Collisions for 72-step and 73-step SHA-1: Improvements in the Method of Characteristics

E. A. Grechnikov
Moscow State University, Russia
grechnik@mccme.ru

July 23, 2010

Abstract

We present a brief report on the collision search for the reduced SHA-1. With a few improvements to the De Cannière-Rechberger automatic collision search method we managed to construct two new collisions for 72- and 73-step reduced SHA-1 hash function.

1 Introduction

Recently in [1] Christophe De Cannière and Christian Rechberger suggested a new method for the automatic construction of collisions for SHA-1 hash function and presented a collision for SHA-1 reduced to 64 steps. Later in [2] they made some improvements to their method and presented a new collision for 70-step SHA-1. Up to this moment that was the best known collision example for reduced SHA-1.

Based on their work and our original improvements we implemented the automatic collision search method and managed to construct a new 2-block collision for 72-step SHA-1 and another one for 73-step SHA-1.

2 The improvements

We refer to [1] for the detailed description of basic method and notations. We have made the following improvements to this method.

2.1 Speed optimizations

We focus on the speed of the longest stage of our implementation, namely the collision search by known characteristics.

1. We note that all characteristics produced by the basic algorithm consist of the following conditions on a pair of bits: `-`, `x`, `0`, `1`, `n`, `u`. Consequently, every condition on a pair of 32-bit variables X and X' can be written as $X \oplus X' = a, X \wedge b = c$, where a, b, c are some constants defined by the characteristic. This representation gives the way to test fast whether a pair of variables satisfies the characteristic.

2. The two last steps, however, are processed differently: the conditions for these steps are ignored when searching for the first block of a collision and are replaced by the condition $X - X' = a$ when searching for the second block of a collision. This special processing significantly decreases the actual work factor as described in [2]. The values of $N_s(i)$ in the tables 3–6 of the Appendix B are given with respect to this correction.

3. The search algorithm on each step i sequentially processes the values from the set ∇W_i, so one must efficiently enumerate sets of the form $X \wedge b = c$ with constant b and c. We use the following fast way: the first element in this set is c, the next element after x is given by the formula $(((x \vee b) + 1) \wedge \bar{b}) + c$, and the enumerating is done when this formula gives c.

4. A characteristic implies limitations on every W_i^2. Sometimes such limitation could not be directly inferred from the conditions on first 16 W_i^2's, but it still gives an equation binding them.

   For example, let us denote by $[X]_j$ the j-th bit of a variable X and let us consider the characteristic from the Table 3. We have the condition $[W_{66}]_4 = 0$ from ∇W_{66}. Because each $[W_i]_j$ is a linear combination of some bits in first 16 expanded message words, we can transform this condition to an equation with first 16 message words; taking into account that the values of some bits are fixed by the characteristic, we obtain the equation $[W_9]_{22} \oplus [W_{11}]_{21} = 0$ or, equivalently, $[W_{11}]_{21} = [W_9]_{22}$. Therefore when enumerating possible values for W_{11}^2, one must take into account this equation.

   However, in many cases, including the example, this is easily achieved without a complication of enumerating, because the task is still to go over all values X such that $X \wedge b = c$; the only difference here is that b and c are not constants, but calculated using previous message words.

5. Sometimes an equation arising from a condition on W_i imposes a restriction on two or more bits of the same message word which is last in this equation. This is not the case for the characteristic from the Table 3, but there is one such equation for the characteristic from the Table 4, namely $[W_{12}]_{21} \oplus [W_{12}]_{22} \oplus [W_9]_{20} \oplus \ldots = 0$ (all bits $[W_i]_j$ with $i < 9$ are omitted for brevity). It is harder than usual to enumerate all values in the set W_{12}^2 which satisfy the equation. Fortunately, the number of such equations is small (zero for the Table 3, just one for the Table 4), so we solve this problem by dividing the search space into two subspaces for each equation. In this example the first subspace has $[W_{12}]_{21} = 0$ and the second one has $[W_{12}]_{21} = 1$. Because the number of subspaces is small and the search itself consumes most of the time, the cost of additional operations to handle this division is negligible.

6. State update function in SHA-1 as a function of expanded message word is invertible. Therefore when looking for the values on the step i of the hash function, one can go over values for A_{i+1}^2 as easily as over values for W_i^2. If the size of the set ∇A_{i+1}^2 is less than the message freedom at the step i, then using A_{i+1}^2 as the source and calculating W_i^2 gives some gain in the speed.

2.2 Work factor formula

The modification of the search described in the last paragraph requires redefinition of the work factor. Namely, instead of the original definitions

$$\begin{aligned} P_u(i) &= P(A^2_{i+1} \in \nabla A_{i+1} | A^2_{i-j} \in \nabla A_{i-j} \text{ for } 0 \le j < 5, \text{ and } W^2_i \in \nabla W_i) \\ P_c(i) &= P(\exists W^2_i \in \nabla W_i : A^2_{i+1} \in \nabla A_{i+1} | A^2_{i-j} \in \nabla A_{i-j} \text{ for } 0 \le j < 5) \end{aligned}$$

the following definitions should be used when the size of the set ∇A^2_{i+1} is less than the message freedom at the step i:

$$\begin{aligned} P_u(i) &= P(W^2_i \in \nabla W_i | A^2_{i-j} \in \nabla A_{i-j} \text{ for } 0 \le j < 5, \text{ and } A^2_{i+1} \in \nabla A_{i+1}) \\ P_c(i) &= P(\exists A^2_{i+1} \in \nabla A_{i+1} : W^2_i \in \nabla W_i | A^2_{i-j} \in \nabla A_{i-j} \text{ for } 0 \le j < 5) \end{aligned}$$

The message freedom $F_W(i)$ for given characteristic equals the size of the set ∇W^2_i divided by 2^k, where k is the number of equations with $\{W_j\}$ with i being the biggest index in the equation. It should be redefined as the size of ∇A^2_{i+1} divided by 2^k with the same k.

For one specific characteristic this redefinition usually changes the value of work factor only by a small amount. However, the second stage of the collision generation, namely generation of the (nonlinear) characteristic, usually yields better results when using this variant of the work factor as target function for optimization.

2.3 Propagation optimization

Sometimes the propagation of conditions in individual steps does not guarantee that all conditions are found due to the interference between different steps. Let us consider the following example from one of the real experiments:

i	∇A_i	∇W_i
-3:	01000000110010010101000111011000	
-2:	01100010111010110111001111111010	
-1:	11101111110011011010101110001001	
0:	01100111010001010010001100000001	
1:	n01n1-----1-----1--11-01111u1001	x-nu----------------00-0u1u10un
2:	u01n01----0-10--0----un-un10110n	--nn---1--------1--01-----10u000
3:	01n1nnnnnnnnnnnnn0nnn-0---01n1n1	001--------------------0u00--un
4:	011n0n001111u1un000-1111u101--11	uu0n000-----------------xnn--u0
5:	101n000n00n0n1000n0nu000-011--10	

One can verify that for each of 4 steps in the table there exists an input and an output satisfying the characteristic, and all conditions from the table could not be set any stronger without a loss of variants in each step. This means that the propagation for this characteristic does not impose any new conditions. However, there is no set of variables which satisfies all 4 steps. In less extreme cases the characteristic is not contradictory, but the propagation on per-step basis fails to find all conditions which follow from the current set.

We use the following way to circumvent such effects. In the example there are two variants for $\{[A_0]_{23}, [A'_0]_{23}\}$, namely $[A_0]_{23} = [A'_0]_{23} = 0$ and $[A_0]_{23} = [A'_0]_{23} = 1$. We save the current characteristic, impose the condition $[A_0]_{23} = [A'_0]_{23} = 0$ and try to propagate this condition as usual; it involves several other conditions which eventually

lead to a contradiction. We restore the saved characteristic and impose now the condition $[A_0]_{23} = [A'_0]_{23} = 1$; it involves several other conditions and still eventually leads to a contradiction. Because all variants are over, we conclude that the saved characteristic is contradictory itself. A less extreme (and more usual) situation is illustrated by choices for $\{[A_0]_{20}, [A'_0]_{20}\}$; here the additional condition $[A_0]_{20} = [A'_0]_{20} = 1$ leads to a contradiction, but the opposite condition $[A_0]_{20} = [A'_0]_{20} = 0$ does not; here we decide that the saved characteristic involves the second condition.

The exhaustion of all positions with subsequent per-step propagation of every possible condition in a position is a relatively hard operation. For the stage 2 of the method, namely random trials of positions where to impose the - restriction, this strategy is inefficient. We use the following simple strategy: remember all changed bits from the previous characteristic and try only positions near the changed bits. However, the simple strategy seems to be insufficient for the stage 3 of the method, namely an optimization of one characteristic found by the previous step. Each step of the stage 3 is itself the exhaustion of all positions with tests for the new work factor, selecting the variant with the best new work factor. We modify this procedure in the following way. We keep the best work factor found so far, initializing with the work factor for the previous step. We try to add each possible condition, use the per-step propagation procedure, calculate the work factor, and if the new work factor is better than the old one, run the costly exhausting propagation.

3 Calculations

We used the new Moscow State University cluster "Lomonosov" to carry out calculations for the collision search. The collisions and corresponding charecteristics could be found in Appendix A and B. Here we discuss some details of the calculations and the time they took.

Initially we were looking for a 72-step collision. The estimated work factor was about $2^{52.9}$ visited nodes or, equivalently, about $2^{47.6}$ compression function evaluations (not including the impact of additional operations for generating inputs and testing outputs). After all optimizations the final search for the second block of a collision took 13748 seconds (less than 4 hours) with 8192 executing cores. We did not stop the search immediately, and during 8 hours of calculations two other collisions were found.

After the success in 4 hours for 72 steps it became clear that we can build a 73-step collision still in reasonable time and without a significant interference with other users of the cluster. Indeed, incrementing number of steps in the hash function from 72 to 73 results in a factor of 8 in the work factor estimated by L-characteristic. So we also tried to look for a 73-step collision. The new estimated work factor was about $2^{56.0}$ visited nodes ($2^{50.7}$ compression function evaluations). The actual time for the search of the second block was significantly lower than expected, only 2693 seconds (less than one hour) with 16384 cores due to some portion of luck; the found block was the first input which satisfied the characteristic up to the step 70 inclusive (but not the first for 69 steps), whereas for given characteristic it is natural to expect 2^7 such inputs per one collision. In fact, the calculation of the first block with the estimated work factor of $2^{52.2}$ visited nodes took longer, namely 18801 seconds with 8192 cores.

References

[1] Christophe De Cannière and Christian Rechberger. *Finding SHA-1 Characteristics: General Results and Applications.* In Proceedings of ASIACRYPT, volume 4284 of LNCS, pages 1–20. Springer, 2006.

[2] Christophe De Cannière, Florian Mendel, and Christian Rechberger. *Collisions for 70-step SHA-1: On the Full Cost of Collision Search.* In Proceedings of Selected Areas in Cryptography, volume 4876 of LNCS, pages 56-73. Springer, 2007.

A Collisions for the 72- and 73- step reduced SHA-1

Table 1. Example of a 72-step SHA-1 collision using the standard IV

i	Message 1, first block				Message 1, second block			
1–4	3025A31B	5F59436A	0F8879FB	BC105B37	EFD21A91	D9BF0685	F1A113A6	3DD066F8
5–8	7027A2DD	D01BB3AD	FE93CD37	9BA04133	584BFE78	785A1B43	E4788FB7	FC75B5C7
9–12	1ED31745	91A434B0	DE7FFC1B	23C8AF2E	16161BF1	41FFD877	741768BA	FA77D91D
13–16	BF7D8CBF	03E95C5A	E28006FF	960257A8	951713BA	C918ECB0	25D1CCBD	28FC51EE
i	Message 2, first block				Message 2, second block			
1–4	8025A348	6F594362	0F8879B8	6C105B45	5FD21AC2	E9BF068D	F1A113E5	EDD0668A
5–8	C027A2CD	201BB3CF	3E93CD75	9BA04103	E84BFE68	885A1B21	24788FF5	FC75B5F7
9–12	FED31707	B1A434D0	3E7FFC5A	03C8AF7E	F6161BB3	61FFD817	941768FB	DA77D94D
13–16	7F7D8CFE	E3E95C28	428006FC	560257BA	551713FB	2918ECC2	85D1CCBE	E8FC51FC
i	XOR-differences are the same for both blocks							
1–4	B0000053	30000008	00000043	D0000072	B0000053	30000008	00000043	D0000072
5–8	B0000010	F0000062	C0000042	00000030	B0000010	F0000062	C0000042	00000030
9–12	E0000042	20000060	E0000041	20000050	E0000042	20000060	E0000041	20000050
13–16	C0000041	E0000072	A0000003	C0000012	C0000041	E0000072	A0000003	C0000012
i	The colliding hash values							
1–5	9767B27C	20258492	1CB52F9E	C3DE9884	90340C86			

Table 2. Example of a 73-step SHA-1 collision using the standard IV

i	Message 1, first block				Message 1, second block			
1–4	0008FD3A	5030156A	1579C26A	39FDB111	6D0ED8E7	799C24C1	2C0D2CB1	8F195EFA
5–8	DAD82EFB	43512ECE	EC7CF4D4	AF6DD8DA	3DF30C98	67C66D0E	AE975974	90C24B82
9–12	85D47221	A14721A6	A0D0F5C9	925B8E10	07D0F970	19882826	A200140F	6241CD6E
13–16	29F82476	8AA46689	3FEE95A1	8E00AFAA	DEFA9EB3	7C0A5ADF	3A7A8AE4	59BA9D11
i	Message 2, first block				Message 2, second block			
1–4	9008FD4A	E0301539	2579C262	39FDB152	FD0ED897	C99C2492	1C0D2CB9	8F195EB9
5–8	0AD82E89	F3512EDE	1C7CF4B6	6F6DD898	EDF30CEA	D7C66D1E	5E975916	50C24BC0
9–12	85D47211	414721E4	80D0F5A9	725B8E51	07D0F940	F9882864	8200146F	8241CD2F
13–16	09F82426	4AA466C8	DFEE95D3	2E00AFA9	FEFA9EE3	BC0A5A9E	DA7A8A96	F9BA9D12
i	XOR-differences are the same for both blocks							
1–4	90000070	B0000053	30000008	00000043	90000070	B0000053	30000008	00000043
5–8	D0000072	B0000010	F0000062	C0000042	D0000072	B0000010	F0000062	C0000042
9–12	00000030	E0000042	20000060	E0000041	00000030	E0000042	20000060	E0000041
13–16	20000050	C0000041	E0000072	A0000003	20000050	C0000041	E0000072	A0000003
i	The colliding hash values							
1–5	AD84BC2B	50E6084F	03578AC1	3FE924DD	BC8F9B07			

B Characteristics for the 72- and 73- step reduced SHA-1

Table 3. Characteristic used for the first block of the 72-step collision

i	∇A_i	∇W_i	F_W	$P_u(i)$	$P_c(i)$	$N_s(i)$
-4:	00001111010010111000011111000011					
-3:	01000000110010010101000111011000					
-2:	01100010111010110111001111111010					
-1:	11101111110011011010101110001001					
0:	01100111010001010010001100000001	n0uu000000100101-----0110n0u10uu	2	0.00	0.00	4.99
1:	uu0n11111101101000-1-01111nn1u1n	01nu111101011---0----0110110u010	1	0.00	0.00	6.99
2:	110n0001010100011000-n1nn10100n0	000011111000100-01-1---11u1110uu	1	0.00	0.00	7.99
3:	101001101110100n0uun00-1unn010un	un1u110000010000-------10nuu01u1	0	0.00	0.00	8.99
4:	nnn01001011nn0u101111011110u0110	n1uu0000001001111010---0110u1101	0	0.00	0.00	8.99
5:	1000n0un0u000001u1n011un111n100n	uunu0000000110111011-----nu011n1	0	0.00	0.00	8.99
6:	n1unnnnnnnnnn1n01011nnu0n00010u1	uu1111101001001111001l-10n1101u1	0	0.00	0.00	8.99
7:	0011010111111nuu1u001001u01100u0	10011011101000000----001-0uu0011	1	0.00	0.00	8.99
8:	n0000001101011 0unnn-nnn11110nu0	nnn1111011010---000101110u0001n1	1	0.00	0.00	9.99
9:	n1000001100000-01100100n100u11n1	10n10001--100100001--1001nu10000	0	0.00	0.00	10.99
10:	0001010111111111111011n1000n0unu1	uun111100111111-------000n01101u	7	0.00	0.00	10.99
11:	n101110101111---------unn00u0100	00u0001111-------------10n1n1110	9	-2.00	-1.83	17.99
12:	0100101111011----------1111101n1	un111111-----------------1n11111u	6	-0.20	-0.20	24.99
13:	n101101110001011--------01100000	nnn000111110-------------unu10u0	6	-1.00	-0.91	30.79
14:	1010011110110111---------0101u00	u1u00010100--------------11111uu	3	-0.56	-0.56	35.79
15:	n1010000010011110000------0010011	un01011000000-1-----------1n10n0	11	-2.05	-0.13	38.22
16:	011010001010100----------0010n1	0un00101001-------------1u11111n	0	0.00	0.00	47.17
17:	n00011101-----------------001100	nn10000--1--------------00un01n1	0	-3.00	-0.83	47.17
18:	101---011-----------------11001	01u011111010-1-----------010101n	0	-0.17	-0.17	44.17
19:	-000----------------------00---	nn0101011----------------100101n0	0	0.00	0.00	44.00
20:	---------------------------01n-	nnu000-0---------------01u1000n0	0	-1.00	-1.00	44.00
21:	-------------------------------n-	0un01111111-------------1u0111n0	0	0.00	0.00	43.00
22:	----------------------------------	n0101110----------------001100u0	0	0.00	0.00	43.00
23:	----------------------------------	01111-00----------------0010111	0	0.00	0.00	43.00
24:	----------------------------------	1001010011-------------011111001	0	0.00	-0.00	43.00
25:	----------------------------------	n11110----------------1100010011	0	0.00	0.00	43.00
26:	----------------------------------	1110-10-1---------------0001100u0	0	-1.00	-1.00	43.00
27:	-----------------------------u-	01000010----------------0n110011	0	0.00	0.00	42.00
28:	----------------------------------	000011---0--------------01100110	0	-2.00	-2.00	42.00
29:	-----------------------------u-	n11-11-1---1-------------n111000	0	0.00	0.00	40.00
30:	----------------------------------	u0010111----------------00000001	0	-2.00	-2.00	40.00
31:	-------------------------------n-	1000---1----------------u111001	0	0.00	0.00	38.00
32:	----------------------------------	u0-00-1---------------000010101u	0	-2.00	-2.00	38.00
33:	---------------------------------n	10110-1----------------10un00111	0	0.00	0.00	36.00
34:	----------------------------------	n100---0---------------0000000un	0	-1.00	-1.00	36.00
35:	----------------------------------	0x11-1-----------------0101000n1	0	-2.00	-1.00	35.00
36:	-----------------------------n-	nu10-1----------------011u100111	0	-1.00	-1.00	33.00
37:	----------------------------------	nn---10----------------0111000u0	0	-1.00	-1.00	32.00
38:	----------------------------------	x01-0----------------0011010110	0	0.00	-0.00	31.00
39:	----------------------------------	u1001------------------100110101	0	0.00	-0.00	31.00
40:	----------------------------------	u1---1----------------00000001n1	0	-1.00	-1.00	31.00
41:	-------------------------------n-	01-1-0-0---------------10u10001-	0	0.00	0.00	30.00
42:	----------------------------------	1101-------------------0110001u0	0	-1.00	-1.00	30.00
43:	----------------------------------	x--01------------------01011111	0	-1.00	-1.00	29.00
44:	----------------------------------	n-0-1-1----------------11110001-1	0	-1.00	-1.00	28.00
45:	----------------------------------	n-0----1---------------111001010	0	0.00	0.00	27.00
46:	----------------------------------	---1-------------------1010001u1	0	-1.00	-1.00	27.00
47:	-----------------------------u-	-1---0-----------------1n011-01	0	0.00	-0.00	26.00
48:	----------------------------------	-1--------------------1111001100	0	-2.00	-2.00	26.00
49:	-----------------------------u-	x10-------------------111n0001--	0	-1.00	-1.00	24.00
50:	----------------------------------	n----------------------10111-1n-	0	-2.00	-2.00	23.00
51:	----------------------------------	0----------------------110100000	0	-1.00	-1.00	21.00
52:	----------------------------------	x0------------------010111001--	0	-1.00	-1.00	20.00
53:	----------------------------------	x0-0------------------10110-00-1	0	0.00	0.00	19.00
54:	----------------------------------	----------------------0001101000	0	0.00	-0.00	19.00
55:	----------------------------------	1----------------------00101---0	0	0.00	0.00	19.00
56:	----------------------------------	1-0------------------1110-11-0-	0	0.00	0.00	19.00
57:	----------------------------------	----------------------110100-0-	0	0.00	0.00	19.00
58:	----------------------------------	----------------------000100---0	0	0.00	0.00	19.00
59:	----------------------------------	-0----------------------10-01-0--	0	0.00	0.00	19.00
60:	----------------------------------	----------------------111000-n--	0	-1.00	-0.19	19.00
61:	-------------------------------n--	----------------------1u0---10-	0	0.00	0.00	18.00
62:	----------------------------------	----------------------11-11-0x--	0	-1.00	0.00	18.00
63:	----------------------------------	-0----------------------11000n--x	0	-2.00	-0.19	17.00
64:	-----------------------------n----	------------------10100u00---n-x	0	-2.00	-0.42	15.00
65:	-----------------------------n--	------------------0010-u1-0x1-u	0	-1.00	-0.00	13.00
66:	----------------------------------	------------------11000101n-xx-	0	-3.00	-0.36	12.00
67:	---------------------------n----	------------------011u0---0n-xx	0	-3.00	-0.42	9.00
68:	---------------------------n----	------------------00-u1-0xn-ux	0	-3.00	-0.42	6.00
69:	---------------------------n----	------------------01u0-n-xx-u	0	-3.00	-0.36	3.00
70:	-------------------------n------	------------------u01---nxxx-	0	-4.00	-0.91	0.00
71:	-------------------------n----	----------------------u1-1x--u--	0	-1.00	-0.00	0.00
72:	----------------------------					

Table 4. Characteristic used for the second block of the 72-step collision

i	∇A_i	∇W_i	F_W	$P_u(i)$	$P_c(i)$	$N_s(i)$
-4:	00001100101111011011000000010n010					
-3:	11101110100011111100100100000nu001					
-2:	10010101001111001110010111n00101					
-1:	10001011001111100000111111nuuuu101					
0:	01001000101111011111001u1nuuu000	u1un11111101-----0----101n0u00nu	7	0.00	0.00	0.00
1:	n10u01101101-----1u1--010n10111n	11nu100-----11---0-00--01000n101	4	0.00	0.00	0.00
2:	1111nnnnnnnnn10-0-1n--0nu0nn011	1111000110----01--0--0111n1001un	0	0.00	0.00	4.00
3:	11un0011u1010101nnnn0uun00unu1nu	nn1u1101110--------001-01uuu10n0	1	0.00	0.00	4.00
4:	000001111uu10n0n-n1n1n11000110u1	n1nu1000010-1-------11--011u1000	1	-5.00	-5.00	5.00
5:	u011nu11n0110011u11-n10nu010000u	nuuu10000101-------110---un000u1	0	0.00	0.00	0.00
6:	0100nuuuuuuuuuuu10010un11u0u0nn	uu10010001111000---------n1101u1	3	0.00	0.00	0.00
7:	00000100111010010n--u-nun11u0010	111111000111-------1-10-11nn0111	2	0.00	0.00	0.00
8:	n0110010111000000000-11-01011001	nnn1011000------------111u1100n1	8	0.00	0.00	0.00
9:	111110001000-------1-01110110000	01n0000-1---------------0uu10111	7	-1.00	-0.96	6.99
10:	n0011100000000-------0-u010unnn1	nuu1010000------------01n11101n	10	-4.00	-0.83	12.99
11:	1010101010101----------un00011nn	11u110100---------------0n0u1101	12	-1.00	-0.83	18.99
12:	100010000001-----------011011n1	un01010-----------------1x11101n	8	-1.19	-1.18	29.99
13:	n1010100111111----------10111110	uun0100100---------------nuu00n0	9	-5.00	-0.91	36.80
14:	01010000100001-----------1010n00	n0u001011----------------01111nu	2	-0.02	-0.02	40.80
15:	n10000100000101110-------0001111	nn10100011111------------1n11u0	11	-2.23	-0.07	42.78
16:	001000011010010-----------1111n1	1nn0001011-1------------1u10110u	0	-0.00	0.00	51.54
17:	n00010010-----------------101001	nn00000-----------------01un11u1	0	-3.42	-1.09	51.54
18:	0010--110-----------------11001	11u010100000-0-----------001010u	0	-0.13	-0.13	48.13
19:	-001----------------------100--	nu111010----------------100101u0	0	0.00	0.00	48.00
20:	----------------------------00u-	nun100------------------n1101n0	0	-1.00	-1.00	48.00
21:	----------------------------n-	0un011100---------------0u0000u1	0	0.00	0.00	47.00
22:	----------	n101101-----------------110110u1	0	0.00	0.00	47.00
23:	----------	10001-0-----------------1010101	0	0.00	-0.00	47.00
24:	----------	01011101----------------111001011	0	0.00	-0.00	47.00
25:	----------	u10000-----------------110111101	0	0.00	0.00	47.00
26:	----------	0000-11-1--------------1-00000n1	0	-1.00	-1.00	47.00
27:	----------------------------n-	0010100-----------------1u100000	0	0.00	0.00	46.00
28:	----------	01000-------------------0011100	0	-2.00	-2.00	46.00
29:	----------------------------u-	n10-00-0----------------n111001	0	0.00	0.00	44.00
30:	----------	u01010------------------11010111	0	-2.00	-2.00	44.00
31:	----------------------------u-	1100----0---------------n010001	0	0.00	0.00	42.00
32:	----------	u1-01-1----------------00001010n	0	-2.00	-2.00	42.00
33:	----------------------------u	00100-1----------------10nu00110	0	0.00	0.00	40.00
34:	----------	u11---------------------0011000un	0	-1.00	-1.00	40.00
35:	----------	1x10-1-----------------0010000u1	0	-2.00	-1.00	39.00
36:	----------------------------u-	uu01-0-----------------11n101010	0	-1.00	-1.00	37.00
37:	----------	uu---01----------------1100110u0	0	-1.00	-1.00	36.00
38:	----------	x00-0-------------------100001000	0	0.00	-0.00	35.00
39:	----------	u01-0-------------------010100110	0	0.00	-0.00	35.00
40:	----------	u----1----------------1-100010n0	0	-1.00	-1.00	35.00
41:	----------------------------n-	10-1---------------------01u10011-	0	0.00	0.00	34.00
42:	----------	00-1---------------------0101100u0	0	-1.00	-1.00	34.00
43:	----------	x--00--------------------00100100	0	-1.00	-1.00	33.00
44:	----------	n-0-0-1----------------000011-1	0	-1.00	-1.00	32.00
45:	----------	u-1----1---------------100000000	0	0.00	0.00	31.00
46:	----------	---0-1----------------1110111u-	0	-1.00	-0.42	31.00
47:	----------------------------u-	-0---1-------------------0n111-00	0	0.00	0.00	30.00
48:	----------	-0--------------------111111100	0	-2.00	-2.00	30.00
49:	----------------------------u-	x01---------------------001n1110--	0	-1.00	-1.00	28.00
50:	----------	n-----------------------01000-1n-	0	-2.00	-2.00	27.00
51:	----------	1-----------------------00000001-	0	-1.00	-1.00	25.00
52:	----------	x1-0--------------------000101---	0	-1.00	-1.00	24.00
53:	----------	x--0---------------------01011-00-1	0	0.00	0.00	23.00
54:	----------	------------------------0101110-1	0	0.00	0.00	23.00
55:	----------	1-----------------------01010---0	0	0.00	0.00	23.00
56:	----------	1-1---------------------101-01-1-	0	0.00	0.00	23.00
57:	----------	------------------------110000-1-	0	0.00	0.00	23.00
58:	----------	-1----------------------1001----1	0	0.00	0.00	23.00
59:	----------	-0----------------------01-01-0--	0	0.00	0.00	23.00
60:	----------	------------------------01111-n--	0	-1.00	-0.19	23.00
61:	----------------------------n--	------------------------0u1---10-	0	0.00	0.00	22.00
62:	----------	------------------------00-00-0x--	0	-1.00	0.00	22.00
63:	----------	------------------------1101-n--x	0	-2.00	-0.19	21.00
64:	----------------------------n---	------------------01010u1----u-u	0	-2.00	-1.42	19.00
65:	----------------------------u--	--------------------101-n1-1x--u	0	-1.00	0.00	17.00
66:	----------	--------------------1110001-u-xx-	0	-3.00	-0.36	16.00
67:	----------------------------u----	--------------------00n0---0u-xx	0	-3.00	-0.42	13.00
68:	----------------------------u---	--------------------0--n0-1xu-ux	0	-3.00	-0.42	10.00
69:	----------------------------u---	----------------------11n1-u-xx-n	0	-3.00	-0.36	7.00
70:	----------------------------u-----	--------------------n1----uxnx-	0	-4.00	-1.83	4.00
71:	----------------------------u---	------------------------n1-1x--u--	0	-3.00	-0.35	1.00
72:	----------------------n----u---					

Table 5. Characteristic used for the first block of the 73-step collision

i	∇A_i	∇W_i	F_W	$P_u(i)$	$P_c(i)$	$N_s(i)$
-4:	00001111010010111000011111000011					
-3:	01000000110010010101000111011000					
-2:	01100010111010110111001111111010					
-1:	11101111110011011010101110001001					
0:	01100111010001010010001100000001	n00n00000000---------1010nuu1010	8	-0.50	0.00	0.00
1:	u0nu11111011------0--101111n1101	n1nu000----------------10u1n10un	7	-0.09	-0.08	0.08
2:	u01n1110100100----1-0--nnn10101n	00nu0101-------1-------00110u010	4	0.00	0.00	5.40
3:	010u0100111111101n--u--100nuu0n0	001110011111----------10n0100nu	5	-0.11	-0.05	9.40
4:	nn1n1n0000001nnn---0--n110000000	uu0u10101---------------1uuu10u1	3	-1.00	-1.00	14.29
5:	10u100uu1un10-100n--u-011u000u00	n1nn0011-10--------------10n1110	2	0.00	0.00	16.29
6:	0n0001000011n0n110--u-1010000010	uuun11000111-------------un101n0	2	-2.23	-2.23	18.29
7:	n1u1111100n00101uu01-nnn-1u11001	un101111011011--1--------u0110u0	1	-2.00	-2.00	18.05
8:	0nnn1110nnn1110u1n0u0-100u0nun00	1000010111010100---------0un0001	1	-2.00	-2.00	17.05
9:	101unnnnnnnnnnnnnnnn0-0101110u1	unu000010100-------------n1001u0	4	0.00	0.00	16.05
10:	1011011111000000--1100u--100u110	10u000001101-00----------un01001	2	-1.00	-1.00	20.05
11:	1100010000110111110 0unn--11n111n	unn1001001011011---------n-1000n	5	-1.00	-1.00	21.05
12:	n1110111100111111-----01110111n1	00u010011111-------------x1u0110	14	-3.11	0.00	25.05
13:	00101000001-----------11---100n1	un001010-----------------n001-0u	13	-5.00	-1.83	35.94
14:	u0010000100----------------10-nn	nnu1111------------------xun00n1	2	-3.00	-1.00	43.94
15:	11110011010000000----------11n10	u0n011100000-------------0-010un	11	-3.93	-1.50	42.94
16:	n1001110111111--------------0011	nn1101000----------------111u-0n0	0	-0.00	0.00	50.01
17:	11110100--------------------1n1	1uu011101----------------u11100u	0	-0.01	0.00	50.01
18:	n10-------------------------010	uu00001------------------1-un01n1	0	-1.00	-0.91	50.00
19:	--1----------------------------	10u1100-----------------0-1-111u	0	0.00	0.00	49.00
20:	----------------------------	uu100011-----------------10000n1	0	-1.00	-1.00	49.00
21:	----------------------------n-	nun010-0-----------------u11-0n1	0	-2.00	-2.00	48.00
22:	----------------------------n-	1un111-1-----------------u-101u1	0	-1.00	-1.00	46.00
23:	----------------------------	u100011-----------------0-1011u0	0	-1.00	-1.00	45.00
24:	----------------------------	10110-1-----------------11010010	0	0.00	-0.00	44.00
25:	----------------------------	00000-0-----------------0-110000	0	0.00	0.00	44.00
26:	----------------------------	n00110------------------1101001	0	0.00	0.00	44.00
27:	----------------------------	0010-10--------------------0-0n0	0	-1.00	-1.00	44.00
28:	----------------------------n-	1110-00-----------------u001101	0	0.00	0.00	43.00
29:	----------------------------	10101--------------------0-1--110	0	-2.00	-2.00	43.00
30:	----------------------------n-	u11-0--------------------u011101	0	0.00	0.00	41.00
31:	----------------------------	u00-11-1-----------------100000	0	-2.00	-2.00	41.00
32:	----------------------------n-	1101---1----------------10u-00011	0	0.00	0.00	39.00
33:	----------------------------	n1-00-0------------------1-1011u	0	-2.00	-2.00	39.00
34:	----------------------------n	01-01-1------------------0un11011	0	0.00	0.00	37.00
35:	----------------------------	n00----------------------00-010un	0	-1.00	-1.00	37.00
36:	----------------------------	0x1----------------------1000110n1	0	-2.00	-1.00	36.00
37:	----------------------------n-	ux01-1-------------------1u-00100	0	-1.00	0.00	34.00
38:	----------------------------	nn---01------------------0101001n1	0	-1.00	-1.00	33.00
39:	----------------------------	x11-1--------------------1001110	0	0.00	0.00	32.00
40:	----------------------------	x10-0--------------------01111001	0	-1.00	-1.00	32.00
41:	----------------------------	u----1-------------------10-01n0	0	-1.00	-1.00	31.00
42:	----------------------------n-	1------1----------------0u10001-	0	0.00	-0.00	30.00
43:	----------------------------	10-1---------------------1-110u-	0	-1.00	-1.00	30.00
44:	----------------------------	x--11--------------------10-11011	0	-1.00	-1.00	29.00
45:	----------------------------	u-0-1-0------------------0---00-0	0	-1.00	-1.00	28.00
46:	----------------------------	n-1----1----------------100000-1	0	0.00	0.00	27.00
47:	----------------------------	---1---------------------00001n-	0	-1.00	-0.42	27.00
48:	----------------------------n-	-----1-----------------0-u-00-1-	0	0.00	-0.00	26.00
49:	----------------------------	-1----------------------000-10-01	0	-2.00	-2.00	26.00
50:	----------------------------n-	x01----------------------0u0010--	0	-1.00	-1.00	24.00
51:	----------------------------	u----------------------0-1110-1u-	0	-2.00	-2.00	23.00
52:	----------------------------	0----------------------00010-10-	0	-1.00	-1.00	21.00
53:	----------------------------	x0---------------------1--0-00---	0	-1.00	-1.00	20.00
54:	----------------------------	x--0--------------------1011-0---	0	0.00	0.00	19.00
55:	----------------------------	------------------------01--01-1	0	0.00	0.00	19.00
56:	----------------------------	1------------------------01011---0	0	0.00	0.00	19.00
57:	----------------------------	0-1----------------------11-10-1-	0	0.00	0.00	19.00
58:	----------------------------	------------------------111-01-0-	0	0.00	0.00	19.00
59:	----------------------------	------------------------1-----0	0	0.00	0.00	19.00
60:	----------------------------	-0-----------------------11-0-----	0	0.00	0.00	19.00
61:	----------------------------	--------------------------1-n--	0	-1.00	-0.19	19.00
62:	----------------------------n--	------------------------0u1---10-	0	0.00	0.00	18.00
63:	----------------------------	------------------------0--11-0x--	0	-1.00	0.00	18.00
64:	----------------------------	----------------------1-1-10-n--x	0	-2.00	-0.19	17.00
65:	----------------------------n---	----------------------00u1----n-x	0	-2.00	-0.42	15.00
66:	----------------------------n--	----------------------00-u---x--u	0	-1.00	-0.00	13.00
67:	----------------------------	----------------------1--11-n-xx-	0	-3.00	-0.36	12.00
68:	--------------------------n----	----------------------u0---0n-xx	0	-3.00	-0.42	9.00
69:	--------------------------n---	----------------------1-u0-0xn-ux	0	-3.00	-0.42	6.00
70:	--------------------------n---	----------------------u1-n-xx-u	0	-3.00	-0.36	3.00
71:	-------------------------n-----	----------------------u-----nxxx-	0	-4.00	-0.91	0.00
72:	--------------------------n----	----------------------u---x--u--	0	-1.00	-0.00	0.00
73:	----------------------------					

Table 6. Characteristic used for the second block of the 73-step collision

i	∇A_i	∇W_i	F_W	$P_u(i)$	$P_c(i)$	$N_s(i)$
-4:	10001100111100100101001001 01n011					
-3:	00101100000110100100011010 1nu101					
-2:	11001100000010001010001111 n01010					
-1:	10000010010100111111101110 n10101					
0:	11000101100010001011 1nu00n000001	n11n11010000111011011 0001uun0111	0	0.00	0.00	0.00
1:	n01n011011101011nu010nnnn0nn0110	n1uu100110011----010---01u0n00nu	3	0.00	0.00	0.00
2:	nu1n11110001n0nu-110u--1101u1u0n	00un1100000-110---1--1001011n001	1	0.00	0.00	1.87
3:	0111110n01n0010u1u11-un11nun1nu0	10001111000110-------1-01u1110un	3	0.00	0.00	2.87
4:	1110u10001u0001-01-u-0001u000111	nn1u110111----------------nnu10n0	2	0.00	0.00	5.87
5:	001unnnnnn1nnnn-n011-u1n01n1100u	n1un01111--001-----0110-000n1110	0	0.00	0.00	7.87
6:	111011111001nnnnnnnn0n00n0u11000	unun11101001----0--------uu101n0	1	0.00	0.00	7.87
7:	u1010101111nuuuu10-nu01n010n110n	un01000011000----------11n0000u0	1	-1.00	-1.00	8.87
8:	10100100010101000u00-n0n01100nn	00000111110-------1----101uu0000	0	0.00	0.00	8.87
9:	00000001110101000010n10111nu100	nnn1100110001000---0---00n1001u0	4	-0.19	0.00	8.87
10:	n011101010000101---01-u01111001u	10u00010000----------1000nn01111	10	-1.60	-0.30	12.68
11:	10111110010----------un0001u1100	nuu000-0----------------0u10111n	13	-1.00	-0.68	21.07
12:	u011110011----------1111100n0	11n111101----------------n1u0011	11	-4.00	-3.83	33.07
13:	100011001011----------1-01011u0	nu1111000----------------u01111u	6	-2.00	-1.98	40.07
14:	u10111010001100----------00100nn	nnu1101001111----------xun01n0	10	-3.00	-1.42	44.07
15:	001101011111--------------000n01	n1n11001----------------00100nu	9	-5.00	-0.91	51.07
16:	n10001011000--------------1001011	nu110101----------------111u00u0	0	-2.00	-0.06	55.07
17:	01100111---0---------------110n1	1nu0101011101----------u11001u	0	-0.07	-0.06	53.07
18:	n00---0--------------------00111	uu01010----------------01un11u1	0	-1.00	-0.91	53.00
19:	-10-----------------------111--	11u11-1-0--------------01101000u	0	0.00	0.00	52.00
20:	----------------------------10--	uu001110----------------010110n1	0	-2.00	-2.00	52.00
21:	---------------------------0-n-	unu111----------------0u1110n0	0	-2.00	-2.00	50.00
22:	--------------------------------n-	1un1-0-0----------------u1000u0	0	0.00	0.00	48.00
23:	----------------------------------	n011110----------------110110n0	0	0.00	0.00	48.00
24:	----------------------------------	11011----------------0111101010	0	0.00	-0.00	48.00
25:	----------------------------------	000-0-1----------------110110010	0	0.00	0.00	48.00
26:	----------------------------------	n01010----------------00010111	0	0.00	0.00	48.00
27:	----------------------------------	0111-10----------------000101n0	0	-1.00	-1.00	48.00
28:	----------------------------n-	01-1-0--0----------------u111000	0	0.00	0.00	47.00
29:	----------------------------------	01100----------------01000011	0	-2.00	-2.00	47.00
30:	----------------------------n-	u10-0----------------u000001	0	0.00	0.00	45.00
31:	----------------------------------	n-1-1----------------10000101	0	-2.00	-2.00	45.00
32:	----------------------------n-	0011---1----------------00u101000	0	0.00	0.00	43.00
33:	----------------------------------	n0-00----------------01010001u	0	-2.00	-2.00	43.00
34:	----------------------------n	-0-1----------------10un01000	0	0.00	0.00	41.00
35:	----------------------------------	n00----------------11101010un	0	-1.00	-1.00	41.00
36:	----------------------------------	1x0---1----------------1110000n0	0	-2.00	-1.00	40.00
37:	----------------------------n-	ux1--1----------------110u01011-	0	-1.00	0.00	38.00
38:	----------------------------------	un---1----------------1110001u1	0	-1.00	-1.00	37.00
39:	----------------------------------	x01-1----------------1001011111	0	0.00	0.00	36.00
40:	----------------------------------	x1--1----------------1100001-0	0	-1.00	-1.00	36.00
41:	----------------------------------	u----0----------------1100001n1	0	-1.00	-1.00	35.00
42:	----------------------------n-	1------1----------------1u11000-	0	0.00	-0.00	34.00
43:	----------------------------------	1--0----------------011110-u-	0	-1.00	-1.00	34.00
44:	----------------------------------	x--11----------------111111001	0	-1.00	-1.00	33.00
45:	----------------------------------	n-1-1-0----------------0110000-0	0	-1.00	-1.00	32.00
46:	----------------------------------	x-0----0----------------0011-0-1	0	0.00	-0.00	31.00
47:	----------------------------------	---10----------------1000000n-	0	-1.00	-0.42	31.00
48:	----------------------------n-	--0--1----------------001u001-0-	0	0.00	-0.00	30.00
49:	----------------------------------	-1----------------1011-1-1-	0	-2.00	-1.42	30.00
50:	----------------------------n-	x00----------------01u1100--	0	-1.00	-1.00	28.00
51:	----------------------------------	u----------------011000-1u-	0	-2.00	-2.00	27.00
52:	----------------------------------	0----------------0100-0-0--	0	-1.00	-1.00	25.00
53:	----------------------------------	x1----------------1001110---	0	-1.00	-1.00	24.00
54:	----------------------------------	x--0----------------1111-1---	0	0.00	0.00	23.00
55:	----------------------------------	----------------111-1-0--0	0	0.00	0.00	23.00
56:	----------------------------------	1----------------11001---1	0	0.00	0.00	23.00
57:	----------------------------------	0-0----------------1111-01-0-	0	0.00	0.00	23.00
58:	----------------------------------	----------------0-0-1--0-	0	0.00	0.00	23.00
59:	----------------------------------	----------------00010----1	0	0.00	0.00	23.00
60:	----------------------------------	-1----------------00-0-----	0	0.00	0.00	23.00
61:	----------------------------------	----------------1-0-0--n--	0	-1.00	-0.19	23.00
62:	----------------------------n--	----------------0u0---10-	0	0.00	0.00	22.00
63:	----------------------------------	----------------11-00-1x--	0	-1.00	0.00	22.00
64:	----------------------------------	----------------011-1-1--n--x	0	-2.00	-0.19	21.00
65:	----------------------------n---	----------------0001u0----n-x	0	-2.00	-0.42	19.00
66:	----------------------------n--	----------------0000-u---x--u	0	-1.00	-0.00	17.00
67:	----------------------------------	----------------1-0-1--n-xx-	0	-3.00	-0.36	16.00
68:	--------------------------n-----	----------------1u1---0u-xx	0	-3.00	-0.42	13.00
69:	--------------------------u----	----------------1-n1-1xu-ux	0	-3.00	-0.42	10.00
70:	--------------------------u----	----------------n--u-xx-u	0	-3.00	-0.36	7.00
71:	-------------------------u-----	----------------n0----uuxx-	0	-4.00	-1.00	4.00
72:	-------------------------u-----	----------------0-n---u--u--	0	-3.00	-1.15	1.00
73:	---------------------u--u------					