

Finding SHA-1 Characteristics -General Results and Applications

<u>Christophe De Cannière</u> and <u>Christian Rechberger</u>

NIST Hash Function Workshop 2006

Institute for Applied Information Processing and Communications (IAIK) - <u>Krypto Group</u>

Faculty of Computer Science Graz University of Technology



To appear at ASIACRYPT 2006





Finding Collisions as a Continuing Optimization Process



work factor







- Two key techniques of Wang et al.:
 - •Manually find suitable complex characteristic NL₁ and NL₂
 - Advanced message modification to improve work factor
- Methods are rather ad hoc (manual)Optimization?





New View – Roughly Illustrated





Principles

Generalized conditions







2

work factor



1024

Leedom freedom freedom

- Generalized conditions
- •Use "bit-sliced design" to efficiently
 - Propagate conditions within one step transformation
 - Propagate conditions among all step transformations





2

work factor



1024

Leedom freedom freedom

- Generalized conditions
- •Use "bit-sliced design" to efficiently
 - Propagate conditions within one step transformation
 - Propagate conditions among all step transformations
- Precise estimate of work factor
 - Model: simple depth-first exhaustive search
 - #nodes in search tree

Continuously add more conditions to improve work factor





New View – Roughly Illustrated







New View – Roughly Illustrated







Example: 64-step SHA-1 Collision

i		Message 1,	first block	ς
1-4	63DAEFDD	30A0D167	52EDCDA4	90012F5F
5-8	0DB4DFB5	E5A3F9AB	AE66EE56	12A5663F
9-12	D0320F85	8505C67C	756336DA	DFFF4DB9
13-16	596D6A95	0855F129	429A41B3	ED5AE1CD
i		Message 1,	second bloc	k
1-4	3B2AB4E1	AAD112EF	669C9BAE	5DEA4D14
5-8	1DBE220E	AB46A5E0	96E2D937	F3E58B63
9-12	BE594F1C	BD63F044	50C42AA5	8B793546
13-16	A9B24128	816FD53A	D1B663DC	B615DD01
i	Message 2, first block			
1-4	63DAEFDE	70A0D135	12EDCDE4	70012F0D
5-8	ADB4DFB5	65A3F9EB	8E66EE57	32A5665F
9-12	50320F84	C505C63E	B5633699	9FFF4D9B
13-16	596D6A96	4855F16B	829A41F0	2D5AE1EF
13-16 <i>i</i>	596D6A96	4855F16B Message 2,	829A41F0 second bloc	2D5AE1EF k
13-16 <i>i</i> 1-4	596D6A96 3B2AB4E2	4855F16B Message 2, EAD112BD	829A41F0 second bloc 269C9BEE	2D5AE1EF k BDEA4D46
13-16 <i>i</i> 1-4 5-8	596D6A96 3B2AB4E2 BDBE220E	4855F16B Message 2, EAD112BD 2B46A5A0	829A41F0 second bloc 269C9BEE B6E2D936	2D5AE1EF k BDEA4D46 D3E58B03
13-16 <i>i</i> 1-4 5-8 9-12	596D6A96 3B2AB4E2 BDBE220E 3E594F1D	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6	2D5AE1EF k BDEA4D46 D3E58B03 CB793564
$ \begin{array}{c} 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\ \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23
$ \begin{array}{c} 13-16 \\ i \\ 1-4 \\ 5-8 \\ 9-12 \\ 13-16 \\ i \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks
$ \begin{array}{r} 13-16 \\ i \\ 1-4 \\ 5-8 \\ 9-12 \\ 13-16 \\ \hline i \\ 1-4 \\ \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks E0000052
$ \begin{array}{r} 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\\\\hline i\\ 1-4\\ 5-8\\\\\hline \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003 A0000000	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052 80000040	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040 20000001	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks E0000052 20000060
$ \begin{array}{r} 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\\\\hline i\\ 1-4\\ 5-8\\ 9-12\\\\\hline \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003 A0000000 80000001	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052 80000040 40000042	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040 20000001 C0000043	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks E0000052 20000060 40000022
$ \begin{array}{r} 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\\\\hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\\\\hline \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003 A0000000 80000001 00000003	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052 80000040 40000042 40000042	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040 20000001 C0000043 C0000043	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 locks E0000052 20000060 40000022 C0000022
$ \begin{array}{r} 13-16\\ i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\ \hline i\\ i\\ \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003 A0000000 80000001 00000003	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052 80000040 40000042 40000042	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040 20000001 C0000043 C0000043 ng hash valu	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks E0000052 20000060 40000022 C0000022
$ \begin{array}{r} 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\ \hline i\\ 1-4\\ 5-8\\ 9-12\\ 13-16\\ \hline i\\ 1-4\\ \hline i\\ 1-4\\ \hline \end{array} $	596D6A96 3B2AB4E2 BDBE220E 3E594F1D A9B2412B XOR 00000003 A0000000 80000001 00000003 T A750337B	4855F16B Message 2, EAD112BD 2B46A5A0 FD63F006 C16FD578 -difference 40000052 80000040 40000042 40000042 'he collidir 55FFFDBB	829A41F0 second bloc 269C9BEE B6E2D936 90C42AE6 11B6639F for both b 40000040 20000040 20000043 C0000043 C0000043 ng hash valu C08DB36C	2D5AE1EF k BDEA4D46 D3E58B03 CB793564 7615DD23 Locks E0000052 20000060 40000022 C0000022 es 0C6CFD97

- 64-step 2-block colliding pair of messages
- Work factor was equivalent to 2³⁵ SHA-1 computations (1 day on a single PC)





Summary – What's new?

Automatically finding complex characteristics for SHA-1

Precise calculation of work factor and available degrees of freedom for collision search

New and slim final search procedure





Future Work / Work in Progress

- Updated 80-step estimate
- Apply to other hash functions like RIPEMD-160, SHA-2 members
- Allow arbitrary different messages before colliding block
- Speedup for herding attacks



Finding SHA-1 Characteristics

<u>Christophe De Cannière</u> and <u>Christian Rechberger</u>

Institute for Applied Information Processing and Communications (IAIK) - <u>Krypto Group</u>

Faculty of Computer Science Graz University of Technology



http://www.iaik.tugraz.at/research/krypto