A MD5 compression function constants

Table A-1: *MD5 Addition and Rotation Constants and message block expansion.*

t	AC_t	RC_t	W_t
0	$\texttt{d76aa478}_{16}$	7	m_0
1	$\texttt{e8c7b756}_{16}$	12	m_1
2	$\texttt{242070db}_{16}$	17	m_2
3	$\texttt{c1bdceee}_{16}$	22	m_3
4	$\texttt{f57c0faf}_{16}$	7	m_4
5	$\texttt{4787c62a}_{16}$	12	m_5
6	$\texttt{a8304613}_{16}$	17	m_6
7	$\texttt{fd469501}_{16}$	22	m_7
8	$\texttt{698098d8}_{16}$	7	m_8
9	$\texttt{8b44f7af}_{16}$	12	m_9
10	$\texttt{ffff5bb1}_{16}$	17	m_{10}
11	$\texttt{895cd7be}_{16}$	22	m_{11}
12	$\texttt{6b901122}_{16}$	7	m_{12}
13	$\texttt{fd987193}_{16}$	12	m_{13}
14	$\texttt{a679438e}_{16}$	17	m_{14}
15	$\texttt{49b40821}_{16}$	22	m_{15}

t	AC_t	RC_t	W_t
16	$\texttt{f61e2562}_{16}$	5	m_1
17	$\texttt{c040b340}_{16}$	9	m_6
18	$\texttt{265e5a51}_{16}$	14	m_{11}
19	$\texttt{e9b6c7aa}_{16}$	20	m_0
20	$\texttt{d62f105d}_{16}$	5	m_5
21	$\texttt{02441453}_{16}$	9	m_{10}
22	$\texttt{d8a1e681}_{16}$	14	m_{15}
23	$\texttt{e7d3fbc8}_{16}$	20	m_4
24	$\texttt{21e1cde6}_{16}$	5	m_9
25	$\texttt{c33707d6}_{16}$	9	m_{14}
26	$\texttt{f4d50d87}_{16}$	14	m_3
27	$\texttt{455a14ed}_{16}$	20	m_8
28	$\texttt{a9e3e905}_{16}$	5	m_{13}
29	$\texttt{fcefa3f8}_{16}$	9	m_2
30	$\texttt{676f02d9}_{16}$	14	m_7
31	$\texttt{8d2a4c8a}_{16}$	20	m_{12}

t	AC_t	RC_t	W_t
32	$\texttt{fffa3942}_{16}$	4	m_5
33	$\texttt{8771f681}_{16}$	11	m_8
34	$\texttt{6d9d6122}_{16}$	16	m_{11}
35	$\texttt{fde5380c}_{16}$	23	m_{14}
36	$\texttt{a4beea44}_{16}$	4	m_1
37	$\texttt{4bdecfa9}_{16}$	11	m_4
38	$\texttt{f6bb4b60}_{16}$	16	m_7
39	$\texttt{bebfbc70}_{16}$	23	m_{10}
40	$\texttt{289b7ec6}_{16}$	4	m_{13}
41	$\texttt{eaa127fa}_{16}$	11	m_0
42	$\texttt{d4ef3085}_{16}$	16	m_3
43	$\texttt{04881d05}_{16}$	23	m_6
44	$\texttt{d9d4d039}_{16}$	4	m_9
45	$\texttt{e6db99e5}_{16}$	11	m_{12}
46	$\texttt{1fa27cf8}_{16}$	16	m_{15}
47	$\texttt{c4ac5665}_{16}$	23	m_2

t	AC_t	RC_t	W_t
48	$\texttt{f4292244}_{16}$	6	m_0
49	$\texttt{432aff97}_{16}$	10	m_7
50	$\texttt{ab9423a7}_{16}$	15	m_{14}
51	$\texttt{fc93a039}_{16}$	21	m_5
52	$\texttt{655b59c3}_{16}$	6	m_{12}
53	$\texttt{8f0ccc92}_{16}$	10	m_3
54	$\texttt{ffeff47d}_{16}$	15	m_{10}
55	$\texttt{85845dd1}_{16}$	21	m_1
56	$\texttt{6fa87e4f}_{16}$	6	m_8
57	$\texttt{fe2ce6e0}_{16}$	10	m_{15}
58	$\texttt{a3014314}_{16}$	15	m_6
59	$\texttt{4e0811a1}_{16}$	21	m_{13}
60	$\texttt{f7537e82}_{16}$	6	m_4
61	$\texttt{bd3af235}_{16}$	10	m_{11}
62	$\texttt{2ad7d2bb}_{16}$	15	m_2
63	$\texttt{eb86d391}_{16}$	21	m_9

B MD5 and SHA-1 bitconditions

Table B-1: *Bitconditions for MD5 and SHA-1.*

$\mathtt{q_t[i]}$	condition on $(\mathbf{Q_t[i]}, \mathbf{Q'_t[i]})$	direct/indirect	direction
`.`	$Q_t[i] = Q'_t[i]$	direct	
`+`	$Q_t[i] = 0, \quad Q'_t[i] = 1$	direct	
`-`	$Q_t[i] = 1, \quad Q'_t[i] = 0$	direct	
`0`	$Q_t[i] = Q'_t[i] = 0$	direct	
`1`	$Q_t[i] = Q'_t[i] = 1$	direct	
`^`	$Q_t[i] = Q'_t[i] = Q_{t-1}[i]$	indirect	backward
`v`	$Q_t[i] = Q'_t[i] = Q_{t+1}[i]$	indirect	forward
`!`	$Q_t[i] = Q'_t[i] = \overline{Q_{t-1}[i]}$	indirect	backward
`y`	$Q_t[i] = Q'_t[i] = \overline{Q_{t+1}[i]}$	indirect	forward
`m`	$Q_t[i] = Q'_t[i] = Q_{t-2}[i]$	indirect	backward
`w`	$Q_t[i] = Q'_t[i] = Q_{t+2}[i]$	indirect	forward
`#`	$Q_t[i] = Q'_t[i] = \overline{Q_{t-2}[i]}$	indirect	backward
`h`	$Q_t[i] = Q'_t[i] = \overline{Q_{t+2}[i]}$	indirect	forward
`?`	$Q_t[i] = Q'_t[i] \wedge (Q_t[i] = 1 \vee Q_{t-2}[i] = 0)$	indirect	backward
`q`	$Q_t[i] = Q'_t[i] \wedge (Q_{t+2}[i] = 1 \vee Q_t[i] = 0)$	indirect	forward
`r`	$Q_t[i] = Q'_t[i] = RL(Q_{t-1}, 30)[i]$	indirect	backward
`u`	$Q_t[i] = Q'_t[i] = RR(Q_{t+1}, 30)[i]$	indirect	forward
`R`	$Q_t[i] = Q'_t[i] = \overline{RL(Q_{t-1}, 30)[i]}$	indirect	backward
`U`	$Q_t[i] = Q'_t[i] = \overline{RR(Q_{t+1}, 30)[i]}$	indirect	forward
`s`	$Q_t[i] = Q'_t[i] = RL(Q_{t-2}, 30)[i]$	indirect	backward
`c`	$Q_t[i] = Q'_t[i] = RR(Q_{t+2}, 30)[i]$	indirect	forward
`S`	$Q_t[i] = Q'_t[i] = \overline{RL(Q_{t-2}, 30)[i]}$	indirect	backward
`C`	$Q_t[i] = Q'_t[i] = \overline{RR(Q_{t+2}, 30)[i]}$	indirect	forward

Note: these conditions are tailored for the boolean functions of MD5 and the first and second round boolean function of SHA-1.

C MD5 boolean function bitconditions

The four tables in this appendix correspond to the four rounds of MD5, i.e., $0 \leq t < 16$, $16 \leq t < 32$, $32 \leq t < 48$ and $48 \leq t < 64$. The '$\mathfrak{abc}$' in each of the first columns denotes the three differential bitconditions $(\mathfrak{q}_t[i], \mathfrak{q}_{t-1}[i], \mathfrak{q}_{t-2}[i])$ for the relevant t and $0 \leq i \leq 31$, with each table containing all 27 possible triples. Columns $2, 3, 4$ contain forward bitconditions $FC(t, \mathfrak{abc}, g)$ for $g = 0, +1, -1$, respectively, and columns $5, 6, 7$ contain backward bitconditions $BC(t, \mathfrak{abc}, g)$ for those same g-values, respectively. The parenthesized number next to a triple $\mathfrak{def}$ is $|U_{\mathfrak{def}}|$, the amount of freedom left. An entry is left empty if $g \notin V_{t,\mathfrak{abc}}$. We refer to Section 6.2.2 for more details.

C.1 Bitconditions applied to boolean function F

Table C-1: *Round 1 ($0 \leq t < 16$) bitconditions applied to boolean function F:*

$$F(X, Y, Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z)$$

D.B.	Forward bitconditions			Backward bitconditions		
abc	$g = 0$	$g = +1$	$g = -1$	$g = 0$	$g = +1$	$g = -1$
... (8)	... (8)			... (8)		
..+ (4)	1.+ (2)	0.+ (2)		1.+ (2)	0.+ (2)	
..- (4)	1.- (2)		0.- (2)	1.- (2)		0.- (2)
.+. (4)	0+. (2)	1+. (2)		0+. (2)	1+. (2)	
.++ (2)		.++ (2)			.++ (2)	
.+- (2)		1+- (1)	0+- (1)		1+- (1)	0+- (1)
.-. (4)	0-. (2)		1-. (2)	0-. (2)		1-. (2)
.-+ (2)		0-+ (1)	1-+ (1)		0-+ (1)	1-+ (1)
.-- (2)			.-- (2)			.-- (2)
+.. (4)	+.v (2)	+10 (1)	+01 (1)	+^. (2)	+10 (1)	+01 (1)
+.+ (2)	+0+ (1)	+1+ (1)		+0+ (1)	+1+ (1)	
+.- (2)	+1- (1)		+0- (1)	+1- (1)		+0- (1)
++. (2)	++1 (1)	++0 (1)		++1 (1)	++0 (1)	
+++ (1)		+++ (1)			+++ (1)	
++- (1)	++- (1)			++- (1)		
+-. (2)	+-0 (1)		+-1 (1)	+-0 (1)		+-1 (1)
+-+ (1)	+-+ (1)			+-+ (1)		
+-- (1)			+-- (1)			+-- (1)
-.. (4)	-.v (2)	-01 (1)	-10 (1)	-^. (2)	-01 (1)	-10 (1)
-.+ (2)	-1+ (1)	-0+ (1)		-1+ (1)	-0+ (1)	
-.- (2)	-0- (1)		-1- (1)	-0- (1)		-1- (1)
-+. (2)	-+0 (1)	-+1 (1)		-+0 (1)	-+1 (1)	
-++ (1)		-++ (1)			-++ (1)	
-+- (1)	-+- (1)			-+- (1)		
--. (2)	--1 (1)		--0 (1)	--1 (1)		--0 (1)
--+ (1)	--+ (1)			--+ (1)		
--- (1)			--- (1)			--- (1)

C.2 Bitconditions applied to boolean function G

Table C-2: *Round 2 ($16 \leq t < 32$) bitconditions applied to boolean function G:*

$$G(X, Y, Z) = (Z \wedge X) \oplus (\overline{Z} \wedge Y)$$

D.B.		Forward bitconditions						Backward bitconditions					
abc		$g = 0$		$g = +1$		$g = -1$		$g = 0$		$g = +1$		$g = -1$	
...	(8)	...	(8)					...	(8)				
..+	(4)	.v+	(2)	10+	(1)	01+	(1)	^.+	(2)	10+	(1)	01+	(1)
..-	(4)	.v-	(2)	01-	(1)	10-	(1)	^.-	(2)	01-	(1)	10-	(1)
.+.	(4)	.+1	(2)	.+0	(2)			.+1	(2)	.+0	(2)		
.++	(2)	0++	(1)	1++	(1)			0++	(1)	1++	(1)		
.+-	(2)	1+-	(1)	0+-	(1)			1+-	(1)	0+-	(1)		
.-.	(4)	.-1	(2)			.-0	(2)	.-1	(2)			.-0	(2)
.-+	(2)	1-+	(1)			0-+	(1)	1-+	(1)			0-+	(1)
.--	(2)	0--	(1)			1--	(1)	0--	(1)			1--	(1)
+..	(4)	+.0	(2)	+.1	(2)			+.0	(2)	+.1	(2)		
+.+	(2)	+1+	(1)	+0+	(1)			+1+	(1)	+0+	(1)		
+.-	(2)	+0-	(1)	+1-	(1)			+0-	(1)	+1-	(1)		
++.	(2)			++.	(2)					++.	(2)		
+++	(1)			+++	(1)					+++	(1)		
++-	(1)			++-	(1)					++-	(1)		
+-.	(2)			+-1	(1)	+-0	(1)			+-1	(1)	+-0	(1)
+-+	(1)	+-+	(1)					+-+	(1)				
+--	(1)	+--	(1)					+--	(1)				
-..	(4)	-.0	(2)			-.1	(2)	-.0	(2)			-.1	(2)
-.+	(2)	-0+	(1)			-1+	(1)	-0+	(1)			-1+	(1)
-.-	(2)	-1-	(1)			-0-	(1)	-1-	(1)			-0-	(1)
-+.	(2)			-+0	(1)	-+1	(1)			-+0	(1)	-+1	(1)
-++	(1)	-++	(1)					-++	(1)				
-+-	(1)	-+-	(1)					-+-	(1)				
--.	(2)					--.	(2)					--.	(2)
--+	(1)					--+	(1)					--+	(1)
---	(1)					---	(1)					---	(1)

C.3 Bitconditions applied to boolean function H

Table C-3: *Round 3 ($32 \leq t < 48$) bitconditions applied to boolean function H:*

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

D.B.	Forward bitconditions			Backward bitconditions		
abc	$g = 0$	$g = +1$	$g = -1$	$g = 0$	$g = +1$	$g = -1$
... (8)	... (8)			... (8)		
..+ (4)		.v+ (2)	.y+ (2)		^.+ (2)	!.+ (2)
..- (4)		.y- (2)	.v- (2)		!.- (2)	^.- (2)
.+. (4)		.+w (2)	.+h (2)		m+. (2)	#+. (2)
.++ (2)	.++ (2)			.++ (2)		
.+- (2)	.+- (2)			.+- (2)		
.-. (4)		.-h (2)	.-w (2)		#-. (2)	m-. (2)
.-+ (2)	.-+ (2)			.-+ (2)		
.-- (2)	.-- (2)			.-- (2)		
+.. (4)		+.v (2)	+.y (2)		+^. (2)	+!. (2)
+.+ (2)	+.+ (2)			+.+ (2)		
+.- (2)	+.- (2)			+.- (2)		
++. (2)	++. (2)			++. (2)		
+++ (1)		+++ (1)			+++ (1)	
++- (1)			++- (1)			++- (1)
+-. (2)	+-. (2)			+-. (2)		
+-+ (1)			+-+ (1)			+-+ (1)
+-- (1)		+-- (1)			+-- (1)	
-.. (4)		-.y (2)	-.v (2)		-!. (2)	-^. (2)
-.+ (2)	-.+ (2)			-.+ (2)		
-.- (2)	-.- (2)			-.- (2)		
-+. (2)	-+. (2)			-+. (2)		
-++ (1)			-++ (1)			-++ (1)
-+- (1)		-+- (1)			-+- (1)	
--. (2)	--. (2)			--. (2)		
--+ (1)		--+ (1)			--+ (1)	
--- (1)			--- (1)			--- (1)

C.4 Bitconditions applied to boolean function I

Table C-4: *Round 4 ($48 \leq t < 64$) bitconditions applied to boolean function I:*

$$I(X, Y, Z) = Y \oplus (X \vee \overline{Z})$$

D.B.		Forward bitconditions						Backward bitconditions					
abc		$g = 0$		$g = +1$		$g = -1$		$g = 0$		$g = +1$		$g = -1$	
...	(8)	...	(8)					...	(8)				
..+	(4)	1.+	(2)	01+	(1)	00+	(1)	1.+	(2)	01+	(1)	00+	(1)
..-	(4)	1.-	(2)	00-	(1)	01-	(1)	1.-	(2)	00-	(1)	01-	(1)
.+.	(4)			0+1	(1)	.+q	(3)			0+1	(1)	?+.	(3)
.++	(2)	0++	(1)			1++	(1)	0++	(1)			1++	(1)
.+-	(2)	0+-	(1)			1+-	(1)	0+-	(1)			1+-	(1)
.-.	(4)			.-q	(3)	0-1	(1)			?-.	(3)	0-1	(1)
.-+	(2)	0-+	(1)	1-+	(1)			0-+	(1)	1-+	(1)		
.--	(2)	0--	(1)	1--	(1)			0--	(1)	1--	(1)		
+..	(4)	+.0	(2)	+01	(1)	+11	(1)	+.0	(2)	+01	(1)	+11	(1)
+.+	(2)	+.+	(2)					+.+	(2)				
+.-	(2)			+0-	(1)	+1-	(1)			+0-	(1)	+1-	(1)
++.	(2)	++1	(1)			++0	(1)	++1	(1)			++0	(1)
+++	(1)					+++	(1)					+++	(1)
++-	(1)	++-	(1)					++-	(1)				
+-.	(2)	+-1	(1)	+-0	(1)			+-1	(1)	+-0	(1)		
+-+	(1)			+-+	(1)					+-+	(1)		
+--	(1)	+--	(1)					+--	(1)				
-..	(4)	-.0	(2)	-11	(1)	-01	(1)	-.0	(2)	-11	(1)	-01	(1)
-.+	(2)			-1+	(1)	-0+	(1)			-1+	(1)	-0+	(1)
-.-	(2)	-.-	(2)					-.-	(2)				
-+.	(2)	-+1	(1)			-+0	(1)	-+1	(1)			-+0	(1)
-++	(1)	-++	(1)					-++	(1)				
-+-	(1)					-+-	(1)					-+-	(1)
--.	(2)	--1	(1)	--0	(1)			--1	(1)	--0	(1)		
--+	(1)	--+	(1)					--+	(1)				
---	(1)			---	(1)					---	(1)		

D MD5 chosen-prefix collision birthday search cost

In this appendix notation and variables are as in Section 6.5.2. The columns p, C_{tr} and M denote the values $-\log_2(p_{r,k,w})$, $\log_2(C_{\text{tr}}(r,k,w))$ and the minimum required memory such that $C_{\text{coll}}(r,k,w,M) \leq C_{\text{tr}}(r,k,w)$, respectively.

$r=3$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0												
4										34.01	51.33	2TB
8							33.42	53.03	748GB	31.31	51.98	174GB
12	34.01	55.33	2TB	32.42	54.53	374GB	30.55	53.6	103GB	28.24	52.44	21GB
16	31.	55.83	141GB	29.65	55.15	55GB	27.36	54.01	12GB	25.6	53.13	4GB
20	27.51	56.08	13GB	26.18	55.42	5GB	24.53	54.59	2GB	23.26	53.96	673MB
24	24.33	56.49	2GB	23.35	56.	714MB	22.17	55.41	315MB	21.19	54.92	160MB
28	21.11	56.88	152MB	20.56	56.6	103MB	19.98	56.32	70MB	19.57	56.11	52MB
32	17.88	57.26	17MB	17.88	57.27	17MB	17.89	57.27	17MB	17.88	57.27	17MB

$r=3$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0				31.68	48.17	225GB	30.25	47.45	84GB	28.01	46.33	18GB
4	32.2	50.43	323GB	29.92	49.29	67GB	28.06	48.36	19GB	26.2	47.43	6GB
8	28.83	50.74	32GB	27.33	49.99	11GB	25.88	49.26	5GB	24.47	48.56	2GB
12	26.63	51.64	7GB	25.14	50.9	3GB	23.96	50.3	2GB	22.94	49.8	537MB
16	24.31	52.48	2GB	23.27	51.96	675MB	22.49	51.57	394MB	21.86	51.26	255MB
20	22.28	53.46	340MB	21.62	53.13	215MB	21.14	52.9	155MB	20.73	52.69	117MB
24	20.53	54.59	102MB	20.01	54.33	71MB	19.65	54.15	55MB	19.38	54.01	46MB
28	19.25	55.95	42MB	19.02	55.83	36MB	18.82	55.74	31MB	18.65	55.65	28MB
32	17.88	57.27	17MB	17.88	57.27	17MB	17.88	57.27	17MB	17.88	57.27	17MB

$r=4$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0							34.	49.33	2TB	30.19	47.42	81GB
4				33.42	51.04	749GB	30.36	49.51	90GB	27.59	48.12	14GB
8	35.	53.83	3TB	30.3	51.48	87GB	27.21	49.93	11GB	24.87	48.76	2GB
12	29.58	53.12	53GB	27.53	52.09	13GB	24.59	50.62	2GB	22.47	49.56	388MB
16	26.26	53.45	6GB	24.36	52.51	2GB	22.06	51.36	292MB	20.38	50.51	91MB
20	23.16	53.91	628MB	21.5	53.08	199MB	19.72	52.19	58MB	18.54	51.6	26MB
24	20.25	54.45	84MB	19.09	53.87	38MB	17.8	53.23	16MB	16.86	52.76	8MB
28	17.26	54.95	11MB	16.63	54.64	7MB	16.02	54.34	5MB	15.6	54.13	4MB
32	14.29	55.47	2MB	14.29	55.47	2MB	14.29	55.47	2MB	14.29	55.47	2MB

$r=4$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	26.98	45.81	9GB	24.45	44.55	2GB	22.14	43.4	310MB	20.33	42.49	88MB
4	24.95	46.8	3GB	22.82	45.73	493MB	21.04	44.84	144MB	19.55	44.1	52MB
8	22.63	47.64	432MB	20.92	46.79	133MB	19.58	46.12	53MB	18.56	45.61	26MB
12	20.67	48.66	112MB	19.41	48.03	47MB	18.45	47.55	24MB	17.71	47.18	15MB
16	19.08	49.86	37MB	18.19	49.42	21MB	17.56	49.1	13MB	17.08	48.86	10MB
20	17.66	51.16	14MB	17.09	50.87	10MB	16.7	50.67	8MB	16.39	50.52	6MB
24	16.25	52.45	6MB	15.82	52.24	4MB	15.54	52.09	4MB	15.33	51.99	3MB
28	15.31	53.98	3MB	15.09	53.87	3MB	14.93	53.79	3MB	14.78	53.72	2MB
32	14.29	55.47	2MB	14.29	55.47	2MB	14.29	55.47	2MB	14.29	55.47	2MB

$r=5$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	35.	49.83	3TB	31.2	47.92	161GB	27.13	45.89	10GB	23.74	44.2	938MB
4	33.42	51.04	749GB	28.47	48.56	25GB	24.63	46.64	2GB	21.58	45.12	210MB
8	28.61	50.63	27GB	25.61	49.13	4GB	22.	47.33	280MB	19.39	46.02	46MB
12	25.43	51.04	3GB	22.74	49.7	468MB	19.66	48.15	56MB	17.53	47.09	13MB
16	22.36	51.51	360MB	20.02	50.34	72MB	17.59	49.12	14MB	15.95	48.3	5MB
20	19.38	52.01	46MB	17.48	51.07	13MB	15.67	50.16	4MB	14.55	49.6	2MB
24	16.68	52.66	7MB	15.35	52.	3MB	14.06	51.36	2MB	13.17	50.91	1MB
28	13.92	53.29	2MB	13.22	52.93	1MB	12.61	52.63	1MB	12.21	52.43	1MB
32	11.2	53.92	1MB	11.2	53.93	1MB	11.2	53.92	1MB	11.2	53.93	1MB

$r=5$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	20.53	42.59	102MB	18.03	41.34	18MB	16.17	40.41	5MB	14.92	39.79	3MB
4	18.94	43.79	34MB	17.	42.82	9MB	15.57	42.11	4MB	14.53	41.59	2MB
8	17.27	44.96	11MB	15.79	44.22	4MB	14.75	43.7	2MB	14.01	43.33	2MB
12	15.92	46.28	5MB	14.84	45.75	2MB	14.09	45.37	2MB	13.56	45.11	1MB
16	14.8	47.73	2MB	14.06	47.35	2MB	13.55	47.1	1MB	13.18	46.92	1MB
20	13.79	49.22	1MB	13.31	48.98	1MB	12.99	48.82	1MB	12.76	48.7	1MB
24	12.64	50.64	1MB	12.29	50.47	1MB	12.07	50.36	1MB	11.91	50.28	1MB
28	11.95	52.3	1MB	11.76	52.2	1MB	11.62	52.14	1MB	11.5	52.07	1MB
32	11.2	53.92	1MB	11.2	53.93	1MB	11.2	53.92	1MB	11.2	53.93	1MB

$r=6$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	31.2	47.92	161GB	26.73	45.69	8GB	21.78	43.22	241MB	18.14	41.4	20MB
4	28.18	48.42	20GB	23.89	46.27	2GB	19.56	44.11	52MB	16.46	42.55	6MB
8	24.66	48.66	2GB	21.17	46.91	158MB	17.37	45.01	12MB	14.79	43.72	2MB
12	21.67	49.16	224MB	18.6	47.62	27MB	15.43	46.04	3MB	13.4	45.03	1MB
16	18.82	49.74	31MB	16.21	48.43	6MB	13.74	47.2	1MB	12.23	46.44	1MB
20	16.03	50.34	5MB	13.97	49.31	2MB	12.2	48.43	1MB	11.18	47.92	1MB
24	13.54	51.1	1MB	12.11	50.38	1MB	10.86	49.75	1MB	10.04	49.35	1MB
28	11.03	51.84	1MB	10.28	51.47	1MB	9.69	51.17	1MB	9.33	50.99	1MB
32	8.56	52.6	1MB	8.56	52.6	1MB	8.56	52.6	1MB	8.56	52.6	1MB

$r=6$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	15.12	39.88	3MB	13.05	38.85	1MB	11.73	38.19	1MB	10.91	37.78	1MB
4	14.05	41.35	2MB	12.44	40.55	1MB	11.39	40.02	1MB	10.7	39.68	1MB
8	12.92	42.79	1MB	11.73	42.19	1MB	10.95	41.8	1MB	10.44	41.54	1MB
12	12.01	44.33	1MB	11.14	43.9	1MB	10.57	43.61	1MB	10.2	43.42	1MB
16	11.25	45.95	1MB	10.64	45.64	1MB	10.24	45.45	1MB	9.98	45.32	1MB
20	10.53	47.59	1MB	10.14	47.39	1MB	9.89	47.27	1MB	9.72	47.19	1MB
24	9.59	49.12	1MB	9.31	48.98	1MB	9.14	48.9	1MB	9.04	48.85	1MB
28	9.09	50.87	1MB	8.93	50.79	1MB	8.82	50.74	1MB	8.73	50.69	1MB
32	8.56	52.6	1MB	8.56	52.6	1MB	8.56	52.6	1MB	8.56	52.6	1MB

$r=7$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	26.82	45.73	8GB	22.2	43.43	323MB	17.02	40.83	9MB	13.4	39.02	1MB
4	24.02	46.34	2GB	19.68	44.16	56MB	15.16	41.9	3MB	12.18	40.41	1MB
8	21.1	46.88	151MB	17.23	44.94	11MB	13.37	43.01	1MB	10.97	41.81	1MB
12	18.32	47.49	22MB	14.96	45.8	3MB	11.82	44.24	1MB	9.98	43.31	1MB
16	15.67	48.16	4MB	12.87	46.76	1MB	10.48	45.56	1MB	9.13	44.89	1MB
20	13.1	48.88	1MB	10.93	47.79	1MB	9.26	46.95	1MB	8.35	46.5	1MB
24	10.82	49.74	1MB	9.32	48.99	1MB	8.15	48.4	1MB	7.43	48.04	1MB
28	8.56	50.6	1MB	7.78	50.22	1MB	7.23	49.94	1MB	6.91	49.78	1MB
32	6.34	51.5	1MB	6.34	51.5	1MB	6.34	51.5	1MB	6.34	51.5	1MB

$r=7$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	10.8	37.73	1MB	9.25	36.95	1MB	8.35	36.5	1MB	7.84	36.25	1MB
4	10.13	39.39	1MB	8.9	38.78	1MB	8.17	38.41	1MB	7.74	38.19	1MB
8	9.42	41.03	1MB	8.5	40.57	1MB	7.94	40.3	1MB	7.61	40.13	1MB
12	8.82	42.74	1MB	8.15	42.4	1MB	7.74	42.19	1MB	7.48	42.07	1MB
16	8.31	44.48	1MB	7.84	44.24	1MB	7.55	44.1	1MB	7.37	44.01	1MB
20	7.82	46.23	1MB	7.51	46.08	1MB	7.32	45.99	1MB	7.21	45.93	1MB
24	7.06	47.86	1MB	6.84	47.75	1MB	6.72	47.69	1MB	6.66	47.65	1MB
28	6.71	49.68	1MB	6.58	49.62	1MB	6.5	49.58	1MB	6.43	49.54	1MB
32	6.34	51.5	1MB	6.34	51.5	1MB	6.34	51.5	1MB	6.34	51.5	1MB

$r=8$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	23.39	44.02	732MB	18.21	41.43	21MB	12.88	38.76	1MB	9.52	37.09	1MB
4	20.57	44.61	105MB	15.94	42.29	5MB	11.39	40.02	1MB	8.69	38.67	1MB
8	17.91	45.28	17MB	13.77	43.21	1MB	9.99	41.32	1MB	7.86	40.26	1MB
12	15.35	46.	3MB	11.78	44.22	1MB	8.79	42.72	1MB	7.17	41.91	1MB
16	12.91	46.78	1MB	10.	45.32	1MB	7.75	44.2	1MB	6.59	43.62	1MB
20	10.56	47.61	1MB	8.35	46.5	1MB	6.81	45.73	1MB	6.03	45.34	1MB
24	8.49	48.57	1MB	6.97	47.81	1MB	5.91	47.28	1MB	5.29	46.97	1MB
28	6.48	49.56	1MB	5.71	49.18	1MB	5.21	48.93	1MB	4.93	48.79	1MB
32	4.54	50.6	1MB	4.54	50.6	1MB	4.54	50.6	1MB	4.54	50.6	1MB

$r=8$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	7.45	36.05	1MB	6.37	35.51	1MB	5.8	35.23	1MB	5.5	35.08	1MB
4	7.06	37.85	1MB	6.18	37.42	1MB	5.71	37.18	1MB	5.45	37.05	1MB
8	6.63	39.64	1MB	5.96	39.31	1MB	5.6	39.12	1MB	5.39	39.02	1MB
12	6.26	41.46	1MB	5.77	41.21	1MB	5.49	41.07	1MB	5.34	40.99	1MB
16	5.94	43.29	1MB	5.59	43.12	1MB	5.39	43.02	1MB	5.28	42.97	1MB
20	5.61	45.13	1MB	5.38	45.01	1MB	5.25	44.95	1MB	5.18	44.92	1MB
24	5.01	46.83	1MB	4.85	46.75	1MB	4.77	46.71	1MB	4.73	46.69	1MB
28	4.78	48.71	1MB	4.68	48.67	1MB	4.62	48.64	1MB	4.58	48.62	1MB
32	4.54	50.6	1MB	4.54	50.6	1MB	4.54	50.6	1MB	4.54	50.6	1MB

$r=9$	$w=0$			$w=1$			$w=2$			$w=3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	20.16	42.4	79MB	14.62	39.64	2MB	9.38	37.02	1MB	6.46	35.56	1MB
4	17.56	43.1	13MB	12.63	40.64	1MB	8.26	38.45	1MB	5.93	37.29	1MB
8	15.09	43.87	3MB	10.75	41.7	1MB	7.2	39.92	1MB	5.41	39.03	1MB
12	12.73	44.69	1MB	9.06	42.86	1MB	6.3	41.47	1MB	4.96	40.81	1MB
16	10.51	45.58	1MB	7.57	44.11	1MB	5.53	43.09	1MB	4.57	42.61	1MB
20	8.39	46.52	1MB	6.2	45.43	1MB	4.83	44.74	1MB	4.2	44.42	1MB
24	6.53	47.59	1MB	5.05	46.85	1MB	4.12	46.39	1MB	3.63	46.14	1MB
28	4.77	48.71	1MB	4.05	48.35	1MB	3.61	48.13	1MB	3.4	48.02	1MB
32	3.14	49.9	1MB	3.14	49.9	1MB	3.14	49.9	1MB	3.14	49.9	1MB

$r=9$	$w=4$			$w=5$			$w=6$			$w=7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	4.95	34.8	1MB	4.25	34.45	1MB	3.92	34.28	1MB	3.76	34.21	1MB
4	4.73	36.69	1MB	4.15	36.4	1MB	3.87	36.26	1MB	3.74	36.2	1MB
8	4.49	38.57	1MB	4.04	38.35	1MB	3.82	38.24	1MB	3.72	38.18	1MB
12	4.28	40.47	1MB	3.94	40.3	1MB	3.78	40.21	1MB	3.69	40.17	1MB
16	4.09	42.37	1MB	3.85	42.25	1MB	3.73	42.19	1MB	3.67	42.16	1MB
20	3.88	44.27	1MB	3.72	44.19	1MB	3.64	44.15	1MB	3.6	44.13	1MB
24	3.42	46.04	1MB	3.32	45.99	1MB	3.27	45.96	1MB	3.25	45.95	1MB
28	3.28	47.97	1MB	3.21	47.93	1MB	3.18	47.92	1MB	3.16	47.9	1MB
32	3.14	49.9	1MB	3.14	49.9	1MB	3.14	49.9	1MB	3.14	49.9	1MB

$r = 10$	$w = 0$			$w = 1$			$w = 2$			$w = 3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	17.28	40.97	11MB	11.47	38.06	1MB	6.54	35.6	1MB	4.18	34.42	1MB
4	14.87	41.76	3MB	9.77	39.21	1MB	5.73	37.19	1MB	3.87	36.26	1MB
8	12.6	42.63	1MB	8.18	40.42	1MB	4.97	38.81	1MB	3.56	38.11	1MB
12	10.45	43.55	1MB	6.79	41.72	1MB	4.34	40.49	1MB	3.3	39.97	1MB
16	8.45	44.55	1MB	5.57	43.11	1MB	3.8	42.22	1MB	3.06	41.86	1MB
20	6.56	45.61	1MB	4.48	44.56	1MB	3.31	43.98	1MB	2.83	43.74	1MB
24	4.92	46.79	1MB	3.53	46.09	1MB	2.78	45.71	1MB	2.42	45.53	1MB
28	3.44	48.04	1MB	2.78	47.72	1MB	2.44	47.54	1MB	2.28	47.47	1MB
32	2.13	49.39	1MB	2.13	49.39	1MB	2.13	49.39	1MB	2.13	49.39	1MB
$r = 10$	$w = 4$			$w = 5$			$w = 6$			$w = 7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	3.17	33.91	1MB	2.77	33.71	1MB	2.6	33.62	1MB	2.53	33.59	1MB
4	3.06	35.85	1MB	2.72	35.69	1MB	2.58	35.62	1MB	2.52	35.59	1MB
8	2.94	37.8	1MB	2.68	37.66	1MB	2.56	37.61	1MB	2.51	37.58	1MB
12	2.83	39.74	1MB	2.63	39.64	1MB	2.54	39.6	1MB	2.5	39.58	1MB
16	2.73	41.69	1MB	2.59	41.62	1MB	2.52	41.59	1MB	2.49	41.57	1MB
20	2.61	43.63	1MB	2.51	43.58	1MB	2.47	43.56	1MB	2.45	43.55	1MB
24	2.28	45.47	1MB	2.22	45.44	1MB	2.2	45.42	1MB	2.19	45.42	1MB
28	2.2	47.43	1MB	2.16	47.41	1MB	2.15	47.4	1MB	2.14	47.39	1MB
32	2.13	49.39	1MB	2.13	49.39	1MB	2.13	49.39	1MB	2.13	49.39	1MB

$r = 11$	$w = 0$			$w = 1$			$w = 2$			$w = 3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	14.72	39.68	2MB	8.77	36.71	1MB	4.34	34.5	1MB	2.61	33.63	1MB
4	12.5	40.58	1MB	7.36	38.	1MB	3.8	36.23	1MB	2.45	35.55	1MB
8	10.43	41.54	1MB	6.06	39.36	1MB	3.3	37.98	1MB	2.29	37.47	1MB
12	8.49	42.57	1MB	4.94	40.8	1MB	2.89	39.77	1MB	2.15	39.4	1MB
16	6.7	43.68	1MB	3.98	42.32	1MB	2.54	41.59	1MB	2.02	41.34	1MB
20	5.06	44.86	1MB	3.15	43.9	1MB	2.22	43.44	1MB	1.89	43.27	1MB
24	3.64	46.15	1MB	2.42	45.54	1MB	1.86	45.25	1MB	1.63	45.14	1MB
28	2.44	47.54	1MB	1.91	47.28	1MB	1.66	47.16	1MB	1.56	47.11	1MB
32	1.49	49.07	1MB	1.49	49.07	1MB	1.49	49.07	1MB	1.49	49.07	1MB
$r = 11$	$w = 4$			$w = 5$			$w = 6$			$w = 7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	2.02	33.33	1MB	1.82	33.24	1MB	1.75	33.2	1MB	1.73	33.19	1MB
4	1.97	35.31	1MB	1.81	35.23	1MB	1.75	35.2	1MB	1.72	35.19	1MB
8	1.92	37.29	1MB	1.79	37.22	1MB	1.74	37.2	1MB	1.72	37.19	1MB
12	1.87	39.26	1MB	1.77	39.21	1MB	1.73	39.19	1MB	1.72	39.19	1MB
16	1.83	41.24	1MB	1.75	41.2	1MB	1.73	41.19	1MB	1.72	41.18	1MB
20	1.76	43.21	1MB	1.71	43.18	1MB	1.7	43.17	1MB	1.69	43.17	1MB
24	1.55	45.1	1MB	1.52	45.09	1MB	1.52	45.08	1MB	1.51	45.08	1MB
28	1.52	47.09	1MB	1.5	47.08	1MB	1.49	47.07	1MB	1.49	47.07	1MB
32	1.49	49.07	1MB	1.49	49.07	1MB	1.49	49.07	1MB	1.49	49.07	1MB

$r = 12$	$w = 0$			$w = 1$			$w = 2$			$w = 3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	12.45	38.55	1MB	6.53	35.59	1MB	2.78	33.71	1MB	1.66	33.16	1MB
4	10.43	39.54	1MB	5.39	37.02	1MB	2.45	35.55	1MB	1.59	35.12	1MB
8	8.55	40.6	1MB	4.37	38.51	1MB	2.15	37.4	1MB	1.52	37.09	1MB
12	6.81	41.73	1MB	3.51	40.08	1MB	1.91	39.28	1MB	1.46	39.06	1MB
16	5.24	42.95	1MB	2.8	41.72	1MB	1.71	41.18	1MB	1.41	41.03	1MB
20	3.85	44.25	1MB	2.2	43.43	1MB	1.54	43.09	1MB	1.35	43.	1MB
24	2.66	45.66	1MB	1.69	45.17	1MB	1.32	44.98	1MB	1.2	44.93	1MB
28	1.75	47.2	1MB	1.37	47.01	1MB	1.23	46.94	1MB	1.18	46.92	1MB
32	1.15	48.9	1MB	1.15	48.9	1MB	1.15	48.9	1MB	1.15	48.9	1MB
$r = 12$	$w = 4$			$w = 5$			$w = 6$			$w = 7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	1.38	33.02	1MB	1.3	32.98	1MB	1.28	32.97	1MB	1.28	32.96	1MB
4	1.36	35.01	1MB	1.3	34.98	1MB	1.28	34.97	1MB	1.28	34.96	1MB
8	1.35	37.	1MB	1.3	36.97	1MB	1.28	36.97	1MB	1.28	36.96	1MB
12	1.33	38.99	1MB	1.29	38.97	1MB	1.28	38.96	1MB	1.27	38.96	1MB
16	1.31	40.98	1MB	1.29	40.97	1MB	1.28	40.96	1MB	1.27	40.96	1MB
20	1.29	42.97	1MB	1.27	42.96	1MB	1.26	42.96	1MB	1.26	42.95	1MB
24	1.17	44.91	1MB	1.16	44.91	1MB	1.16	44.91	1MB	1.16	44.91	1MB
28	1.16	46.91	1MB	1.16	46.9	1MB	1.15	46.9	1MB	1.15	46.9	1MB
32	1.15	48.9	1MB	1.15	48.9	1MB	1.15	48.9	1MB	1.15	48.9	1MB

$r = 13$	$w = 0$			$w = 1$			$w = 2$			$w = 3$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	10.45	37.55	1MB	4.73	34.69	1MB	1.78	33.22	1MB	1.2	32.93	1MB
4	8.62	38.64	1MB	3.86	36.26	1MB	1.62	35.13	1MB	1.18	34.91	1MB
8	6.93	39.79	1MB	3.09	37.87	1MB	1.47	37.06	1MB	1.15	36.9	1MB
12	5.41	41.03	1MB	2.47	39.56	1MB	1.35	39.	1MB	1.13	38.89	1MB
16	4.06	42.35	1MB	1.98	41.31	1MB	1.26	40.95	1MB	1.12	40.88	1MB
20	2.91	43.78	1MB	1.59	43.12	1MB	1.18	42.92	1MB	1.1	42.87	1MB
24	1.96	45.31	1MB	1.27	44.96	1MB	1.08	44.87	1MB	1.04	44.85	1MB
28	1.33	46.99	1MB	1.11	46.88	1MB	1.05	46.85	1MB	1.03	46.84	1MB
32	1.03	48.84	1MB	1.03	48.84	1MB	1.03	48.84	1MB	1.03	48.84	1MB
$r = 13$	$w = 4$			$w = 5$			$w = 6$			$w = 7$		
k	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M	p	C_{tr}	M
0	1.1	32.88	1MB	1.08	32.87	1MB	1.08	32.86	1MB	1.08	32.86	1MB
4	1.1	34.87	1MB	1.08	34.87	1MB	1.08	34.86	1MB	1.08	34.86	1MB
8	1.09	36.87	1MB	1.08	36.87	1MB	1.08	36.86	1MB	1.08	36.86	1MB
12	1.09	38.87	1MB	1.08	38.87	1MB	1.08	38.86	1MB	1.08	38.86	1MB
16	1.09	40.87	1MB	1.08	40.86	1MB	1.08	40.86	1MB	1.08	40.86	1MB
20	1.08	42.86	1MB	1.07	42.86	1MB	1.07	42.86	1MB	1.07	42.86	1MB
24	1.03	44.84	1MB	1.03	44.84	1MB	1.03	44.84	1MB	1.03	44.84	1MB
28	1.03	46.84	1MB	1.03	46.84	1MB	1.03	46.84	1MB	1.03	46.84	1MB
32	1.03	48.84	1MB	1.03	48.84	1MB	1.03	48.84	1MB	1.03	48.84	1MB

E Rogue CA Construction

Table E-1: *The to-be-signed part of our end-user X.509-certificate. Available from:* `http://www.win.tue.nl/hashclash/rogue-ca/downloads/real.cert.tbs.bin`.

Bytes (hex)	offset	description
30 82 03 9b	0–3	header
a0 03 02 01 02	4–8	version number
02 03 09 cf c7	9–13	serial number (‘*643015*’)
30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00	14–28	signature algorithm (‘*md5withRSAEncryption*’)
30 5a 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 1c 30 1a 06 03 55 04 0a 13 13 45 71 75 69 66 61 78 20 53 65 63 75 72 65 20 49 6e 63 2e 31 2d 30 2b 06 03 55 04 03 13 24 45 71 75 69 66 61 78 20 53 65 63 75 72 65 20 47 6c 6f 62 61 6c 20 65 42 75 73 69 6e 65 73 73 20 43 41 2d 31	29 – 120	issuer Distinguished Name (countryName: ‘*US*’, organizationName: ‘*Equifax Secure Inc.*’, commonName: ‘*Equifax Secure Global eBusiness CA*’)
30 1e 17 0d 30 38 31 31 30 33 30 37 35 32 30 32 5a 17 0d 30 39 31 31 30 34 30 37 35 32 30 32 5a	121–152	validity (‘*3 November 2008 07:52:02 UTC*’ –’*3 November 2009 07:52:02 UTC*’)
30 82 01 1c 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 49 30 47 06 03 55 04 0a 13 40 69 2e 62 72 6f 6b 65 2e 74 68 65 2e 69 6e 74 65 72 6e 65 74 2e 61 6e 64 2e 61 6c 6c 2e 69 2e 67 6f 74 2e 77 61 73 2e 74 68 69 73 2e 74 2d 73 68 69 72 74 2e 70 68 72 65 65 64 6f 6d 2e 6f 72 67 31 13 30 11 06 03 55 04 0b 13 0a 47 54 31 31 30 32 39 30 30 31 31 31 30 2f 06 03 55 04 0b 13 28 53 65 65 20 77 77 77 2e 72 61 70 69	153–440	subject Distinguished Name (countryName: ‘*US*’, organizationName: ‘*i.broke.the.internet.and.all .i.got.was.this.t-shirt .phreedom.org*’, organizationalUnitName: ‘*GT11029001*’, organizationalUnitName: ‘*See www.rapidssl.com/resources/cps (c)08*’, organizationalUnitName: ‘*Domain Control Validated - RapidSSL(R)*’, commonName: ‘*i.broke.the.internet.and.all .i.got.was.this.t-shirt*

Table E-1: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	offset	description
64 73 73 6c 2e 63 6f 6d 2f 72 65 73 6f 75 72 63 65 73 2f 63 70 73 20 28 63 29 30 38 31 2f 30 2d 06 03 55 04 0b 13 26 44 6f 6d 61 69 6e 20 43 6f 6e 74 72 6f 6c 20 56 61 6c 69 64 61 74 65 64 20 2d 20 52 61 70 69 64 53 53 4c 28 52 29 31 49 30 47 06 03 55 04 03 13 40 69 2e 62 72 6f 6b 65 2e 74 68 65 2e 69 6e 74 65 72 6e 65 74 2e 61 6e 64 2e 61 6c 6c 2e 69 2e 67 6f 74 2e 77 61 73 2e 74 68 69 73 2e 74 2d 73 68 69 72 74 2e 70 68 72 65 65 64 6f 6d 2e 6f 72 67		*.phreedom.org*')
30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 b2 d3 25 81 aa 28 e8 78 b1 e5 0a d5 3c 0f 36 57 6e a9 5f 06 41 0e 6b b4 cb 07	441 – 734	subject Public Key Info ('*rsaEncryption*', 2048-bit RSA modulus, RSA public exponent '*65537*'):
17 00 00 00 5b fd 6b 1c 7b 9c e8 a9	500 – 511	96-bit birthdaystring
a3 c5 45 0b 36 bb 01 d1 53 aa c3 08 8f 6f f8 4f 3e 87 87 44 11 dc 60 e0 df 92 55 f9 b8 73 1b 54 93 c5 9f d0 46 c4 60 b6 35 62 cd b9 af 1c a8 6b 1a c9 5b 3c 96 37 c0 ed 67 ef bb fe c0 8b 9c 50	512 – 575	1st near-collision block
2f 29 bd 83 22 9e 8e 08 fa ac 13 70 a2 58 7f 62 62 8a 11 f7 89 f6 df b6 67 59 73 16 fb 63 16 8a	576–639	2nd near-collision block

Table E-1: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	offset	description
b4 91 38 ce 2e f5 b6 be 4c a4 94 49 e4 65 51 0a 42 15 c9 c1 30 e2 69 d5 45 7d a5 26 bb b9 61 ec		
62 64 f0 39 e1 e7 bc 68 d8 50 51 9e 1d 60 d3 d1 a3 a7 0a f8 03 20 a1 70 01 17 91 36 4f 02 70 31 86 83 dd f7 0f d8 07 1d 11 b3 13 04 a5 da f0 ae 50 b1 28 0e 63 69 2a 0c 82 6f 8f 47 33 df 6c a2	640 – 703	3rd near-collision block
06 92 f1 4f 45 be d9 30 36 a3 2b 8c d6 77 ae 35 63 7f 4e 4c 9a 93 48 36 d9 9f 02 03 01 00 01	704–734	subject Public Key Info (continued)
	735 – 926	extensions:
a3 81 bd 30 81 ba	735 – 740	extensions header
30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 04 f0	741 – 756	keyUsage (‘*digital signature*’, ‘*nonrepudiation*’, ‘*key encipherment*’, ‘*data encipherment*’)
30 1d 06 03 55 1d 0e 04 16 04 14 cd a6 83 fa a5 60 37 f7 96 37 17 29 de 41 78 f1 87 89 55 e7	757 – 787	subjectKeyIdentifier
30 3b 06 03 55 1d 1f 04 34 30 32 30 30 a0 2e a0 2c 86 2a 68 74 74 70 3a 2f 2f 63 72 6c 2e 67 65 6f 74 72 75 73 74 2e 63 6f 6d 2f 63 72 6c 73 2f 67 6c 6f 62 61 6c 63 61 31 2e 63 72 6c	788 – 848	cRLDistributionPoints (‘*http://crl.geotrust.com* */crls/globalca1.crl*’)
30 1f 06 03 55 1d 23 04 18 30 16 80 14 be a8 a0 74 72 50 6b 44 b7 c9 23 d8 fb a8 ff b3 57 6b 68 6c	849 – 881	authorityKeyIdentifier
30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06 01	882 – 912	extKeyUsage (‘*server authentication*’,

Table E-1: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	offset	description
05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02		'*client authentication*')
30 0c 06 03 55 1d 13 01 01 ff 04 02 30 00	912 – 926	basicConstraints (CA: '*false*', path length: '*none*')

Table E-2: *The to-be-signed part of our rogue CA X.509-certificate. Available from:* `http://www.win.tue.nl/hashclash/rogue-ca/downloads/rogue_ca.cert.tbs.bin`.

Bytes (hex)	offset	description
30 82 03 9b	0–3	header
a0 03 02 01 02	4–8	version number
02 01 41	9–11	serial number ('*65*')
30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00	12–26	signature algorithm ('*md5withRSAEncryption*')
30 5a 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 1c 30 1a 06 03 55 04 0a 13 13 45 71 75 69 66 61 78 20 53 65 63 75 72 65 20 49 6e 63 2e 31 2d 30 2b 06 03 55 04 03 13 24 45 71 75 69 66 61 78 20 53 65 63 75 72 65 20 47 6c 6f 62 61 6c 20 65 42 75 73 69 6e 65 73 73 20 43 41 2d 31	27 – 118	issuer Distinguished Name (countryName: '*US*', organizationName: '*Equifax Secure Inc.*', commonName: '*Equifax Secure Global eBusiness CA*')
30 1e 17 0d 30 34 30 37 33 31 30 30 30 30 30 30 5a 17 0d 30 34 30 39 30 32 30 30 30 30 30 30 5a	119–150	validity ('*31 July 2004 00:00:00 UTC*' –'*2 September 2004 00:00:00 UTC*')
30 3c 31 3a 30 38 06 03 55 04 03 13 31 4d 44 35 20 43 6f 6c 6c 69 73 69 6f 6e 73 20 49 6e 63 2e 20 28 68 74 74 70 3a 2f 2f 77 77 77 2e 70 68 72 65 65 64 6f 6d 2e 6f 72 67 2f 6d 64 35 29	153 – 212	subject Distinguished Name (commonName: '*MD5 Collisions Inc.* *(http://www.phreedom.org/md5)*')
30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d 00 30 81	213 – 374	subject Public Key Info ('*rsaEncryption*', 1024-bit RSA modulus,

Table E-2: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	**offset**	**description**
89 02 81 81 00 ba a6 59 c9 2c 28 d6 2a b0 f8 ed 9f 46 a4 a4 37 ee 0e 19 68 59 d1 b3 03 99 51 d6 16 9a 5e 37 6b 15 e0 0e 4b f5 84 64 f8 a3 db 41 6f 35 d5 9b 15 1f db c4 38 52 70 81 97 5e 8f a0 b5 f7 7e 39 f0 32 ac 1e ad 44 d2 b3 fa 48 c3 ce 91 9b ec f4 9c 7c e1 5a f5 c8 37 6b 9a 83 de e7 ca 20 97 31 42 73 15 91 68 f4 88 af f9 28 28 c5 e9 0f 73 b0 17 4b 13 4c 99 75 d0 44 e6 7e 08 6c 1a f2 4f 1b 41 02 03 01 00 01		RSA public exponent '*65537*')
	375 – 926	extensions:
a3 82 02 24 30 82 02 20	375 – 378	extensions header
30 0b 06 03 55 1d 0f 04 04 03 02 01 c6	383 – 395	keyUsage ('*digital signature*', '*nonrepudiation*', '*certificate signing*', '*CRL signing*' '*offline CRL signing*')
30 0f 06 03 55 1d 13 01 01 ff 04 05 30 03 01 01 ff	396 – 412	basicConstraints (CA: '*true*', path length: '*none*')
30 1d 06 03 55 1d 0e 04 16 04 14 a7 04 60 1f ab 72 43 08 c5 7f 08 90 55 56 1c d6 ce e6 38 eb	413 – 443	subjectKeyIdentifier
30 1f 06 03 55 1d 23 04 18 30 16 80 14 be a8 a0 74 72 50 6b 44 b7 c9 23 d8 fb a8 ff b3 57 6b 68 6c	444 – 476	authorityKeyIdentifier
	477 – 926	netscape comment:
30 82 01 be 06 09 60 86 48 01 86 f8 42 01 0d 04 82 01 af	477 – 495	comment header
16 82 01 ab	496–499	random padding

Table E-2: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	offset	description
33 00 00 00 27 5e 39 e0 89 61 0f 4e	500–511	96-bit birthday string
a3 c5 45 0b 36 bb 01 d1 53 aa c3 08 8f 6f f8 4f 3e 87 87 44 11 dc 60 e0 df 92 55 f9 b8 73 1b 54 93 c5 9f d0 46 c4 60 b6 35 62 cd b9 af 1c a8 69 1a c9 5b 3c 96 37 c0 ed 67 ef bb fe c0 8b 9c 50	512–575	1st near-collision block
2f 29 bd 83 22 9e 8e 08 fa ac 13 70 a2 58 7f 62 62 8a 11 f7 89 f6 df b6 67 59 73 16 fb 63 16 8a b4 91 38 ce 2e f5 b6 be 4c a4 94 49 e4 65 11 0a 42 15 c9 c1 30 e2 69 d5 45 7d a5 26 bb b9 61 ec	576–639	2nd near-collision block
62 64 f0 39 e1 e7 bc 68 d8 50 51 9e 1d 60 d3 d1 a3 a7 0a f8 03 20 a1 70 01 17 91 36 4f 02 70 31 86 83 dd f7 0f d8 07 1d 11 b3 13 04 a5 dc f0 ae 50 b1 28 0e 63 69 2a 0c 82 6f 8f 47 33 df 6c a2	640–703	3rd near-collision block
06 92 f1 4f 45 be d9 30 36 a3 2b 8c d6 77 ae 35 63 7f 4e 4c 9a 93 48 36 d9 9f 02 03 01 00 01 a3 81 bd 30 81 ba 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 04 f0 30 1d 06 03 55 1d 0e 04 16 04 14 cd a6 83 fa a5 60 37 f7 96 37 17 29 de 41 78 f1 87 89 55 e7 30 3b 06 03 55 1d 1f 04 34 30 32 30 30 a0 2e a0 2c 86 2a 68 74 74 70 3a 2f 2f 63 72 6c 2e 67 65 6f 74 72 75	704–926	identical suffix: copied from end-user certificate

Table E-2: *The to-be-signed part of our rogue CA X.509-certificate. (cont.)*

Bytes (hex)	offset	description
73 74 2e 63 6f 6d 2f 63		
72 6c 73 2f 67 6c 6f 62		
61 6c 63 61 31 2e 63 72		
6c 30 1f 06 03 55 1d 23		
04 18 30 16 80 14 be a8		
a0 74 72 50 6b 44 b7 c9		
23 d8 fb a8 ff b3 57 6b		
68 6c 30 1d 06 03 55 1d		
25 04 16 30 14 06 08 2b		
06 01 05 05 07 03 01 06		
08 2b 06 01 05 05 07 03		
02 30 0c 06 03 55 1d 13		
01 01 ff 04 02 30 00		

Table E-3: *Rogue CA - first differential path*

t	Bitconditions: $\mathfrak{q}_t[31]\ldots\mathfrak{q}_t[0]$
-3	....
-2	.....1. .0.0-... .1.10.0. .+---.+-
-1	..1.1.0. .1-++..0 .010101. .+--1---
0	..1.0.-. .+1++^.0 .-1++1-. ^..0+1+-
1	..+.-.-. .+++.+.- .0-11-0. -101+0+0
2	0.+.-... .-0-11.+ .1+00-1. 0..-.-.-
3	0.1.+.0. .-01.0.- ..1.+0.. +..10+0-
4	-.-.+1.. .+.1.+.0 ..+.0+.. -..01-.+
5	+.1..0.. .+..^0.0 ..-.10.. 0...+1.1
6	+.1.1+.. ....+1.- ..-.00.. 0...+-.-
7	+.+..-.. .11.1+.+ ..-.+0.. 1....1.+
8	-.0.0-.. ..1.10.- ....0-.. 1...01.0
9	-.+.1-.. ..-..1.- .^0.1+.. -...0..1
10	0.00+.10 01-00..- ^+.0.-.1 -.101101
11	1.-1-010 11-011.+ +1.10-01 -101+010
12	-^+++1+- ++1+-1^+ 01^-0+1- 00+-+-++
13	1-+0--+- +-+----- --+-+++- ++-+.1--
14	10-1000+ .10+.-10 0-1.-.-. 1-+0010-
15	.11.01++ 000+1000 0-00-010 111+..00
16	..0...11 ...-.+.. .+..0.^. .++..0.+
17	..10+.00 ...1.0.. .0..^.0. .0.^.1..
18	..+.+.1. ...-.-.. .-....0. .-^..-.^
19	..1++.-. ...-.... 0-....+. .....
20	..0++... 0..0.^.. 0+..0... 0^...^..
21	...++.^. 1..^.... +1..1.^. 1....0..
22	...-1... -..... .^..-... +....1..
23	...00... ...0.... ^..... .....-.0
24	...1.... ^..1...0 ....^... ^.0....1
25	....+...1 ....^.+
26	......0. .....+ ..... .0-.....
27	......1. ...^.... ..... .1-....^
28	......-. .....^ ..... .-+.....
29	......0. ....0.....
30	......+. ....^1.....
31	......+. ....
32	......1. ....
33	......0. ....
34–59	....
60	....00...
61	....1...
62	....-+...
63	....?-...
64	......+. ....-...

$$\delta m_{11} = -2^{25}$$

Table E-4: *Rogue CA - second differential path*

t	Bitconditions: $\mathfrak{q}_t[31]\ldots\mathfrak{q}_t[0]$
-3	....
-2	....1.0- +++++... .0.00... ......+-
-1	.0..1^10 0.11-1.. .1.01.^1 .....^0+
0	.1..+--- -1-0-0.. .-.++.-1 .....+--
1	.+..+000 0.++++.. .-.++.1- 111
2	.0..+01+ 11+01-0. ..1.-.++ .....-00
3	.-..-..- .1+0-10. .0011.0+ ..^..-..
4	.+^.-..- .++.+0+. ..+.0.+. ..-.11..
5	.++...0- .+..1.+. ..+...00 ..0.1+..
6	.-1.0.0+ ..0.1.+. ..-...11 ..1.+1..
7	.11...++ .1....+. ..1.^.-- ....-+..
8	.-1...-. ....-.-.00 ....0-..
9	.1-.1.11 ....1.0. ..-00.11 ....++..
10	1+-.01-. .11010.. 10-1+.0. ..0.0-0.
11	0-0.+00. 1001-10^ 110--0+. .01.111^
12	--0^0++^ 0-++-+1+ +-+1-0+0 ^0-^+1+-
13	0++-++++ +1++-1-0 +0-1--+1 ------+1
14	10101.-0 0-1.+0-0 +011.+.- 1+.1-+01
15	.10101+1 0++10.+. 1.0-010- 1100+1-.
16	....0.11 .+..1.-. -...0^.1 .^..--..
17	....1.-. .1^.-.0. 0..^...^ .0..1.^.
18	0...+.-+ .1....-. +...-... .0..-^..
19	......++ .-..^... ...0-... .+......
20	+...^.+0 ...0..^. ^..0+..0 ...0^...
21	+.....0+ .^.1.... ...+1..1 .^.1....
22	-.....-. ...-.... ....^..- ...+....
23	-.0....^ ......0. ...^.... ....
24	1.1...^. ...^..1. ..0....^ ...^.0..
25	0.+..... ......+. ..1..... ....
26	.... .0...... ..+..... ....0-..
27	..^..... .1....^. ....1-..
28	....-...... ..^..... ....-+..
29	.... .0...... ....0..
30	....+...... ....^1..
31	....+...... ....
32	.... .0...... ....
33	.... .1...... ....
34–59	....
60	000
61	100
62	....-++
63	....-++
64	.... -+-..... ....-

$$\delta m_{11} = -2^{22}$$

Table E-5: *Rogue CA - third differential path*

t	Bitconditions: $\mathfrak{q}_t[31]\ldots\mathfrak{q}_t[0]$
-3	....
-2	....1-+... ..01.00. .....
-1	.....0.. ..-++1.0 .010011. .....
0	.....1.. ..-++1.1 .1--0++. .1.....0
1	...^.+.. ..-+.+.- .-0++0-. .1.....1
2	...-.1.. ...+0+.- .-1++1-. .+^....-
3	...0.1.. ..1+...+ ..-...-^ .+-...^-
4	...0.^.0 ^.1+.0.+ .1-10..+ .-0..^+.
5	.^...+.0 -.0....- ......10 .+0..-10
6	.+...0.- 0.-0...+ ..1....- .+..10-.
7	.0...-1+ 1.+....- .....^.1 .-..110.
8	.1...-1+ +.+....0 ..0..+.1 .1..-.0.
9	......-- +.+^...0 ..0..0.+ .0..-.0.
10	10..11-- +.0+0000 .1-0.+.+ .-.1-.01
11	11..11-0 -.101111 01-1^110 ^+.1-1-0
12	-+.^-0+- +.-+++++ 1--+-101 +-1-10+-
13	+0.+---- 1.11-001 ---00.+- 0-0+-+++
14	11.1+-0+ 0.+-011+ 1.-1-.1+ 0.-010.0
15	00.0+.10 ..1+0.-0 11-01.1- .01-1100
16	....0^.+ .0+1.0.- .01.0..1 ..^+.0..
17	.+..^.0. .0.0.1^. .1^++.00 ...1.1..
18	.+....0^ .-^..+.^ .-.++.1. ...+.-..
19	0-....-. ....--.+. ...+....
20	1-..0... 0^...^.. .^.0-... 0..0.^..
21	+0..1.^. 1....0.. ...1-.^. 1..^....
22	.^..+... -....1.. ...+1... +.......
23	^....... .....+.0 ....0... ...0....
24	....^... ^.0....1 ...^.... ^..1...0
25	....^.- ....-...1
26	..... .0+..... ......0. ....-
27	..... .1+....^ ......1. ...^....
28	..... .+-..... ......+. ....^
29	....0..... ......0. .....
30	..... .^1..... ......-. .....
31	....-. .....
32	....1. .....
33	....0. .....
34–59	....
60	....0... ....
61	.......1 01011... ....
62	.......0 .1.1+... ....
63	.......+ -----... ....
64	....+-..+ --.-.--. .....

$$\delta m_{11} = 2^9$$

F SHA-1 disturbance vector analysis

The tables shown in this appendix are based on the disturbance vector cost function $\mathrm{FDC}_{u,t_b,\epsilon}$ which is a modification of the cost function FDC_{u,t_b} presented in Section 7.5.11. The cost function FDC_{u,t_b} uses Algorithms 7-2 and 7-3 (p. 150 and 151) to determine sets $\mathcal{A}_{i,j}$. The cost function $\mathrm{FDC}_{u,t_b,\epsilon}$ uses a simple modification of these algorithms that works instead of sets $\mathcal{A}_{i,j}$ with sets $\mathcal{A}'_{i,j}$ of the form:

$$\mathcal{A}'_{i,j} \subseteq \{(\mathcal{P}, g(\mathcal{S}_\mathcal{P})) \mid (\mathcal{P}, \mathcal{S}_\mathcal{P}) \in \mathcal{A}_{i,j}\}, \quad \text{where } g(\mathcal{S}_\mathcal{P}) \subseteq \mathcal{S}_\mathcal{P} \text{ for all } \mathcal{P}. \tag{F.1}$$

We add in both algorithms a step 3.5 between step 3 and step 4 that, for each value of t in step 3, removes all message difference vectors in the previous $\mathcal{A}'_{i,j}$ (thus either $(i,j) = (t_b, t-1)$ or $(i,j) = (t+1, t_e)$) with a too low total success probability. Let $\mathcal{W} = \{w \mid (w,p) \in \mathcal{S}, (\mathcal{P}, \mathcal{S}) \in \mathcal{A}'_{i,j}\}$ and for $w \in \mathcal{W}$ let

$$p_w = \sum_{(\mathcal{P},\mathcal{S}) \in \mathcal{A}'_{i,j}} \sum_{\substack{(w,p) \in \mathcal{S} \\ w'=w}} p$$

be the total success probability of w. Let $p_{\max} = \max_{w \in \mathcal{W}} p_w$ be the maximum of these total success probabilities. Then after $p_{\max}$ has been determined we remove from $\mathcal{A}'_{i,j}$ all occurrences of message difference vectors w for which $p_w < \epsilon \cdot p_{\max}$, where $\epsilon \in [0,1]$ is some chosen fraction. Next we remove all pairs of the form $(\mathcal{P}, \emptyset)$ from $\mathcal{A}'_{i,j}$. More precisely, let $\widetilde{\mathcal{A}}'_{i,j}$ denote the contents of the set $\mathcal{A}'_{i,j}$ in these algorithms before step 3.5, then the contents of $\mathcal{A}'_{i,j}$ after step 3.5 is determined as:

$$\mathcal{A}'_{i,j} = \left\{ \left(\mathcal{P}, \mathrm{Trim}\left(\widetilde{\mathcal{S}}'_\mathcal{P}\right)\right) \;\middle|\; \left(\mathcal{P}, \widetilde{\mathcal{S}}'_\mathcal{P}\right) \in \widetilde{\mathcal{A}}'_{i,j} \wedge \mathrm{Trim}\left(\widetilde{\mathcal{S}}'_\mathcal{P}\right) \neq \emptyset \right\},$$
$$\mathrm{Trim}\left(\widetilde{\mathcal{S}}'_\mathcal{P}\right) = \left\{ (w,p) \in \widetilde{\mathcal{S}}'_\mathcal{P} \;\middle|\; p_w \geq \epsilon \cdot p_{\max} \right\}.$$

Informally, $\mathcal{A}'_{i,j}$ contains a subset of the information present in $\mathcal{A}_{i,j}$ (Equation F.1), thus it follows that $\mathrm{FDC}_{u,t_b,\epsilon}((DV_t)_{t=0}^{79}) \leq \mathrm{FDC}_{u,t_b}((DV_t)_{t=0}^{79})$ for all disturbance vectors $(DV_t)_{t=0}^{79}$. For $\epsilon = 0$, it is clear that nothing will we removed in the added procedure and thus $\mathrm{FDC}_{u,t_b,\epsilon}$ is equivalent to FDC_{u,t_b}. Moreover, the outcome of $\mathrm{FDC}_{u,t_b,\epsilon}$ will also be the same as that of FDC_{u,t_b} if ϵ is small enough so that no optimal message difference vectors are removed in this manner. For $\epsilon \leq 0.5$ we have not noticed a difference in outcomes so far, but we have noticed differences for values of ϵ that were even slightly bigger than 0.5.

The numbers presented in the following tables are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$ for $u \in \{0,\ldots,7\}$. For each disturbance vector and each value of u, we try the values $0, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}$ for ϵ in that order and keep the first result (and thus lowest value for ϵ) for which the computation succeeds within 24 hours using the 8GB of RAM available. An empty result in the following tables reflects the fact that the computations failed for all these values for ϵ either due a too long runtime or a memory allocation failure.

Table F-1: *Most interesting disturbance vectors*

	u							
DV	0	1	2	3	4	5	6	7
I(48, 0)	75.00 ϵ=0	71.84 ϵ=0	71.61 ϵ=0	71.51 ϵ=0	71.46 ϵ=0	71.44 ϵ=0	71.43 ϵ=0	71.42 ϵ=0
I(49, 0)	76.00 ϵ=0	72.59 ϵ=0	72.34 ϵ=0	72.24 ϵ=0	72.19 ϵ=0	72.17 ϵ=0	72.16 ϵ=0	72.15 ϵ=0
I(50, 0)	75.00 ϵ=0	72.02 ϵ=0	71.95 ϵ=0	71.93 ϵ=0	71.92 ϵ=0	71.92 ϵ=0	71.92 ϵ=0	71.92 ϵ=0
II(46, 0)	76.00 ϵ=0	71.85 ϵ=0	71.83 ϵ=1/2					
II(50, 0)	78.00 ϵ=0	73.52 ϵ=0	73.23 ϵ=0	73.12 ϵ=0	73.06 ϵ=0	73.04 ϵ=0	73.03 ϵ=0	73.02 ϵ=0
II(51, 0)	77.00 ϵ=0	72.55 ϵ=0	72.18 ϵ=0	72.02 ϵ=0	71.95 ϵ=0	71.91 ϵ=0	71.89 ϵ=0	71.88 ϵ=0
II(52, 0)	75.00 ϵ=0	71.88 ϵ=0	71.87 ϵ=0	71.76 ϵ=0	71.76 ϵ=0	71.75 ϵ=0	71.75 ϵ=0	71.75 ϵ=0

The columns are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$.

Table F-2: *Overview of disturbance vectors* $I(K, 0)$

	u							
DV	0	1	2	3	4	5	6	7
I(42, 0)	82.68 ϵ=0	78.67 ϵ=0	78.36 ϵ=1/4					
I(43, 0)	82.00 ϵ=0	77.65 ϵ=0	77.31 ϵ=1/8					
I(44, 0)	81.00 ϵ=0	77.41 ϵ=0	77.1 ϵ=0	76.98 ϵ=0	76.93 ϵ=1/8	76.90 ϵ=1/8	76.89 ϵ=1/8	76.89 ϵ=1/8
I(45, 0)	81.00 ϵ=0	76.91 ϵ=0	76.66 ϵ=0	76.54 ϵ=0	76.49 ϵ=0	76.47 ϵ=1/8	76.46 ϵ=1/8	76.45 ϵ=1/8
I(46, 0)	79.00 ϵ=0	75.02 ϵ=0	74.92 ϵ=0	74.84 ϵ=0	74.83 ϵ=0	74.83 ϵ=0	74.83 ϵ=0	74.83 ϵ=1/8
I(47, 0)	79.00 ϵ=0	75.15 ϵ=0	74.83 ϵ=0	74.71 ϵ=0	74.65 ϵ=0	74.63 ϵ=0	74.62 ϵ=0	74.61 ϵ=0
I(48, 0)	75.00 ϵ=0	71.84 ϵ=0	71.61 ϵ=0	71.51 ϵ=0	71.46 ϵ=0	71.44 ϵ=0	71.43 ϵ=0	71.42 ϵ=0
I(49, 0)	76.00 ϵ=0	72.59 ϵ=0	72.34 ϵ=0	72.24 ϵ=0	72.19 ϵ=0	72.17 ϵ=0	72.16 ϵ=0	72.15 ϵ=0
I(50, 0)	75.00 ϵ=0	72.02 ϵ=0	71.95 ϵ=0	71.93 ϵ=0	71.92 ϵ=0	71.92 ϵ=0	71.92 ϵ=0	71.92 ϵ=0
I(51, 0)	77.00 ϵ=0	73.76 ϵ=0	73.53 ϵ=0	73.43 ϵ=0	73.38 ϵ=0	73.36 ϵ=0	73.35 ϵ=0	73.34 ϵ=0
I(52, 0)	79.00 ϵ=0	76.26 ϵ=0	76.24 ϵ=0	76.24 ϵ=0	76.24 ϵ=0	76.24 ϵ=0	76.24 ϵ=0	76.24 ϵ=0
I(53, 0)	82.83 ϵ=0	78.86 ϵ=0	78.79 ϵ=0	78.77 ϵ=0	78.77 ϵ=0	78.77 ϵ=0	78.77 ϵ=0	78.77 ϵ=0
I(54, 0)	82.83 ϵ=0	79.60 ϵ=0	79.38 ϵ=0	79.28 ϵ=0	79.23 ϵ=0	79.21 ϵ=0	79.19 ϵ=0	79.19 ϵ=0
I(55, 0)	81.54 ϵ=0	78.67 ϵ=0	78.42 ϵ=0	78.32 ϵ=0	78.27 ϵ=0	78.25 ϵ=0	78.24 ϵ=0	78.23 ϵ=0
I(56, 0)	81.54 ϵ=0	79.10 ϵ=0	79.03 ϵ=0	79.01 ϵ=0	79.01 ϵ=0	79.01 ϵ=0	79.01 ϵ=0	79.01 ϵ=0

The columns are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$.

Table F-3: *Overview of disturbance vectors* $I(K, 2)$

	u							
DV	0	1	2	3	4	5	6	7
I(42, 2)	85.09 ϵ=0	82.17 ϵ=1/4	81.84 ϵ=1/2	81.72 ϵ=1/2				
I(43, 2)	84.42 ϵ=0	81.15 ϵ=1/4	80.78 ϵ=1/2					
I(44, 2)	84.42 ϵ=0	81.92 ϵ=0	81.57 ϵ=1/4	81.45 ϵ=1/2	81.40 ϵ=1/2	81.38 ϵ=1/2	81.37 ϵ=1/2	81.36 ϵ=1/2
I(45, 2)	83.42 ϵ=0	80.80 ϵ=0	80.52 ϵ=0	80.41 ϵ=1/4	80.36 ϵ=1/2	80.34 ϵ=1/2	80.33 ϵ=1/2	80.32 ϵ=1/2
I(46, 2)	80.42 ϵ=0	78.10 ϵ=0	78.00 ϵ=0	77.99 ϵ=1/8	77.99 ϵ=1/8	77.99 ϵ=1/8	77.99 ϵ=1/8	77.99 ϵ=1/4
I(47, 2)	79.68 ϵ=0	77.01 ϵ=0	76.68 ϵ=0	76.56 ϵ=0	76.51 ϵ=1/8	76.48 ϵ=1/8	76.47 ϵ=1/8	76.47 ϵ=1/8
I(48, 2)	76.68 ϵ=0	74.27 ϵ=0	73.99 ϵ=0	73.88 ϵ=0	73.83 ϵ=0	73.81 ϵ=0	73.80 ϵ=0	73.79 ϵ=0
I(49, 2)	77.00 ϵ=0	74.30 ϵ=0	74.02 ϵ=0	73.92 ϵ=0	73.87 ϵ=0	73.85 ϵ=0	73.84 ϵ=0	73.83 ϵ=0
I(50, 2)	77.00 ϵ=0	74.74 ϵ=0	74.63 ϵ=0	74.61 ϵ=0	74.61 ϵ=0	74.60 ϵ=0	74.60 ϵ=0	74.60 ϵ=0
I(51, 2)	80.00 ϵ=0	77.47 ϵ=0	77.21 ϵ=0	77.11 ϵ=0	77.07 ϵ=0	77.04 ϵ=0	77.03 ϵ=0	77.03 ϵ=0
I(52, 2)	82.00 ϵ=0	79.98 ϵ=0	79.93 ϵ=0	79.92 ϵ=0	79.92 ϵ=0	79.92 ϵ=0	79.92 ϵ=0	79.92 ϵ=0
I(53, 2)	84.00 ϵ=0	81.91 ϵ=0	81.80 ϵ=0	81.78 ϵ=0	81.78 ϵ=0	81.78 ϵ=0	81.78 ϵ=0	81.78 ϵ=0
I(54, 2)	84.00 ϵ=0	81.37 ϵ=0	81.06 ϵ=0	80.95 ϵ=0	80.90 ϵ=0	80.87 ϵ=0	80.86 ϵ=0	80.85 ϵ=0
I(55, 2)	84.00 ϵ=0	81.78 ϵ=0	81.53 ϵ=0	81.43 ϵ=0	81.38 ϵ=0	81.36 ϵ=0	81.34 ϵ=0	81.34 ϵ=0
I(56, 2)	82.00 ϵ=0	80.22 ϵ=0	80.13 ϵ=0	80.12 ϵ=0	80.11 ϵ=0	80.11 ϵ=0	80.11 ϵ=0	80.11 ϵ=0

The columns are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$.

Table F-4: *Overview of disturbance vectors* $II(K, 0)$

DV	u							
	0	1	2	3	4	5	6	7
$II(44,0)$	87.00 ϵ=0	79.51 ϵ=1/2						
$II(45,0)$	83.00 ϵ=0	75.45 ϵ=1/8	74.82 ϵ=1/2					
$II(46,0)$	76.00 ϵ=0	71.85 ϵ=0	71.83 ϵ=1/2					
$II(47,0)$	81.42 ϵ=0	76.23 ϵ=0	75.87 ϵ=1/2					
$II(48,0)$	80.00 ϵ=0	76.11 ϵ=0	75.89 ϵ=0	75.79 ϵ=1/8	75.74 ϵ=1/2			
$II(49,0)$	80.00 ϵ=0	75.04 ϵ=0	74.72 ϵ=0	74.60 ϵ=0	74.55 ϵ=1/8	74.52 ϵ=1/8	74.51 ϵ=1/2	74.51 ϵ=1/2
$II(50,0)$	78.00 ϵ=0	73.52 ϵ=0	73.23 ϵ=0	73.12 ϵ=0	73.06 ϵ=0	73.04 ϵ=0	73.03 ϵ=0	73.02 ϵ=0
$II(51,0)$	77.00 ϵ=0	72.55 ϵ=0	72.18 ϵ=0	72.02 ϵ=0	71.95 ϵ=0	71.91 ϵ=0	71.89 ϵ=0	71.88 ϵ=0
$II(52,0)$	75.00 ϵ=0	71.88 ϵ=0	71.87 ϵ=0	71.76 ϵ=0	71.76 ϵ=0	71.75 ϵ=0	71.75 ϵ=0	71.75 ϵ=0
$II(53,0)$	76.96 ϵ=0	73.65 ϵ=0	73.34 ϵ=1/8	73.23 ϵ=1/8	73.17 ϵ=1/8	73.15 ϵ=1/8	73.14 ϵ=1/8	73.14 ϵ=1/8
$II(54,0)$	77.96 ϵ=0	73.97 ϵ=0	73.74 ϵ=1/8	73.64 ϵ=1/8	73.59 ϵ=1/8	73.57 ϵ=1/8	73.56 ϵ=1/8	73.55 ϵ=1/8
$II(55,0)$	77.96 ϵ=0	75.22 ϵ=1/8	74.99 ϵ=1/2	74.89 ϵ=1/2	74.84 ϵ=1/2	74.82 ϵ=1/2	74.81 ϵ=1/2	74.80 ϵ=1/2
$II(56,0)$	76.96 ϵ=0	74.48 ϵ=1/2	74.18 ϵ=1/2	74.07 ϵ=1/2	74.01 ϵ=1/2	73.99 ϵ=1/2	73.98 ϵ=1/2	73.97 ϵ=1/2

The columns are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$.

Table F-5: *Overview of disturbance vectors* $II(K, 2)$

	u							
DV	0	1	2	3	4	5	6	7
$II(45, 2)$	85.00 ϵ=0	78.64 ϵ=1/2						
$II(46, 2)$	82.00 ϵ=0	77.51 ϵ=1/2						
$II(47, 2)$	85.42 ϵ=0	79.83 ϵ=1/2						
$II(48, 2)$	83.00 ϵ=0	78.81 ϵ=1/2	78.46 ϵ=1/2					
$II(49, 2)$	83.00 ϵ=0	78.09 ϵ=0	77.74 ϵ=1/2					
$II(50, 2)$	81.00 ϵ=0	76.51 ϵ=0	76.16 ϵ=1/8	76.03 ϵ=1/8				
$II(51, 2)$	82.00 ϵ=0	77.74 ϵ=0	77.36 ϵ=1/8	77.20 ϵ=1/8	77.13 ϵ=1/2			
$II(52, 2)$	82.00 ϵ=0	79.07 ϵ=0	78.96 ϵ=0	78.94 ϵ=0	78.94 ϵ=1/8	78.93 ϵ=1/8	78.93 ϵ=1/8	78.93 ϵ=1/2
$II(53, 2)$	83.00 ϵ=0	79.60 ϵ=0	79.30 ϵ=0	79.18 ϵ=0	79.13 ϵ=1/8	79.11 ϵ=1/8	79.09 ϵ=1/8	79.09 ϵ=1/8
$II(54, 2)$	84.00 ϵ=0	80.49 ϵ=0	80.21 ϵ=0	80.10 ϵ=0	80.04 ϵ=1/8	80.02 ϵ=1/8	80.01 ϵ=1/8	80.00 ϵ=1/8
$II(55, 2)$	84.00 ϵ=0	81.20 ϵ=0	80.88 ϵ=0	80.76 ϵ=0	80.71 ϵ=0	80.68 ϵ=0	80.67 ϵ=0	80.67 ϵ=1/8
$II(56, 2)$	85.00 ϵ=0	82.69 ϵ=1/4	82.39 ϵ=1/4	82.27 ϵ=1/4	82.22 ϵ=1/4	82.20 ϵ=1/4	82.19 ϵ=1/4	82.18 ϵ=1/4

The columns are the negative $\log_2$ results of the cost function $\mathrm{FDC}_{u,20,\epsilon}$.

References

[AHMP10] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan, *SHA-3 proposal BLAKE*, Submission to NIST (Round 3), 2010.

[ANPS07] Elena Andreeva, Gregory Neven, Bart Preneel, and Thomas Shrimpton, *Seven-Property-Preserving Iterated Hashing: ROX*, ASIACRYPT (Kaoru Kurosawa, ed.), Lecture Notes in Computer Science, vol. 4833, Springer, 2007, pp. 130–146.

[BC04] Eli Biham and Rafi Chen, *Near-Collisions of SHA-0*, CRYPTO (Matthew K. Franklin, ed.), Lecture Notes in Computer Science, vol. 3152, Springer, 2004, pp. 290–305.

[BCJ+05] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby, *Collisions of SHA-0 and Reduced SHA-1*, EUROCRYPT (Ronald Cramer, ed.), Lecture Notes in Computer Science, vol. 3494, Springer, 2005, pp. 36–57.

[BDPA11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, *The Keccak SHA-3 submission*, Submission to NIST (Round 3), 2011.

[Ber92] Thomas A. Berson, *Differential Cryptanalysis Mod* 2^{32} *with Applications to MD5*, EUROCRYPT, 1992, pp. 71–80.

[BP95] Antoon Bosselaers and Bart Preneel (eds.), *Integrity Primitives for Secure Information Systems, Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040*, Lecture Notes in Computer Science, vol. 1007, Springer, 1995.

[BR06a] Mihir Bellare and Thomas Ristenpart, *Multi-Property-Preserving Hash Domain Extension and the EMD Transform*, ASIACRYPT (Xuejia Lai and Kefei Chen, eds.), Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 299–314.

[BR06b] Steven M. Bellovin and Eric Rescorla, *Deploying a New Hash Algorithm*, NDSS, The Internet Society, 2006.

[BR07] Mihir Bellare and Thomas Ristenpart, *Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms*, ICALP (Lars Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki, eds.), Lecture Notes in Computer Science, vol. 4596, Springer, 2007, pp. 399–410.

[BS90] Eli Biham and Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, CRYPTO (Alfred Menezes and Scott A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer, 1990, pp. 2–21.

[BS91] Eli Biham and Adi Shamir, *Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer*, CRYPTO (Joan Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer, 1991, pp. 156–171.

[BS92] Eli Biham and Adi Shamir, *Differential Cryptanalysis of the Full 16-Round DES*, CRYPTO (Ernest F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer, 1992, pp. 487–496.

[Bun08] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)*, 2008, p. 376.

[Che11] Rafael Chen, *New Techniques for Cryptanalysis of Cryptographic Hash Functions*, Ph.D. thesis, Technion, Aug 2011.

[CJ98] Florent Chabaud and Antoine Joux, *Differential Collisions in SHA-0*, CRYPTO (Hugo Krawczyk, ed.), Lecture Notes in Computer Science, vol. 1462, Springer, 1998, pp. 56–71.

[CMR07] Christophe De Cannière, Florian Mendel, and Christian Rechberger, *Collisions for 70-Step SHA-1: On the Full Cost of Collision Search*, Selected Areas in Cryptography (Carlisle M. Adams, Ali Miri, and Michael J. Wiener, eds.), Lecture Notes in Computer Science, vol. 4876, Springer, 2007, pp. 56–73.

[Coc07] Martin Cochran, *Notes on the Wang et al.* 2^{63} *SHA-1 Differential Path*, Cryptology ePrint Archive, Report 2007/474, 2007.

[CR06] Christophe De Cannière and Christian Rechberger, *Finding SHA-1 Characteristics: General Results and Applications*, ASIACRYPT (Xuejia Lai and Kefei Chen, eds.), Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 1–20.

[CSF+08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Request for Comments, May 2008, RFC 5280.

[Dam89] Ivan Damgård, *A Design Principle for Hash Functions*, CRYPTO (Gilles Brassard, ed.), Lecture Notes in Computer Science, vol. 435, Springer, 1989, pp. 416–427.

[Dau05] Magnus Daum, *Cryptanalysis of Hash Functions of the MD4-Family*, Ph.D. thesis, Ruhr-Universität Bochum, May 2005.

[dBB91] Bert den Boer and Antoon Bosselaers, *An Attack on the Last Two Rounds of MD4*, CRYPTO (Joan Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer, 1991, pp. 194–203.

[dBB93] Bert den Boer and Antoon Bosselaers, *Collisions for the Compression Function of MD5*, EUROCRYPT, 1993, pp. 293–304.

[DBP96] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel, *RIPEMD-160: A Strengthened Version of RIPEMD*, FSE (Dieter Gollmann, ed.), Lecture Notes in Computer Science, vol. 1039, Springer, 1996, pp. 71–82.

[DH76] Whitfield Diffie and Martin E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 6, 644–654.

[DL05] Magnus Daum and Stefan Lucks, *Attacking Hash Functions by Poisoned Messages, "The Story of Alice and her Boss"*, June 2005, `http://th.informatik.uni-mannheim.de/people/lucks/HashCollisions/`.

[Dob96] Hans Dobbertin, *Cryptanalysis of MD5 Compress*, 1996, In Rump Session of EuroCrypt '96.

[Dob98] Hans Dobbertin, *Cryptanalysis of MD4*, J. Cryptology **11** (1998), no. 4, 253–271.

[DP80] D. W. Davies and W. L. Price, *The Application of Digital Signatures Based on Public-Key Cryptosystems*, Proc. Fifth Intl. Computer Communications Conference, October 1980, pp. 525–530.

[FLS+10] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker, *The Skein Hash Function Family*, Submission to NIST (Round 3), 2010.

[GIS05] M. Gebhardt, G. Illies, and W. Schindler, *A Note on Practical Value of Single Hash Collisions for Special File Formats*, NIST First Cryptographic Hash Workshop, October 2005.

[GKM+11] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen, *Grøstl – a SHA-3 candidate*, Submission to NIST (Round 3), 2011.

[Gre10] E. A. Grechnikov, *Collisions for 72-step and 73-step SHA-1: Improvements in the Method of Characteristics*, Cryptology ePrint Archive, Report 2010/413, 2010.

[HC] *HashClash project webpage*, `http://code.google.com/p/hashclash`.

[HK06] Shai Halevi and Hugo Krawczyk, *Strengthening Digital Signatures Via Randomized Hashing*, CRYPTO (Cynthia Dwork, ed.), Lecture Notes in Computer Science, vol. 4117, Springer, 2006, pp. 41–59.

[HPR04] Philip Hawkes, Michael Paddon, and Gregory G. Rose, *Musings on the Wang et al. MD5 Collision*, Cryptology ePrint Archive, Report 2004/264, 2004.

[HS05] Paul Hoffman and Bruce Schneier, *Attacks on Cryptographic Hashes in Internet Protocols*, Internet Request for Comments, November 2005, RFC 4270.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby, *Pseudo-random Generation from one-way functions (Extended Abstracts)*, STOC, ACM, 1989, pp. 12–24.

[Jou04] Antoine Joux, *Multicollisions in Iterated Hash Functions: Application to Cascaded Constructions*, CRYPTO (Matthew K. Franklin, ed.), Lecture Notes in Computer Science, vol. 3152, Springer, 2004, pp. 306–316.

[JP05] Charanjit S. Jutla and Anindya C. Patthak, *A Matching Lower Bound on the Minimum Weight of SHA-1 Expansion Code*, Cryptology ePrint Archive, Report 2005/266, 2005.

[Kam04] Dan Kaminsky, *MD5 To Be Considered Harmful Someday*, Cryptology ePrint Archive, Report 2004/357, 2004.

[KG07] Neil Koblitz and Oded Goldreich, 2007, See `http://www.sigcrap.org/2007/09/14/the-koblitz-controversy/`.

[KK06] John Kelsey and Tadayoshi Kohno, *Herding Hash Functions and the Nostradamus Attack*, EUROCRYPT (Serge Vaudenay, ed.), Lecture Notes in Computer Science, vol. 4004, Springer, 2006, pp. 183–200.

[Kli05] Vlastimil Klima, *Finding MD5 Collisions on a Notebook PC Using Multi-message Modifications*, Cryptology ePrint Archive, Report 2005/102, 2005.

[Kli06] Vlastimil Klima, *Tunnels in Hash Functions: MD5 Collisions Within a Minute*, Cryptology ePrint Archive, Report 2006/105, 2006.

[KS05] John Kelsey and Bruce Schneier, *Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work*, EUROCRYPT (Ronald Cramer, ed.), Lecture Notes in Computer Science, vol. 3494, Springer, 2005, pp. 474–490.

[LdW05] Arjen K. Lenstra and Benne de Weger, *On the Possibility of Constructing Meaningful Hash Collisions for Public Keys*, ACISP (Colin Boyd and Juan Manuel González Nieto, eds.), Lecture Notes in Computer Science, vol. 3574, Springer, 2005, pp. 267–279.

[Lin98] J. H. Van Lint, *Introduction to Coding Theory*, 3rd ed., Graduate Texts in Mathematics, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1998.

[LL05] Jie Liang and Xuejia Lai, *Improved Collision Attack on Hash Function MD5*, Cryptology ePrint Archive, Report 2005/425, 2005.

[Man08] Stephane Manuel, *Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1*, Cryptology ePrint Archive, Report 2008/469, 2008.

[Man11] Stéphane Manuel, *Classification and generation of disturbance vectors for collision attacks against SHA-1*, Des. Codes Cryptography **59** (2011), no. 1-3, 247–263.

[Mer78] Ralph C. Merkle, *Secure Communications Over Insecure Channels*, Commun. ACM **21** (1978), no. 4, 294–299.

[Mer82] Ralph C. Merkle, *Secrecy, Authentication, and Public Key Systems*, UMI Research press, 1982.

[Mer89] Ralph C. Merkle, *One Way Hash Functions and DES*, CRYPTO (Gilles Brassard, ed.), Lecture Notes in Computer Science, vol. 435, Springer, 1989, pp. 428–446.

[MHP09] Cameron McDonald, Philip Hawkes, and Josef Pieprzyk, *Differential Path for SHA-1 with complexity $O(2^{52})$*, Cryptology ePrint Archive, Report 2009/259, 2009.

[Mik04] Ondrej Mikle, *Practical Attacks on Digital Signatures Using MD5 Message Digest*, Cryptology ePrint Archive, Report 2004/356, 2004.

[MP05] Krystian Matusiewicz and Josef Pieprzyk, *Finding Good Differential Patterns for Attacks on SHA-1*, WCC (Øyvind Ytrehus, ed.), Lecture Notes in Computer Science, vol. 3969, Springer, 2005, pp. 164–177.

[MP08] Stéphane Manuel and Thomas Peyrin, *Collisions on SHA-0 in One Hour*, FSE (Kaisa Nyberg, ed.), Lecture Notes in Computer Science, vol. 5086, Springer, 2008, pp. 16–35.

[MPRR06] Florian Mendel, Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, *The Impact of Carries on the Complexity of Collision Attacks on SHA-1*, FSE (Matthew J. B. Robshaw, ed.), Lecture Notes in Computer Science, vol. 4047, Springer, 2006, pp. 278–292.

[MRR07] Florian Mendel, Christian Rechberger, and Vincent Rijmen, *Update on SHA-1*, Rump session of CRYPTO 2007, 2007.

[MS06] James A. Muir and Douglas R. Stinson, *Minimality and other properties of the width- nonadjacent form*, Math. Comput. **75** (2006), no. 253, 369–384.

[NIS93] National Institute of Standards and Technology NIST, *FIPS PUB 180: Secure Hash Standard*, 1993.

[NIS95] National Institute of Standards and Technology NIST, *FIPS PUB 180-1: Secure Hash Standard*, 1995.

[NIS02] National Institute of Standards and Technology NIST, *FIPS PUB 180-2: Secure Hash Standard*, 2002.

[NIS07] National Institute of Standards and Technology NIST, *Announcing Request for Candidate Algorithm Nominations for a new Cryptographic Hash Algorithm (SHA-3) Family*, Federal Register Vol. 72, No. 212, November 2007, Available at `http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf`.

[NIS08] National Institute of Standards and Technology NIST, *FIPS PUB 180-3: Secure Hash Standard*, 2008.

[NIS11] National Institute of Standards and Technology NIST, *Draft FIPS PUB 180-4: Secure Hash Standard*, 2011.

[NSS+06] Yusuke Naito, Yu Sasaki, Takeshi Shimoyama, Jun Yajima, Noboru Kunihiro, and Kazuo Ohta, *Improved Collision Search for SHA-0*, ASIACRYPT (Xuejia Lai and Kefei Chen, eds.), Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 21–36.

[PCTH11] T. Polk, L. Chen, S. Turner, and P. Hoffman, *Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms*, Internet Request for Comments, March 2011, RFC 6194.

[PD05] Robert Primmer and Carl D'Halluin, *Collision and Preimage Resistance of the Centera Content Address*, Technical Report, 2005, EMC Corporation.

[PRR05] Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, *Exploiting Coding Theory for Collision Attacks on SHA-1*, IMA Int. Conf. (Nigel P. Smart, ed.), Lecture Notes in Computer Science, vol. 3796, Springer, 2005, pp. 78–95.

[Rab78] M. O. Rabin, *Digitalized Signatures*, Foundations of Secure Computation (Richard A. DeMillo, David P. Dobkin, Anita K. Jones, and Richard J. Lipton, eds.), Academic Press, 1978, pp. 155–168.

[Riv90a] Ronald L. Rivest, *The MD4 Message Digest Algorithm*, CRYPTO (Alfred Menezes and Scott A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer, 1990, pp. 303–311.

[Riv90b] Ronald L. Rivest, *The MD4 Message-Digest Algorithm*, Internet Request for Comments, October 1990, RFC 1186; obsoleted by RFC 1320.

[Riv92] Ronald L. Rivest, *The MD5 Message-Digest Algorithm*, Internet Request for Comments, April 1992, RFC 1321.

[RO05] Vincent Rijmen and Elisabeth Oswald, *Update on SHA-1*, CT-RSA (Alfred Menezes, ed.), Lecture Notes in Computer Science, vol. 3376, Springer, 2005, pp. 58–71.

[Rog06] Phillip Rogaway, *Formalizing Human Ignorance*, VIETCRYPT (Phong Q. Nguyen, ed.), Lecture Notes in Computer Science, vol. 4341, Springer, 2006, pp. 211–228.

[Rom90] John Rompel, *One-Way Functions are Necessary and Sufficient for Secure Signatures*, STOC, ACM, 1990, pp. 387–394.

[RS04] Phillip Rogaway and Thomas Shrimpton, *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance*, FSE (Bimal K. Roy and Willi Meier, eds.), Lecture Notes in Computer Science, vol. 3017, Springer, 2004, pp. 371–388.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM **21** (1978), no. 2, 120–126.

[Sel06] Peter Selinger, 2006, `http://www.mathstat.dal.ca/~selinger/md5collision/`.

[Sha48] Claude E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal **27** (1948), 379–423, 623–656.

[Sha49] Claude E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal **28** (1949), 657–715.

[SLdW07a] Marc Stevens, Arjen Lenstra, and Benne de Weger, 2007, `http://www.win.tue.nl/hashclash/Nostradamus/`.

[SLdW07b] Marc Stevens, Arjen Lenstra, and Benne de Weger, 2007, `http://www.win.tue.nl/hashclash/SoftIntCodeSign/`.

[SLdW07c] Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities*, EUROCRYPT (Moni Naor, ed.), Lecture Notes in Computer Science, vol. 4515, Springer, 2007, pp. 1–22.

[SLdW12] Marc Stevens, Arjen Lenstra, and Benne de Weger, *Chosen-Prefix Collisions for MD5 and Applications*, To appear in International Journal of Applied Cryptology (IJACT), 2012.

[SNKO05] Yu Sasaki, Yusuke Naito, Noboru Kunihiro, and Kazuo Ohta, *Improved Collision Attack on MD5*, Cryptology ePrint Archive, Report 2005/400, 2005.

[SSA+09a] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger, 2009, `http://www.win.tue.nl/hashclash/rogue-ca/`.

[SSA+09b] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger, *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*, CRYPTO (Shai Halevi, ed.), Lecture Notes in Computer Science, vol. 5677, Springer, 2009, pp. 55–69.

[Ste06] Marc Stevens, *Fast Collision Attack on MD5*, Cryptology ePrint Archive, Report 2006/104, 2006.

[Ste09] Didier Stevens, 2009, `http://blog.didierstevens.com/2009/01/17/`.

[Ste10] Marc Stevens, *SHA-1 near collision attack source code*, Nov 2010, `http://code.google.com/p/hashclash`.

[VJBT08] Jirí Vábek, Daniel Joscák, Milan Bohácek, and Jirí Tuma, *A New Type of 2-Block Collisions in MD5*, INDOCRYPT (Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, eds.), Lecture Notes in Computer Science, vol. 5365, Springer, 2008, pp. 78–90.

[vOW99] Paul C. van Oorschot and Michael J. Wiener, *Parallel Collision Search with Cryptanalytic Applications*, J. Cryptology **12** (1999), no. 1, 1–28.

[Wan06] Xiaoyun Wang, *Cryptanalysis of Hash Functions and Potential Dangers*, RSA Conference 2006 invited talk, 2006.

[WFLY04] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu, *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, Cryptology ePrint Archive, Report 2004/199, 2004.

[Wu11] Hongjun Wu, *The Hash Function JH*, Submission to NIST (Round 3), 2011.

[WY05] Xiaoyun Wang and Hongbo Yu, *How to Break MD5 and Other Hash Functions*, EUROCRYPT (Ronald Cramer, ed.), Lecture Notes in Computer Science, vol. 3494, Springer, 2005, pp. 19–35.

[WYY05a] Xiaoyun Wang, Andrew C. Yao, and Frances Yao, *Cryptanalysis on SHA-1*, NIST Cryptographic Hash Workshop, 2005, `http://csrc.nist.gov/groups/ST/hash/documents/Wang_SHA1-New-Result.pdf`.

[WYY05b] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, *Finding Collisions in the Full SHA-1*, CRYPTO (Victor Shoup, ed.), Lecture Notes in Computer Science, vol. 3621, Springer, 2005, pp. 17–36.

[WYY05c] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin, *Efficient Collision Search Attacks on SHA-0*, CRYPTO (Victor Shoup, ed.), Lecture Notes in Computer Science, vol. 3621, Springer, 2005, pp. 1–16.

[XF09] Tao Xie and Dengguo Feng, *How To Find Weak Input Differences For MD5 Collision Attacks*, Cryptology ePrint Archive, Report 2009/223, 2009.

[XF10] Tao Xie and Deng Guo Feng, *Construct MD5 Collisions Using Just A Single Block Of Message*, Cryptology ePrint Archive, Report 2010/643, 2010.

[XFL08] Tao Xie, DengGuo Feng, and FanBao Liu, *A New Collision Differential For MD5 With Its Full Differential Path*, Cryptology ePrint Archive, Report 2008/230, 2008.

[XLF08] Tao Xie, Fan Bao Liu, and Deng Guo Feng, *Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5?*, Cryptology ePrint Archive, Report 2008/391, 2008.

[YIN+08] Jun Yajima, Terutoshi Iwasaki, Yusuke Naito, Yu Sasaki, Takeshi Shimoyama, Noboru Kunihiro, and Kazuo Ohta, *A strict evaluation method on the number of conditions for the SHA-1 collision search*, ASIACCS (Masayuki Abe and Virgil D. Gligor, eds.), ACM, 2008, pp. 10–20.

[YS05] Jun Yajima and Takeshi Shimoyama, *Wang's sufficient conditions of MD5 are not sufficient*, Cryptology ePrint Archive, Report 2005/263, 2005.

[YSN+07] Jun Yajima, Yu Sasaki, Yusuke Naito, Terutoshi Iwasaki, Takeshi Shimoyama, Noboru Kunihiro, and Kazuo Ohta, *A New Strategy for Finding a Differential Path of SHA-1*, ACISP (Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson, eds.), Lecture Notes in Computer Science, vol. 4586, Springer, 2007, pp. 45–58.

[Yuv79] G. Yuval, *How to Swindle Rabin*, Cryptologia **3** (1979), 187–189.

Index

Notation

$\texttt{01}_2$	Binary notation	17
$\texttt{0f}_{16}$	Hexadecimal notation	17
$\overline{b}$	Bit at position b is -1 in BSDR notation	19
$X \wedge Y$	Bitwise AND	17, 63
$\overline{X}$	Bitwise negation	17, 63
$X \vee Y$	Bitwise OR	17, 63
$X \oplus Y$	Bitwise XOR	17, 63
$RL(X, n)$	Bitwise cyclic left rotation	18, 19, 63, 64
$RR(X, n)$	Bitwise cyclic right rotation	18, 19, 63, 64
$dRL(X, n)$	Bitwise cyclic left rotation of differences	74
ΔX	Bitwise difference	19, 74, 176
δX	Modular difference	19, 74, 176
$X[i]$	Bit selection	18, 19, 63, 64
$X + Y$	Modular addition	18, 63
$X - Y$	Modular subtraction	18, 63
X'	Related variable	19, 74
$\sigma(X)$	Mapping from $\{-1, 0, 1\}^N$ to $\mathbb{Z}_{2^N}$	19, 64
$w \hookrightarrow v$	Substitution rule	152
$w(X)$	Weight of (signed-)bit string	18, 19, 63, 64

List of Algorithms

List of Figures

List of Tables

List of Theorems