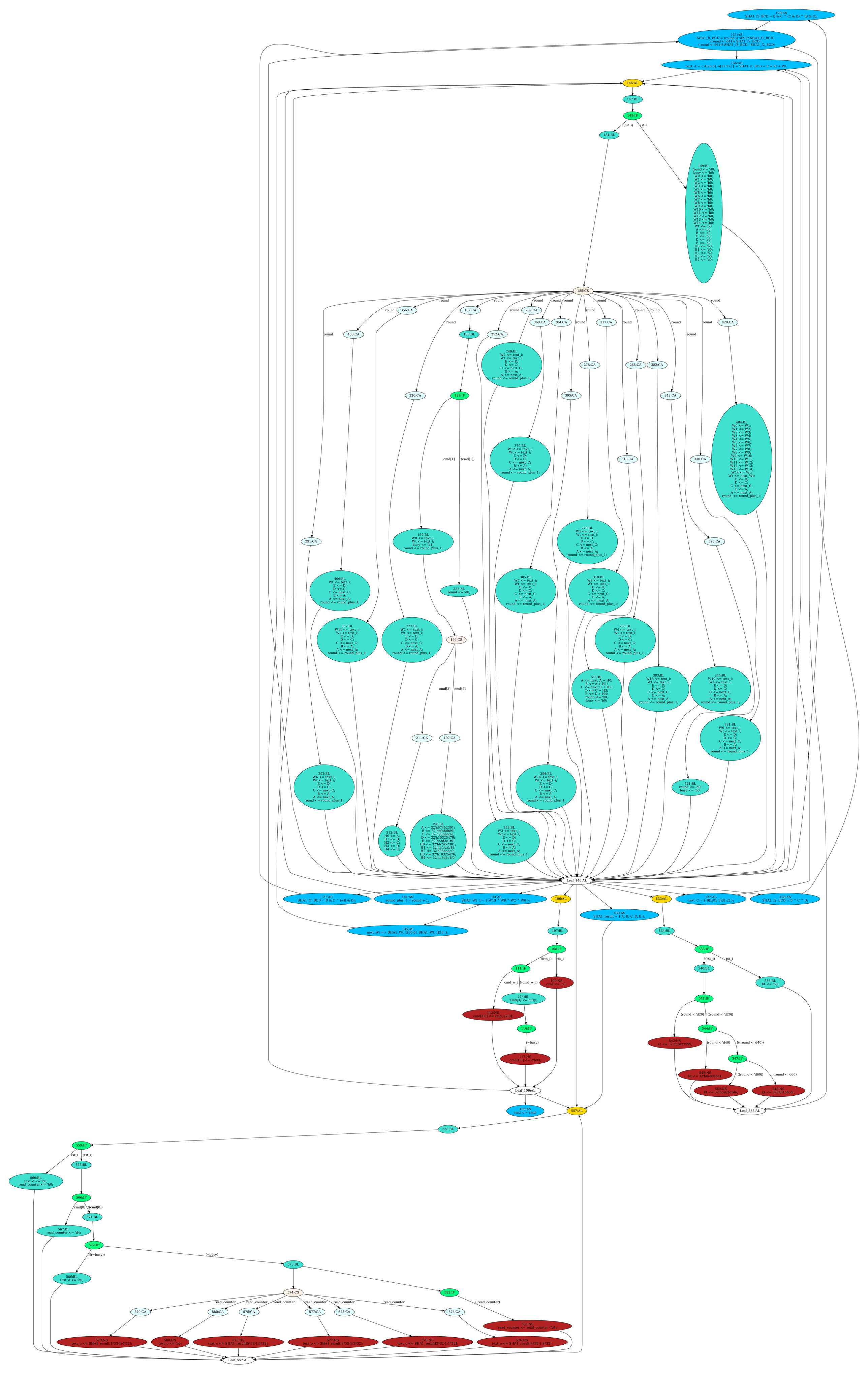
129:AS
SHA1_f3_BCD = B & C ^ (C & D) ^ (B & D);
131:AS
SHA1_ft_BCD = (round < 'd21)? SHA1_f1_BCD :
(round < 'd41)? SHA1_f2_BCD :
(round < 'd61)? SHA1_f3_BCD : SHA1_f2_BCD;
136:AS
next_A = { A[26:0], A[31:27] } + SHA1_ft_BCD + E + Kt + Wt;
146:AL
147:BL
148:IF
!(rst_i)
rst_i
184:BL
149:BL
round <= 'd0;
busy <= 'b0;
W0 <= 'b0;
W1 <= 'b0;
W2 <= 'b0;
W3 <= 'b0;
W4 <= 'b0;
W5 <= 'b0;
W6 <= 'b0;
W7 <= 'b0;
W8 <= 'b0;
W9 <= 'b0;
W10 <= 'b0;
W11 <= 'b0;
W12 <= 'b0;
W13 <= 'b0;
W14 <= 'b0;
Wt <= 'b0;
A <= 'b0;
B <= 'b0;
C <= 'b0;
D <= 'b0;
E <= 'b0;
H0 <= 'b0;
H1 <= 'b0;
H2 <= 'b0;
H3 <= 'b0;
H4 <= 'b0;
185:CS
round
356:CA
187:CA
239:CA
369:CA
304:CA
317:CA
420:CA
408:CA
188:BL
252:CA
240:BL
W2 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
278:CA
265:CA
382:CA
226:CA
189:IF
395:CA
343:CA
484:BL
W0 <= W1;
W1 <= W2;
W2 <= W3;
W3 <= W4;
W4 <= W5;
W5 <= W6;
W6 <= W7;
W7 <= W8;
W8 <= W9;
W9 <= W10;
W10 <= W11;
W11 <= W12;
W12 <= W13;
W13 <= W14;
W14 <= Wt;
Wt <= next_Wt;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
cmd[1]
!(cmd[1])
370:BL
W12 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
510:CA
330:CA
291:CA
190:BL
W0 <= text_i;
Wt <= text_i;
busy <= 'b1;
round <= round_plus_1;
279:BL
W5 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
520:CA
409:BL
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
222:BL
round <= 'd0;
305:BL
W7 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
318:BL
W8 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
357:BL
W11 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
227:BL
W1 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
196:CS
266:BL
W4 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
511:BL
A <= next_A + H0;
B <= A + H1;
C <= next_C + H2;
D <= C + H3;
E <= D + H4;
round <= 'd0;
busy <= 'b0;
383:BL
W13 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
344:BL
W10 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
cmd[2]
cmd[2]
331:BL
W9 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
211:CA
197:CA
292:BL
W6 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
396:BL
W14 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
521:BL
round <= 'd0;
busy <= 'b0;
212:BL
H0 <= A;
H1 <= B;
H2 <= C;
H3 <= D;
H4 <= E;
198:BL
A <= 32'h67452301;
B <= 32'hefcdab89;
C <= 32'h98badcfe;
D <= 32'h10325476;
E <= 32'hc3d2e1f0;
H0 <= 32'h67452301;
H1 <= 32'hefcdab89;
H2 <= 32'h98badcfe;
H3 <= 32'h10325476;
H4 <= 32'hc3d2e1f0;
253:BL
W3 <= text_i;
Wt <= text_i;
E <= D;
D <= C;
C <= next_C;
B <= A;
A <= next_A;
round <= round_plus_1;
Leaf_146:AL
127:AS
SHA1_f1_BCD = B & C ^ (~B & D);
141:AS
round_plus_1 = round + 1;
133:AS
SHA1_Wt_1 = { W13 ^ W8 ^ W2 ^ W0 };
106:AL
533:AL
137:AS
next_C = { B[1:0], B[31:2] };
128:AS
SHA1_f2_BCD = B ^ C ^ D;
139:AS
SHA1_result = { A, B, C, D, E };
135:AS
next_Wt = { SHA1_Wt_1[30:0], SHA1_Wt_1[31] };
107:BL
534:BL
108:IF
!(rst_i)
rst_i
535:IF
!(rst_i)
rst_i
111:IF
109:NS
cmd <= 'b0;
540:BL
536:BL
Kt <= 'b0;
cmd_w_i
!(cmd_w_i)
114:BL
cmd[3] <= busy;
541:IF
112:NS
cmd[2:0] <= cmd_i[2:0];
(round < 'd20)
!((round < 'd20))
116:IF
544:IF
(~busy)
542:NS
Kt <= 32'h5a827999;
(round < 'd40)
!((round < 'd40))
117:NS
cmd[1:0] <= 2'b00;
547:IF
545:NS
Kt <= 32'h6ed9eba1;
!((round < 'd60))
(round < 'd60)
550:NS
Kt <= 32'hca62c1d6;
548:NS
Kt <= 32'h8f1bbcdc;
Leaf_106:AL
Leaf_533:AL
105:AS
cmd_o = cmd;
557:AL
558:BL
559:IF
rst_i
!(rst_i)
565:BL
560:BL
text_o <= 'b0;
read_counter <= 'b0;
566:IF
cmd[0]
!(cmd[0])
571:BL
567:BL
read_counter <= 'd4;
572:IF
!((~busy))
(~busy)
573:BL
586:BL
text_o <= 'b0;
574:CS
582:IF
read_counter
(!read_counter)
579:CA
580:CA
575:CA
577:CA
578:CA
576:CA
583:NS
read_counter <= read_counter - 'd1;
579:NS
text_o <= SHA1_result[1*32-1:0*32];
580:NS
text_o <= 'b0;
575:NS
text_o <= SHA1_result[5*32-1:4*32];
577:NS
text_o <= SHA1_result[3*32-1:2*32];
578:NS
text_o <= SHA1_result[2*32-1:1*32];
576:NS
text_o <= SHA1_result[4*32-1:3*32];
Leaf_557:AL