Table 7-2: Block 7 found using path in Table 7-1

$$
\begin{aligned}
M_7 &= \texttt{93 96 B3 A4 6C D0 FF 7F 14 26 71 1C 45 92 97 B6} \\
&\quad \texttt{5D 1C EF 66 C1 87 51 E0 94 BF 08 F3 B2 98 1C 5C} \\
&\quad \texttt{CE 52 D9 63 D5 A4 25 9A 64 55 7E 4D 1B 9E FE 0D} \\
&\quad \texttt{9A 51 6D 1E 6E C8 BB 37 06 68 25 AE A6 36 16 60} \\
&= \{\ \texttt{a4b39693}_{16},\ \texttt{7fffd06c}_{16},\ \texttt{1c712614}_{16},\ \texttt{b6979245}_{16}, \\
&\quad\ \texttt{66ef1c5d}_{16},\ \texttt{e05187c1}_{16},\ \texttt{f308bf94}_{16},\ \texttt{5c1c98b2}_{16}, \\
&\quad\ \texttt{63d952ce}_{16},\ \texttt{9a25a4d5}_{16},\ \texttt{4d7e5564}_{16},\ \texttt{0dfe9e1b}_{16}, \\
&\quad\ \texttt{1e6d519a}_{16},\ \texttt{37bbc86e}_{16},\ \texttt{ae256806}_{16},\ \texttt{601636a6}_{16}\ \} \\
\\
M'_7 &= \texttt{93 96 B3 A4 6C D0 FF 7F 14 26 71 1C 45 92 97 B6} \\
&\quad \texttt{5D 1C EF 66 C1 87 51 E0 94 BF 08 F3 B2 98 1C 5C} \\
&\quad \texttt{CE 52 D9 63 D5 A4 25 9A 64 55 7E 4D 1B 9E FE 2D} \\
&\quad \texttt{9A 51 6D 1E 6E C8 BB 37 06 68 25 AE A6 36 16 60} \\
&= \{\ \texttt{a4b39693}_{16},\ \texttt{7fffd06c}_{16},\ \texttt{1c712614}_{16},\ \texttt{b6979245}_{16}, \\
&\quad\ \texttt{66ef1c5d}_{16},\ \texttt{e05187c1}_{16},\ \texttt{f308bf94}_{16},\ \texttt{5c1c98b2}_{16}, \\
&\quad\ \texttt{63d952ce}_{16},\ \texttt{9a25a4d5}_{16},\ \texttt{4d7e5564}_{16},\ \texttt{2dfe9e1b}_{16}, \\
&\quad\ \texttt{1e6d519a}_{16},\ \texttt{37bbc86e}_{16},\ \texttt{ae256806}_{16},\ \texttt{601636a6}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_8 &= \texttt{DCA82596835B2D4F2EDB818BFEE0D521} \\
&= \{\texttt{9625a8dc}_{16}, \texttt{4f2d5b83}_{16}, \texttt{8b81db2e}_{16}, \texttt{21d5e0fe}_{16}\} \\
\\
IHV'_8 &= \texttt{DCA82596635B2D4F0EDB818BDEE0D521} \\
&= \{\texttt{9625a8dc}_{16}, \texttt{4f2d5b63}_{16}, \texttt{8b81db0e}_{16}, \texttt{21d5e0de}_{16}\} \\
\\
\delta IHV_8 &= \{0, \delta b_8, \delta b_8, \delta b_8\} \\
\delta b_8 &= -2^5
\end{aligned}
$$

8 Block 8 of 8

Table 8-1: Differential Path - block 8

Using $\delta m_{11} = +2^{27}$

t	Bits Q_t: $b_{31} \dots b_0$	#
-3	10010110 00100101 10101000 11011100	32
-2	00100001 11010101 11100000 11-11110	32
-1	10001011 10000001 11011011 00-01110	32
0	01001111 00101101 01011011 -++00011	32
1	..1..... ......0. ..+-.... 0-+.....	7
2	..00.... ....0^-. ..1+.... 1-+.....	10
3	!.+0..1. ....0-+. ..1+.... .0-.....	11
4	.!0+..0. ....-1-. ...+.... .-+.....	10
5	..+-..-. ....+1-. .1...... .1-.1...	10
6	!.0-..0. ....1... .0.1.!.1 .10.00..	13
7	..1+..01 ....0.0. !+.....0 ..0.+1.1	13
8	!..0..-1 ....! .-.^...- ....-+.0	11
9	.!.0..0+ ......0. .+1-...+ 1-.-	12
10	......1+ .1....1. .100...+ 0.0.0-.-	13
11	.1...11+ .00101-1 !1+0.1.+ 0.101-10	24
12	00^0000- .-101111 .0-000.1 +^-10001	29
13	0+-00-+1 ^0--++-- ^-1+1-.- ++++----	31
14	+110+--- ---+0+-- -----100 .1110100	31
15	101-1-11 101010.0 1+1001.1 11110-0-	30
16	10010010 +00-.1^1 00101+.0 ....-	23
17	01.-.0.. ...0...+ .0..0..1 .....^.1	11
18	1+.-.... ^..+...+ ....0^.- ...0...0	11
19	+0.1.... ...+..01 ....-...	7
20	.-.0..0. ...0.01- ..0....^ ...+....	10
21	^-....1. ...1..-. ..1.^... ...+.0..	9
22	.0....+. .....-0^ ..+..... 0..-....	8
23	.1...... .0...-1. .... 1..-.+..	7
24	......^. .1...+.. ..^..... -..1.+..	7
25	....-...+.. .... 0..0.-..	5
26	....0... .....+.. .... 0....0..	4
27	...01... .^...1.. .... 1....1..	6
28	...1-... .....0.. .... +.......	4
29	...-1...	2
30	...1-... .... ^.......	3
31	...-+...	2
32	...0....	1
33	...!!...	2
$34-60$	....	0
61	....	
62	....+.....	
63	....+.....	
64	....+.....	

Table 8-2: Block 8 found using path in Table 8-1

$$
\begin{aligned}
M_8 &= \texttt{2B D7 D1 16 25 A0 6A 90 73 9B 4D 0A 06 EA 87 2A} \\
&\quad \texttt{3A F9 EB A1 26 29 BE D6 79 40 56 1B D9 37 4A 89} \\
&\quad \texttt{D6 0F 0D 72 2C 9F EB 68 33 EC 53 F0 B0 FD 76 A2} \\
&\quad \texttt{04 7B 66 C9 0F CE B1 D2 E2 2C C0 99 B9 A4 B9 3E} \\
&= \{\ \texttt{16d1d72b}_{16},\ \texttt{906aa025}_{16},\ \texttt{0a4d9b73}_{16},\ \texttt{2a87ea06}_{16}, \\
&\quad\ \texttt{a1ebf93a}_{16},\ \texttt{d6be2926}_{16},\ \texttt{1b564079}_{16},\ \texttt{894a37d9}_{16}, \\
&\quad\ \texttt{720d0fd6}_{16},\ \texttt{68eb9f2c}_{16},\ \texttt{f053ec33}_{16},\ \texttt{a276fdb0}_{16}, \\
&\quad\ \texttt{c9667b04}_{16},\ \texttt{d2b1ce0f}_{16},\ \texttt{99c02ce2}_{16},\ \texttt{3eb9a4b9}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
M'_8 &= \texttt{2B D7 D1 16 25 A0 6A 90 73 9B 4D 0A 06 EA 87 2A} \\
&\quad \texttt{3A F9 EB A1 26 29 BE D6 79 40 56 1B D9 37 4A 89} \\
&\quad \texttt{D6 0F 0D 72 2C 9F EB 68 33 EC 53 F0 B0 FD 76 AA} \\
&\quad \texttt{04 7B 66 C9 0F CE B1 D2 E2 2C C0 99 B9 A4 B9 3E} \\
&= \{\ \texttt{16d1d72b}_{16},\ \texttt{906aa025}_{16},\ \texttt{0a4d9b73}_{16},\ \texttt{2a87ea06}_{16}, \\
&\quad\ \texttt{a1ebf93a}_{16},\ \texttt{d6be2926}_{16},\ \texttt{1b564079}_{16},\ \texttt{894a37d9}_{16}, \\
&\quad\ \texttt{720d0fd6}_{16},\ \texttt{68eb9f2c}_{16},\ \texttt{f053ec33}_{16},\ \texttt{aa76fdb0}_{16}, \\
&\quad\ \texttt{c9667b04}_{16},\ \texttt{d2b1ce0f}_{16},\ \texttt{99c02ce2}_{16},\ \texttt{3eb9a4b9}_{16}\ \}
\end{aligned}
$$

$$
\begin{aligned}
IHV_9 &= \texttt{505D9746FAB00B328018DBC34A87DF11} \\
&= \{\texttt{46975d50}_{16}, \texttt{320bb0fa}_{16}, \texttt{c3db1880}_{16}, \texttt{11df874a}_{16}\}
\end{aligned}
$$

$$
\begin{aligned}
IHV'_9 &= \texttt{505D9746FAB00B328018DBC34A87DF11} \\
&= \{\texttt{46975d50}_{16}, \texttt{320bb0fa}_{16}, \texttt{c3db1880}_{16}, \texttt{11df874a}_{16}\}
\end{aligned}
$$

$$
\delta IHV_9 = \{0, 0, 0, 0\}
$$